# ZyWALL USG 100/200 Series

*Unified Security Gateway*

## User's Guide



### Default Login Details

| | |
|---|---|
| LAN1 Port | P4 |
| IP Address | https://192.168.1.1 |
| User Name | admin |
| Password | 1234 |

Firmware Version 2.12
Edition 1, 6/2009

***www.zyxel.com***

ZyXEL

# About This User's Guide

## Intended Audience

This manual is intended for people who want to want to configure the ZyWALL using the web configurator.

## How To Use This Guide

- Read Chapter 1 on page 31 chapter for an overview of features available on the ZyWALL.
- Read Chapter 3 on page 43 for web browser requirements and an introduction to the main components, icons and menus in the ZyWALL web configurator.
- Read Chapter 4 on page 55 if you're using the wizards for first time setup and you want more detailed information than what the real time online help provides.
- It is highly recommended you read Chapter 5 on page 81 for detailed information on essential terms used in the ZyWALL, what prerequisites are needed to configure a feature and how to use that feature.
- It is highly recommended you read Chapter 6 on page 101 for ZyWALL application examples.
- Subsequent chapters are arranged by menu item as defined in the web configurator. Read each chapter carefully for detailed information on that menu item.
- To find specific information in this guide, use the **Contents Overview**, the **Table of Contents**, the **Index**, or search the PDF file. E-mail techwriters@zyxel.com.tw if you cannot find the information you require.

## Related Documentation

- Quick Start Guide

  The Quick Start Guide is designed to show you how to make the ZyWALL hardware connections, rack mounting and access the web configurator wizards. (See the wizard real time help for information on configuring each screen.) It contains a connection diagram, default settings, handy checklists and information on setting up your network and configuring for Internet access.

- CLI Reference Guide

  The CLI Reference Guide explains how to use the Command-Line Interface (CLI) to configure the ZyWALL.

Note: It is recommended you use the web configurator to configure the ZyWALL.

- Web Configurator Online Help

  Click the help icon in any screen for help in configuring that screen and supplementary information.

- Support Disc

  Refer to the included CD for support documents.

- ZyXEL Web Site

  Please refer to www.zyxel.com for additional support documentation and product certifications.

## User Guide Feedback

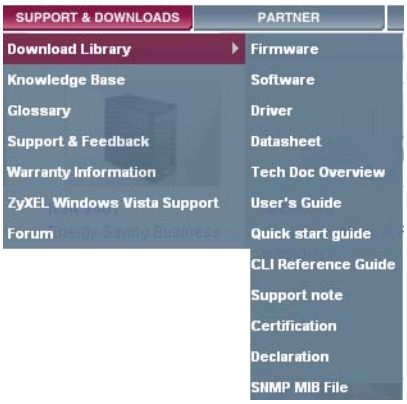
Help us help you. Send all User Guide-related comments, questions or suggestions for improvement to the following address, or use e-mail instead. Thank you!

The Technical Writing Team,
ZyXEL Communications Corp.,
6 Innovation Road II,
Science-Based Industrial Park,
Hsinchu, 300, Taiwan.

E-mail: techwriters@zyxel.com.tw

## Need More Help?

More help is available at www.zyxel.com.




- Download Library

  Search for the latest product updates and documentation from this link. Read the Tech Doc Overview to find out how to efficiently use the User Guide, Quick Start Guide and Command Line Interface Reference Guide in order to better understand how to use your product.

- Knowledge Base

  If you have a specific question about your product, the answer may be here. This is a collection of answers to previously asked questions about ZyXEL products.

- Forum

  This contains discussions on ZyXEL products. Learn from others who use ZyXEL products and share your experiences as well.

## Customer Support

Should problems arise that cannot be solved by the methods listed above, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device.

See http://www.zyxel.com/web/contact_us.php for contact information. Please have the following information ready when you contact an office.

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

## Disclaimer

Graphics in this book may differ slightly from the product due to differences in operating systems, operating system versions, or if you installed updated firmware/software for your device. Every effort has been made to ensure that the information in this manual is accurate.

# Document Conventions

## Warnings and Notes

These are how warnings and notes are shown in this User's Guide.

> **Warnings tell you about things that could harm you or your device.**

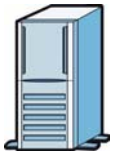
Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

## Syntax Conventions

- The ZyWALL may be referred to as the "ZyWALL", the "device", the "system" or the "product" in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket ( > ) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

## Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The ZyWALL icon is not an exact representation of your device.

| | | |
|---|---|---|
| ZyWALL  | Computer  | Notebook computer  |
| Server  | Firewall  | Telephone  |
| Switch  | Router  | |

# Safety Warnings

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- CAUTION: RISK OF EXPLOSION IF BATTERY (on the motherboard) IS REPLACED BY AN INCORRECT TYPE. DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS. Dispose them at the applicable collection point for the recycling of electrical and electronic equipment. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.

# Contents Overview

# Table of Contents

# PART I
# Getting Started

# 1

# Introducing the ZyWALL

This chapter gives an overview of the ZyWALL. It explains the front panel ports, LEDs, introduces the management methods, and lists different ways to start or stop the ZyWALL.

## 1.1 Overview and Key Default Settings

The ZyWALL is a comprehensive security device. Its flexible configuration helps network administrators set up the network and enforce security policies efficiently. In addition, the ZyWALL provides excellent throughput, making it an ideal solution for reliable, secure service.

The ZyWALL's security features include VPN, firewall, anti-virus, content filtering, IDP (Intrusion Detection and Prevention), ADP (Anomaly Detection and Protection), and certificates. It also provides bandwidth management, Instant Messaging (IM) and Peer to Peer (P2P) control, NAT, port forwarding, policy routing, DHCP server and many other powerful features. Flexible configuration helps you set up the network and enforce security policies efficiently. See Chapter 2 on page 35 for a more detailed overview of the ZyWALL's features.

The ZyWALL provides excellent throughput with the reliability of dual WAN Gigabit Ethernet ports and load balancing. You can also use a 3G cellular card (not included) for a third WAN connection.

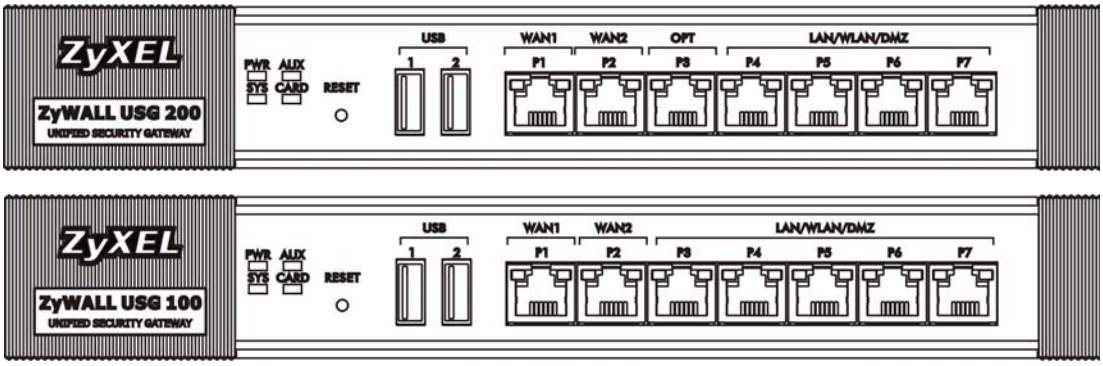
The ZyWALL lets you set up multiple networks for your company. The De-Militarized Zone (DMZ) increases LAN security by providing separate ports for connecting publicly accessible servers. The ZyWALL also provides two separate LAN networks. You can set ports to be part of the LAN1, WLAN, or DMZ. Alternatively, you can deploy the ZyWALL as a transparent firewall in an existing network with minimal configuration.

You can insert a wireless LAN card into the PCMCIA/CardBus slot to add an IEEE 802.11b/g-compliant wireless LAN.

Configure the ZyWALL USG 200's OPT Gigabit Ethernet port as a third WAN port, an additional LAN1, WLAN, or DMZ port or a separate network.

# 1.2 Front Panel

**Figure 1** ZyWALL Front Panel




## 1.2.1 Front Panel LEDs

The following table describes the LEDs.

**Table 1** Front Panel LEDs

| LED | COLOR | STATUS | DESCRIPTION |
|---|---|---|---|
| PWR | | Off | The ZyWALL is turned off. |
| | Green | On | The ZyWALL is turned on. |
| | Red | On | There is a hardware component failure. Shut down the device, wait for a few minutes and then restart the device (see Section 1.4 on page 34). If the LED turns red again, then please contact your vendor. |
| SYS | Green | Off | The ZyWALL is not ready or has failed. |
| | | On | The ZyWALL is ready and running. |
| | | Flashing | The ZyWALL is restarting. |
| AUX | Green | Off | The **AUX** port is not connected. |
| | | Flashing | The **AUX** port is sending or receiving packets. |
| | | On | The **AUX** port is connected. |
| P1, P2, ... | Green | Off | There is no traffic on this port. |
| | | Flashing | The ZyWALL is sending or receiving packets on this port. |
| | Orange | Off | There is no connection on this port. |
| | | On | This port has a successful link. |
| Card | Green | Off | There is no card in the slot. |
| | | On | There is a card in the slot. |
| | | Flashing | The card in the slot is sending or receiving traffic. |

# 1.3 Management Overview

You can use the following ways to manage the ZyWALL.

### Web Configurator

The Web Configurator allows easy ZyWALL setup and management using an Internet browser. This User's Guide provides information about the Web Configurator.

**Figure 2** Managing the ZyWALL: Web Configurator

### Command-Line Interface (CLI)

The CLI allows you to use text-based commands to configure the ZyWALL. You can access it using remote management (for example, SSH or Telnet) or via the console port. See the Command Reference Guide for more information about the CLI.

### Console Port

You can use the console port to manage the ZyWALL using CLI commands. See the Command Reference Guide for more information about the CLI.

The default settings for the console port are as follows.

**Table 2** Console Port Default Settings

| SETTING | VALUE |
|---|---|
| Speed | 115200 bps |
| Data Bits | 8 |
| Parity | None |
| Stop Bit | 1 |
| Flow Control | Off |

# 1.4 Starting and Stopping the ZyWALL

Here are some of the ways to start and stop the ZyWALL.

**Table 3** Starting and Stopping the ZyWALL

| METHOD | DESCRIPTION |
|---|---|
| Turning on the power | A cold start occurs when you turn on the power to the ZyWALL. The ZyWALL powers up, checks the hardware, and starts the system processes. |
| Rebooting the ZyWALL | A warm start (without powering down and powering up again) occurs when you use the **Reboot** button in the **Reboot** screen or when you use the `reboot` command. The ZyWALL writes all cached data to the local storage, stops the system processes, and then does a warm start. |
| Using the RESET button | If you press the **RESET** button, the ZyWALL sets the configuration to its default values and then reboots. |
| Using the `shutdown` command | The `shutdown` command writes all cached data to the local storage and stops the system processes. It does not turn off the power.You have to turn the power off and on manually to start the ZyWALL again. You should use this command before you turn off the ZyWALL. |
| Disconnecting the power | Power off occurs when you turn off the power to the ZyWALL. The ZyWALL simply turns off. It does not stop the system processes or write cached data to local storage. |

Note: It is recommended you use the `shutdown` command before turning off the ZyWALL.

When you apply configuration files or running shell scripts, the ZyWALL does not stop or start the system processes. However, you might lose access to network resources temporarily while the ZyWALL is applying configuration files or running shell scripts.

# 2

# Features and Applications

This chapter introduces the main features and applications of the ZyWALL.

## 2.1 Features

The ZyWALL's security features include VPN, firewall, anti-virus, content filtering, IDP (Intrusion Detection and Prevention), ADP (Anomaly Detection and Protection), and certificates. It also provides bandwidth management, NAT, port forwarding, policy routing, DHCP server and many other powerful features.

The rest of this section provides more information about the features of the ZyWALL.

### High Availability

To ensure the ZyWALL provides reliable, secure Internet access, set up one or more of the following:

- Multiple WAN ports and configure load balancing between these ports.
- One or more 3G (cellular) connections.
- An auxiliary (backup) Internet connection.
- A backup ZyWALL in the event the master ZyWALL fails (device HA).

### Virtual Private Networks (VPN)

Use IPSec, SSL, or L2TP VPN to provide secure communication between two sites over the Internet or any insecure network that uses TCP/IP for communication. The ZyWALL also offers hub-and-spoke IPSec VPN.

### Flexible Security Zones

Many security settings are made by zone, not by interface, port, or network. As a result, it is much simpler to set up and to change security settings in the ZyWALL. You can add interfaces and VPN tunnels to zones.

### Firewall

The ZyWALL's firewall is a stateful inspection firewall. The ZyWALL restricts access by screening data packets against defined access rules. It can also inspect sessions. For example, traffic from one zone is not allowed unless it is initiated by a computer in another zone first.

### Intrusion Detection and Prevention (IDP)

IDP (Intrusion Detection and Protection) can detect malicious or suspicious packets and respond instantaneously. It detects pattern-based attacks in order to protect against network-based intrusions. See Section 31.6.2 on page 533 for a list of attacks that the ZyWALL can protect against. You can also create your own custom IDP rules.

### Anomaly Detection and Prevention (ADP)

ADP (Anomaly Detection and Prevention) can detect malicious or suspicious packets and respond instantaneously. It can detect:

- Anomalies based on violations of protocol standards (RFCs – Requests for Comments)
- Abnormal flows such as port scans.

The ZyWALL's ADP protects against network-based intrusions. See Section 32.3.4 on page 561 and Section 32.3.5 on page 564 for more on the kinds of attacks that the ZyWALL can protect against. You can also create your own custom ADP rules.

### Bandwidth Management

Bandwidth management allows you to allocate network resources according to defined policies. This policy-based bandwidth allocation helps your network to better handle applications such as Internet access, e-mail, Voice-over-IP (VoIP), video conferencing and other business-critical applications.

### Content Filter

Content filtering allows schools and businesses to create and enforce Internet access policies tailored to the needs of the organization.

You can also subscribe to category-based content filtering that allows your ZyWALL to check web sites against an external database of dynamically-updated ratings of millions of web sites. You then simply select categories to block or monitor, such as pornography or racial intolerance, from a pre-defined list.

### Anti-Virus Scanner

With the anti-virus packet scanner, your ZyWALL scans files transmitting through the enabled interfaces into the network. The ZyWALL helps stop threats at the network edge before they reach the local host computers.

### Anti-Spam

The anti-spam feature can mark or discard spam. Use the white list to identify legitimate e-mail. Use the black list to identify spam e-mail. The ZyWALL can also check e-mail against a DNS black list (DNSBL) of IP addresses of servers that are suspected of being used by spammers.

### Application Patrol

Application patrol (App. Patrol) manages instant messenger (IM), peer-to-peer (P2P) applications like MSN and BitTorrent. You can even control the use of a particular application's individual features (like text messaging, voice, video conferencing, and file transfers). Application patrol has powerful bandwidth management including traffic prioritization to enhance the performance of delay-sensitive applications like voice and video. You can also use an option that gives SIP priority over all other traffic. This maximizes SIP traffic throughput for improved VoIP call sound quality.

## 2.2 Packet Flow

This section lists the order in which the ZyWALL applies its features and checks. The following is the key used to describe the packet flow in the ZyWALL.

**Table 4** Packet Flow Key

| | |
|---|---|
| Ethernet | The interface on which the packet is received or sent |
| VLAN | Virtual LAN |
| Encap | The PPPoE or PPTP encapsulation used |
| | |
| ALG | Application Layer Gateway |
| DNAT | Destination NAT |
| | |
| Routing | Routing includes policy routes, interface routing, static routes and load balancing for example. |
| | |
| FW | Firewall (Through ZyWALL) |
| zFW | Firewall (To ZyWALL) |
| IDP | Intrusion Detection and Protection |

**Table 4** Packet Flow Key (continued)

| | |
|---|---|
| ADP | Anomaly Detection and Protection |
| AP | Application Patrol |
| AS | Anti-spam |
| CF | Content Filtering |
| | |
| SNAT | Source NAT |
| IPSec D/E | VPN Decryption/Encryption |
| BWM | Bandwidth Management |
| RM | Remote Management (System) |
| AV | Anti-Virus |

## 2.2.1 Interface to Interface (Through ZyWALL)

Ethernet -> VLAN -> Encap -> ALG -> DNAT-> Routing -> FW -> IDP -> AP-> CF -> AV -> AS -> SNAT -> BWM -> Encap -> VLAN -> Ethernet

## 2.2.2 Interface to Interface (To/From ZyWALL)

To: Ethernet -> VLAN -> Encap -> ALG -> DNAT -> Routing -> zFW -> ADP -> RM
From: RM -> Routing -> BWM -> Encap -> VLAN -> Ethernet

## 2.2.3 Interface to Interface (From VPN Tunnel)

This example shows the flow from a VPN tunnel though the ZyWALL, not to the ZyWALL or to another VPN tunnel (VPN concentrator).

Ethernet -> VLAN -> Encap -> ALG -> DNAT-> Routing -> zFW -> IPSec D -> ALG -> AC -> DNAT-> Routing -> FW -> IDP -> AP -> CF -> AV -> AS -> SNAT -> BWM -> Encap -> VLAN -> Ethernet

## 2.2.4 Interface to Interface (To VPN Tunnel)

This example shows the flow to a VPN tunnel from a source other than the ZyWALL or another VPN tunnel (VPN concentrator).

Ethernet -> VLAN -> Encap -> ALG -> DNAT-> Routing -> FW -> IDP -> AP -> CF -> AV -> AS -> SNAT -> IPSec E -> Routing -> BWM -> Encap -> VLAN -> Ethernet

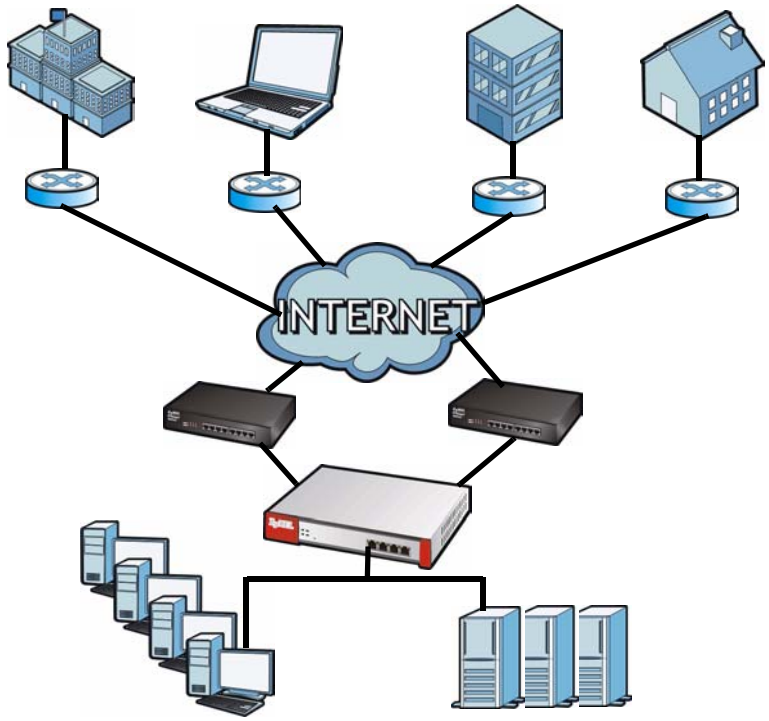
# 2.3 Applications

These are some example applications for your ZyWALL. See also Chapter 6 on page 101 for configuration tutorial examples.

## 2.3.1 VPN Connectivity

Set up VPN tunnels with other companies, branch offices, telecommuters, and business travelers to provide secure access to your network. You can also set up additional connections to the Internet to provide better service.

**Figure 3** Applications: VPN Connectivity




## 2.3.2 SSL VPN Network Access

You can configure the ZyWALL to provide SSL VPN network access to remote users. There are two SSL VPN network access modes: reverse proxy and full tunnel.

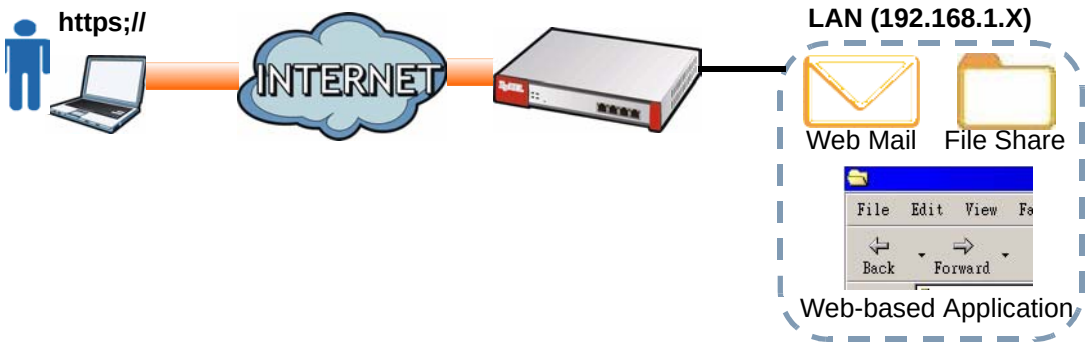
### 2.3.2.1 Reverse Proxy Mode

In reverse proxy mode, the ZyWALL is a proxy that acts on behalf of the local network servers (such as your web and mail servers). As the final destination, the

ZyWALL appears to be the server to remote users. This provides an added layer of protection for your internal servers.

With reverse proxy mode, remote users can easily access any web-based applications on the local network by clicking on links or entering the provided URL. You do not have to install additional client software on the remote user computers for access.

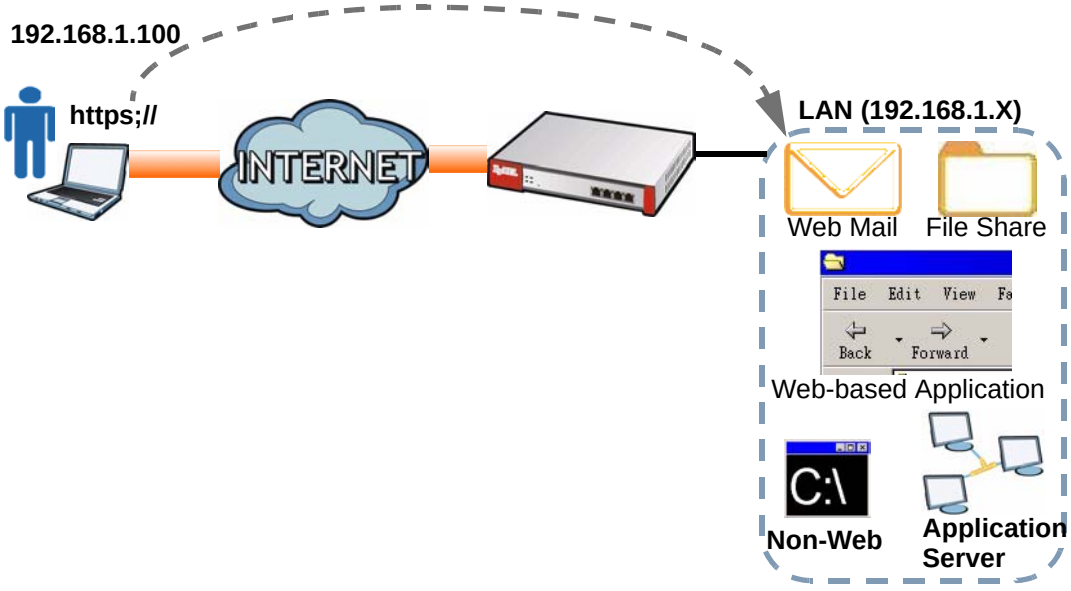
**Figure 4** Network Access Mode: Reverse Proxy




## 2.3.2.2 Full Tunnel Mode

In full tunnel mode, a virtual connection is created for remote users with private IP addresses in the same subnet as the local network. This allows them to access network resources in the same way as if they were part of the internal network.

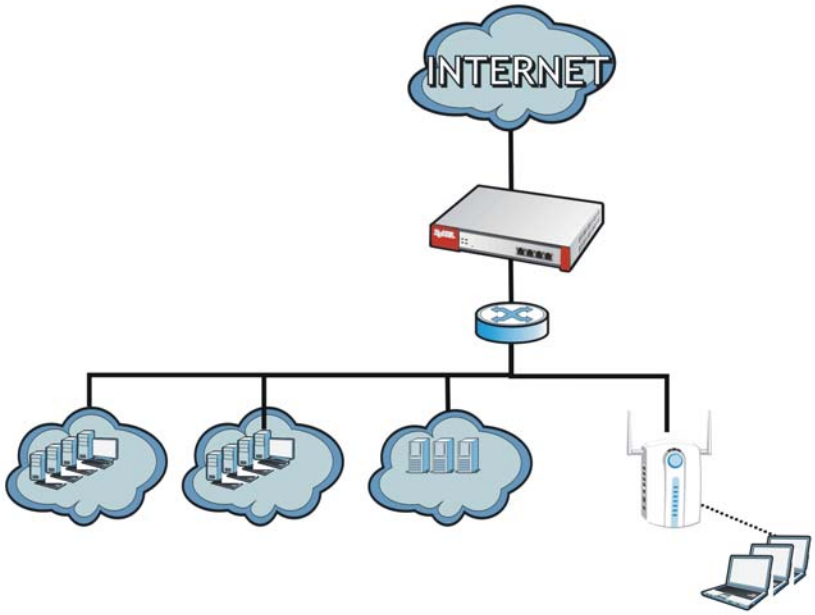
**Figure 5** Network Access Mode: Full Tunnel Mode



### 2.3.3 User-Aware Access Control

Set up security policies that restrict access to sensitive information and shared resources based on the user who is trying to access it.

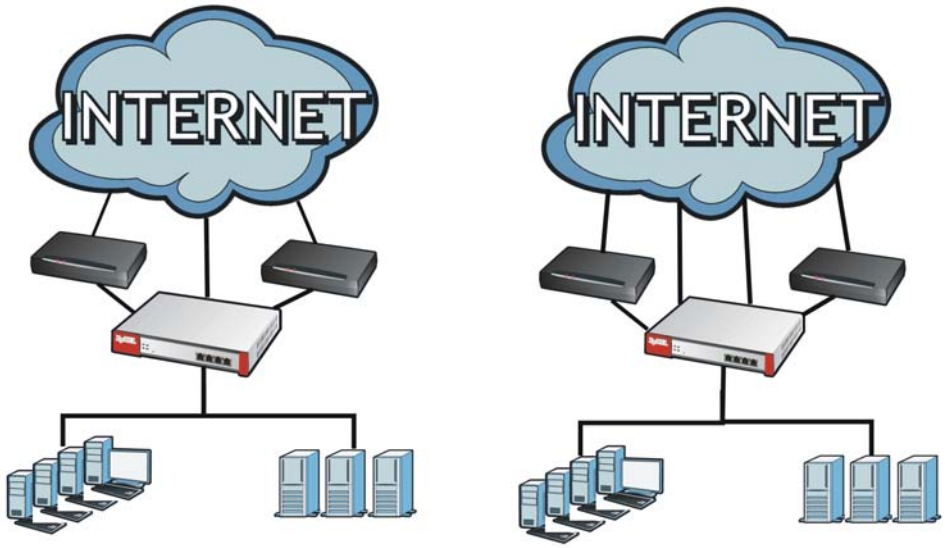
**Figure 6** Applications: User-Aware Access Control




### 2.3.4 Multiple WAN Interfaces

Set up multiple connections to the Internet on the same port, or set up multiple connections on different ports. In either case, you can balance the loads between them.

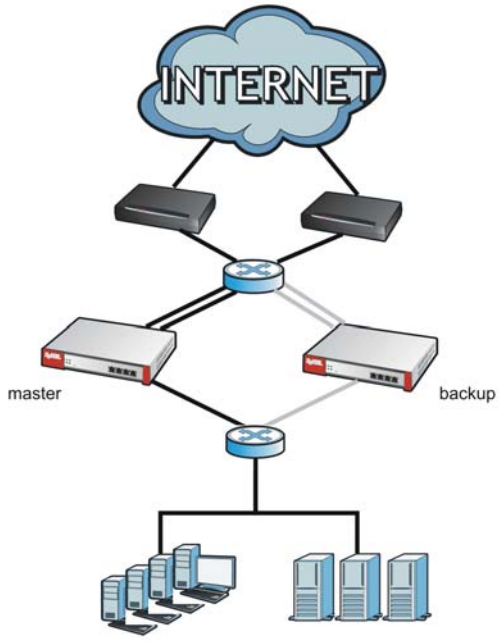
**Figure 7** Applications: Multiple WAN Interfaces



## 2.3.5 Device HA

Set up an additional ZyWALL as a backup gateway to ensure the default gateway is always available for the network.

**Figure 8** Applications: Device HA



# 3

# Web Configurator

The ZyWALL Web Configurator allows easy ZyWALL setup and management using an Internet browser. Unless otherwise specified, the ZyWALL USG 200 screens are shown.

## 3.1 Web Configurator Requirements

In order to use the Web Configurator, you must

- Use Internet Explorer 6.0 or later, Netscape Navigator 7.2 or later, or Firefox 1.0.7 or later
- Allow pop-up windows (blocked by default in Windows XP Service Pack 2)
- Enable JavaScripts (enabled by default)
- Enable Java permissions (enabled by default)
- Enable cookies

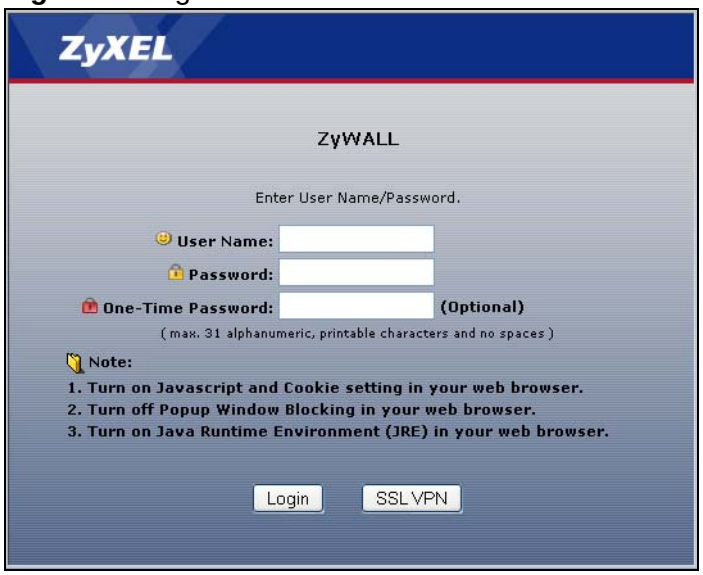
The recommended screen resolution is 1024 x 768 pixels.

## 3.2 Web Configurator Access

1 Make sure your ZyWALL hardware is properly connected. See the Quick Start Guide.

2 Open your web browser, and go to http://192.168.1.1. By default, the ZyWALL automatically routes this request to its HTTPS server, and it is recommended to keep this setting. The **Login** screen appears.

**Figure 9** Login Screen




3 Type the user name (default: “admin”) and password (default: “1234”).

If your account is configured to use an ASAS authentication server, use the OTP (One-Time Password) token to generate a number. Enter it in the **One-Time Password** field. The number is only good for one login. You must use the token to generate a new number the next time you log in.

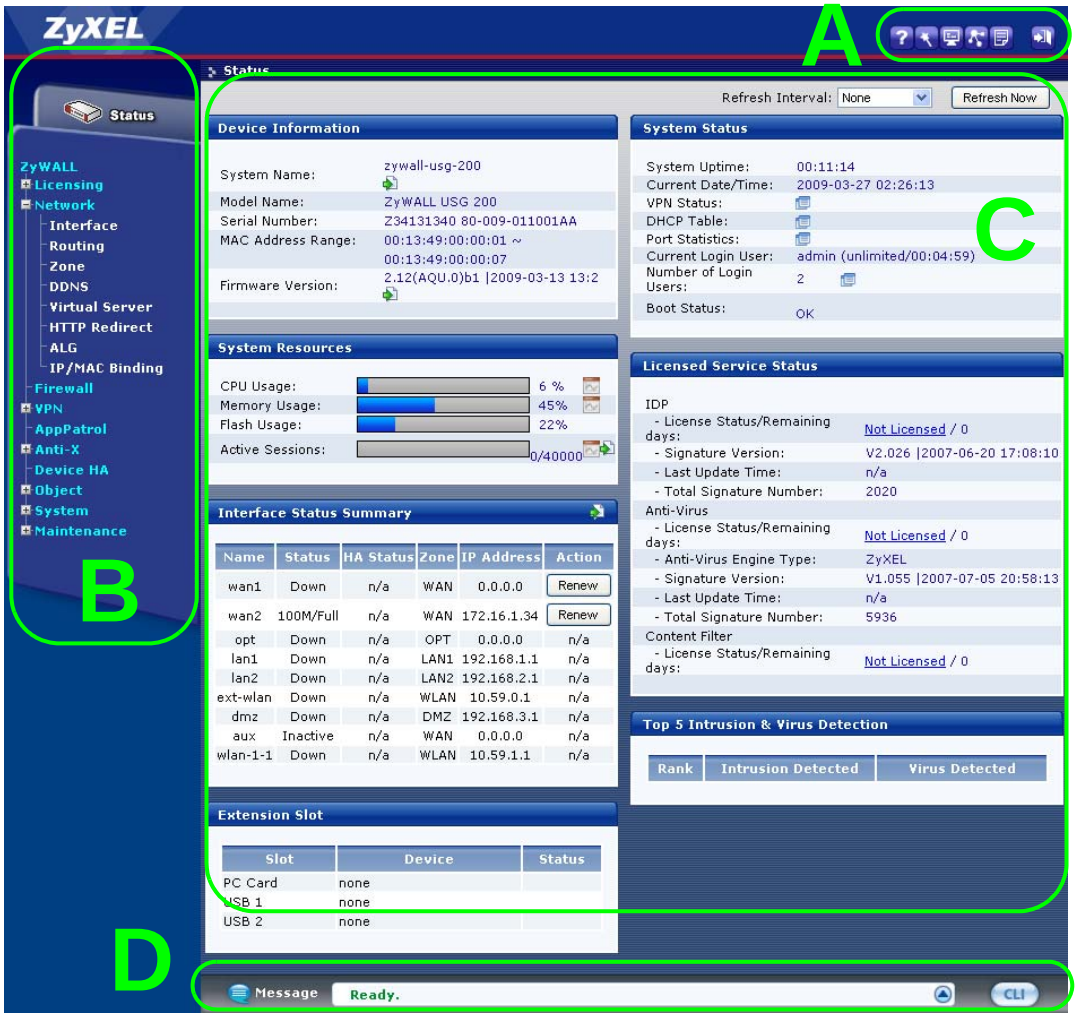
4 Click **Login**. If you logged in using the default user name and password, the **Update Admin Info** screen (Figure 10 on page 44) appears. Otherwise, the main screen (Figure 11 on page 45) appears.

**Figure 10** Update Admin Info Screen

5 The screen above appears every time you log in using the default user name and default password. If you change the password for the default user account, this screen does not appear anymore.

Follow the directions in this screen. If you change the default password, the **Login** screen (Figure 9 on page 44) appears after you click **Apply**. If you click **Ignore**, the main screen appears.

**Figure 11** Main Screen




# 3.3 Web Configurator Main Screen

As illustrated in Figure 11 on page 45, the main screen is divided into these parts:

- **A** - title bar
- **B** - navigation panel
- **C** - main window

- **D** - status bar

## 3.3.1 Title Bar

The title bar provides some icons in the upper right corner.

The icons provide the following functions.

**Table 5** Title Bar: Web Configurator Icons

| ICON | DESCRIPTION |
|---|---|
|  | **Help**: Click this icon to open the help page for the current screen. |
|  | **Wizards**: Click this icon to open one of the Web Configurator wizards. See Chapter 4 on page 55 for more information. |
|  | **Console**: Click this icon to open the console in which you can use the command line interface (CLI). |
|  | **Site Map**: Click this icon to display the site map for the Web Configurator. You can use the site map to go directly to any menu item or any tab in the Web Configurator. |
|  | **About**: Click this icon to display basic information about the ZyWALL. |
|  | **Logout**: Click this icon to log out of the Web Configurator. |

## 3.3.2 Navigation Panel

Use the menu items on the navigation panel to open screens to configure ZyWALL features. The following tables describe each menu item.

**Table 6** Navigation Panel Summary

| LINK | TAB | FUNCTION |
|---|---|---|
| Status | | Use this screen to look at the ZyWALL's general device information, system status, system resource usage, licensed service status, and interface status. |
| Licensing | | |
| Registration | Registration | Use this screen to register the device and activate trial services. |
| | Service | Use this screen to look at the licensed service status and to upgrade licensed services. |
| Update | Anti-Virus | Use this screen to schedule anti-virus signature updates and to update signature information immediately. |
| | IDP/AppPatrol | Use this screen to schedule IDP signature updates and to update signature information immediately. |
| | System Protect | Use this screen to schedule system-protect signature updates and to update signature information immediately. |
| Network | | |

**Table 6** Navigation Panel Summary (continued)

| LINK | TAB | FUNCTION |
|---|---|---|
| Interface | Status | Use this screen to see information about all of the ZyWALL's interfaces and their connection status. |
| | Port Role | Use this screen to set the ZyWALL's flexible ports as LAN1, WLAN, or DMZ. |
| | Ethernet | Use this screen to manage Ethernet interfaces and virtual Ethernet interfaces. |
| | PPP | Use this screen to create and manage PPPoE and PPTP interfaces. |
| | Cellular | Use this screen to configure settings for a cellular Internet connection through an installed 3G card. |
| | WLAN | Use this screen to configure settings for an installed wireless LAN card. |
| | VLAN | Use this screen to create and manage VLAN interfaces and virtual VLAN interfaces. |
| | Bridge | Use this screen to create and manage bridges and virtual bridge interfaces. |
| | Auxiliary | Use this screen to manage the **AUX** port. |
| | Trunk | Use this screen to create and manage trunks for load balancing and link HA. |
| Routing | Policy Route | Use this screen to create and manage routing policies. |
| | Static Route | Use this screen to create and manage IP static routing information. |
| | RIP | Use this screen to configure device-level RIP settings. |
| | OSPF | Use this screen to configure device-level OSPF settings, including areas and virtual links. |
| Zone | | Use this screen to configure zones used to define various policies. |
| DDNS | Profile | Use this screen to define and manage the ZyWALL's DDNS domain names. |
| | Status | Use this screen to view the status of the ZyWALL's DDNS domain names. |
| Virtual Server | | Use this screen to set up and manage port forwarding rules. |
| HTTP Redirect | | Use this screen to set up and manage HTTP redirection rules. |
| ALG | | Use this screen to configure SIP, H.323, and FTP pass-through settings. |
| IP/MAC Binding | Summary | Use this screen to configure IP to MAC address bindings for devices connected to each supported interface. |
| | Exempt List | Use this screen to configure ranges of IP addresses to which the ZyWALL does not apply IP/MAC binding. |
| | Monitor | Use this screen to display the devices that have received an IP address from ZyWALL interfaces with IP/MAC binding enabled. |
| Firewall | Firewall | Use this screen to create and manage level-3 traffic rules. |
| | Session Limit | Use this screen to limit the number of concurrent NAT/firewall sessions a client can use. |
| VPN | | |

**Table 6** Navigation Panel Summary (continued)

| LINK | TAB | FUNCTION |
|---|---|---|
| IPSec VPN | VPN Connection | Use this screen to configure IPSec tunnels. |
| | VPN Gateway | Use this screen to configure IKE tunnels. |
| | Concentrator | Use this screen to configure VPN concentrators (hub-and-spoke VPN). |
| | SA Monitor | Use this screen to monitor current IPSec VPN tunnels. |
| SSL VPN | Access Privilege | Use this screen to configure SSL VPN access rights for users and groups. |
| | Connection Monitor | Use this screen to monitor current SSL VPN connection. |
| | Global Setting | Use this screen to configure the ZyWALL's SSL VPN settings that apply to all connections. |
| L2TP VPN | L2TP Over IPSec | Use this screen to configure L2TP Over IPSec VPN settings. |
| | Session Monitor | Use this screen to monitor current L2TP Over IPSec VPN sessions. |
| AppPatrol | General | Use this screen to enable or disable traffic management by application and see registration and signature information. |
| | Common | Use this screen to manage traffic of the most commonly used web, file transfer and e-mail protocols. |
| | Instant Messenger | Use this screen to manage instant messenger traffic. |
| | Peer to Peer | Use this screen to manage peer-to-peer traffic. |
| | VoIP | Use this screen to manage VoIP traffic. |
| | Streaming | Use this screen to manage streaming traffic. |
| | Other | Use this screen to manage other kinds of traffic. |
| | Statistics | Use this screen to view bandwidth usage and traffic statistics for the protocols that the ZyWALL is managing. |
| Anti-X | | |
| Anti-Virus | General | Use this screen to turn anti-virus on or off, set up anti-virus policies and check the anti-virus engine type and the anti-virus license and signature status. |
| | Black/White List | Use this screen to set up anti-virus black (blocked) and white (allowed) lists of virus file patterns. |
| | Signature | Use these screens to search for signatures by signature name or attributes and configure how the ZyWALL uses them. |
| IDP | General | Use this screen to look at and manage IDP bindings. |
| | Profile | Use this screen to create and manage IDP profiles. |
| | Custom Signatures | Use this screen to create, import, or export custom signatures. |
| ADP | General | Use this screen to look at and manage ADP bindings. |
| | Profile | Use this screen to create and manage ADP profiles. |

**Table 6** Navigation Panel Summary (continued)

| LINK | TAB | FUNCTION |
|---|---|---|
| Content Filter | General | Use this screen to create and manage content filter policies. |
| | Filter Profile | Use this screen to create and manage the detailed filtering rules for content filtering policies. |
| | Cache | Use this screen to manage the URL cache in the ZyWALL. |
| Anti-Spam | General | Use these screens to turn anti-spam on or off and manage anti-spam policies. |
| | Black/White List | Use these screens to set up a black list to identify spam and a white list to identify legitimate e-mail. |
| | DNSBL | Use these screens to have the ZyWALL check e-mail against DNS Black Lists. |
| | Status | Use this screen to see how many mail sessions the ZyWALL is currently checking and DNSBL statistics. |
| Device HA | General | Use this to configure device HA global settings, and see the status of each interface monitored by device HA. |
| | Active-Passive Mode | Use these screens to configure (the new) active-passive mode device HA. |
| | Legacy Mode | Use these screens to use legacy mode device HA with other ZyWALLs that already have device HA setup using a firmware version earlier than 2.10. |
| Object | | |
| User/Group | User | Use this screen to create and manage users. |
| | Group | Use this screen to create and manage groups of users. |
| | Setting | Use this screen to manage default settings for all users, general settings for user sessions, and rules to force user authentication. |
| Address | Address | Use this screen to create and manage host, range, and network (subnet) addresses. |
| | Address Group | Use this screen to create and manage groups of addresses. |
| Service | Service | Use this screen to create and manage TCP and UDP services. |
| | Service Group | Use this screen to create and manage groups of services. |
| Schedule | | Use this screen to create one-time and recurring schedules. |
| AAA Server | Active Directory-Default | Use this screen to configure the default Active Directory settings. |
| | Active Directory-Group | Use this screen to create and manage groups of Active Directory servers. |
| | LDAP-Default | Use this screen to configure the default LDAP settings. |
| | LDAP-Group | Use this screen to create and manage groups of LDAP servers. |
| | RADIUS-Default | Use this screen to configure the default RADIUS settings. |
| | RADIUS-Group | Use this screen to create and manage groups of RADIUS servers. |
| Auth. Method | | Use these screens to create and manage ways of authenticating users. |

**Table 6** Navigation Panel Summary (continued)

| LINK | TAB | FUNCTION |
|---|---|---|
| Certificate | My Certificates | Use this screen to create and manage the ZyWALL's certificates. |
| | Trusted Certificates | Use this screen to import and manage certificates from trusted sources. |
| SSL Application | | Use these screens to create SSL web application or file sharing objects. |
| System | | |
| Host Name | | Use this screen to configure the system and domain name for the ZyWALL. |
| Date/Time | | Use this screen to configure the current date, time, and time zone in the ZyWALL. |
| Console Speed | | Use this screen to set the console speed. |
| DNS | | Use this screen to configure the DNS server and address records for the ZyWALL. |
| WWW | Service Control | Use this screen to configure HTTP, HTTPS, and general authentication. |
| | Login Page | Use this screen to configure how the login and access user screens look. |
| SSH | | Use this screen to configure the SSH server and SSH service settings for the ZyWALL. |
| TELNET | | Use this screen to configure the telnet server settings for the ZyWALL. |
| FTP | | Use this screen to configure the FTP server settings for the ZyWALL. |
| SNMP | | Use this screen to configure SNMP communities and services. |
| Dial-in Mgmt. | | Use this screen to configure settings for an out of band management connection through a modem connected to the **AUX** port. |
| Vantage CNM | | Use this screen to configure and allow your ZyWALL to be managed by the Vantage CNM server. |
| Language | | Use this screen to select the language of the ZyWALL's Web Configurator screens. |
| Maintenance | | |
| File Manager | Configuration File | Use this screen to manage and upload configuration files for the ZyWALL. |
| | Firmware Package | Use this screen to look at the current firmware version and to upload firmware. |
| | Shell Script | Use this screen to manage and run shell script files for the ZyWALL. |
| Log | View Log | Use this screen to look at log entries. |
| | Log Setting | Use this screen to configure the system log, e-mail logs, and remote syslog servers. |

**Table 6** Navigation Panel Summary (continued)

| LINK | TAB | FUNCTION |
|---|---|---|
| Report | Traffic Statistics | Use this screen to collect traffic information and display basic reports about it. |
| | Session Monitor | Use this screen to display the status of all current sessions. |
| | Anti-Virus | Use this screen to collect and display statistics on the viruses that the ZyWALL has detected. |
| | IDP | Use this screen to collect and display statistics on the intrusions that the ZyWALL has detected. |
| | Content Filter | Use this screen to collect and display content filter statistics |
| | Anti-Spam | Use this screen to start or stop data collection and view spam statistics. |
| | Email Daily Report | Use this screen to configure where and how to send daily reports and what reports to send. |
| Diagnostics | | Use this screen to have the ZyWALL collect diagnostic information. |
| Reboot | | Use this screen to restart the ZyWALL. |

## 3.3.3 Main Window

The main window shows the screen you select in the menu. It is discussed in the rest of this document.

Right after you log in, the **Status** screen is displayed. See Chapter 7 on page 149 for more information about the **Status** screen.

## 3.3.4 Message Bar

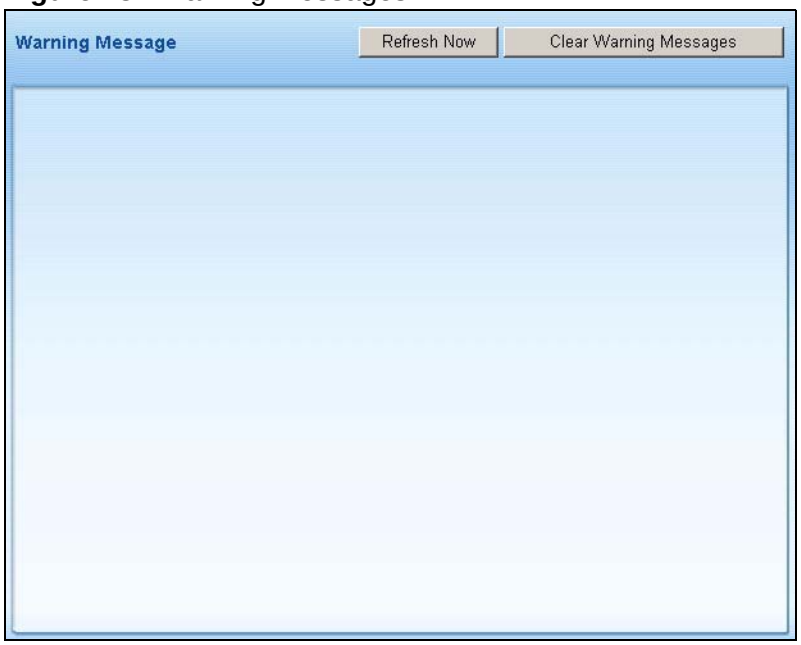
The message bar displays configuration status information. Check the message bar after you click **Apply** or **OK** to verify that the configuration has been updated.

**Figure 12** Message Bar

### 3.3.4.1 Warning Messages

Click the up arrow to view the ZyWALL's current warning messages. These warning messages display in a popup window, such as the following.

**Figure 13** Warning Messages



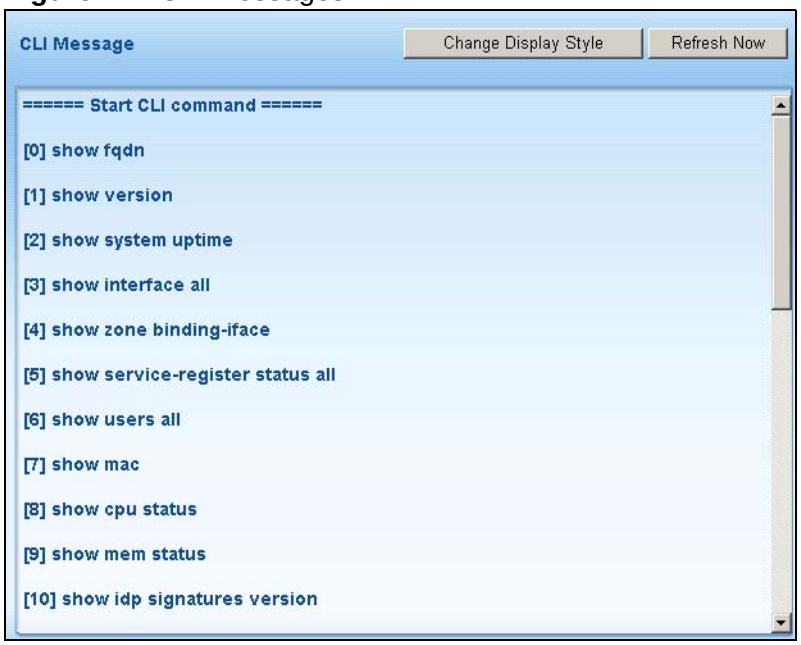

Click **Refresh Now** to update the screen. Close the popup window when you are done with it.

Click **Clear Warning Messages** to remove the current warning messages from the window.

### 3.3.4.2 CLI Messages

Click **CLI** to look at the CLI commands sent by the Web Configurator. These commands appear in a popup window, such as the following.

**Figure 14** CLI Messages




Click **Change Display Style** to show or hide the index numbers for the commands (the commands are more convenient to copy and paste without the index numbers).

Click **Refresh Now** to update the screen. For example, if you just enabled a particular feature, you can look at the commands the Web Configurator generated to enable it. Close the popup window when you are done with it.

See the Command Reference Guide for information about the commands.

# 4

# Wizard Setup

## 4.1 Wizard Setup Overview

The Web Configurator's setup wizards help you configure Internet and VPN connection settings. This chapter provides information on configuring the Wizard setup screens in the Web Configurator. See the feature-specific chapters in this User's Guide for background information.

Note: Use the installation wizards only for initial configuration starting from the default configuration.

Changes you make in an installation or VPN wizard may not be applied if you have already changed the ZyWALL's configuration. In the Web Configurator, click the **Wizard** icon  to open the **Wizard Setup Welcome** screen.

**Figure 15** Wizard Setup Welcome

- **INSTALLATION SETUP, ONE ISP**

  Click this link to open a wizard to set up a single Internet connection for Gigabit Ethernet **wan1**. See Section 4.2 on page 56.

- **INSTALLATION SETUP, TWO ISP**

  Click this link to open a wizard to set up Internet connections for Gigabit Ethernet interfaces **wan1** and **wan2**. See Section 4.4 on page 65. You can connect one interface to one ISP (or network) and connect the other to a second ISP (or network). You can use the second WAN connection for load balancing to increase overall network throughput or as a backup to enhance network reliability. This wizard also configures a WAN trunk. See Chapter 11 on page 263 for more on load balancing and trunks.

- **VPN SETUP**

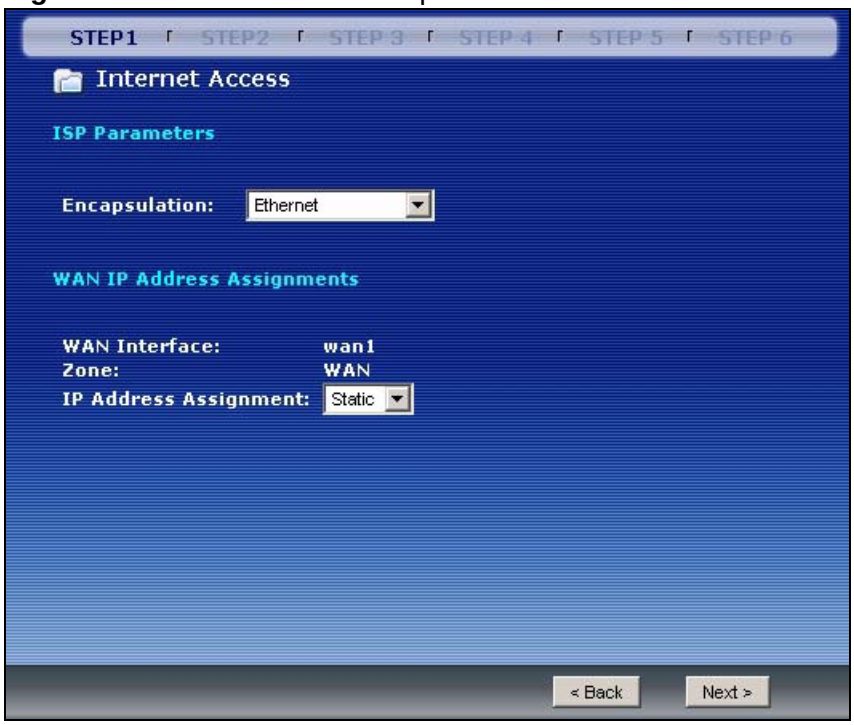
  Use **VPN SETUP** to configure a VPN connection. See Section 4.5 on page 67.

# 4.2 Installation Setup, One ISP

The wizard screens vary depending on what encapsulation type you use. Refer to information provided by your ISP to know what to enter in each field. Leave a field blank if you don't have that information.

Note: Enter the Internet access information exactly as your ISP gave it to you.

**Figure 16** Internet Access: Step 1



The following table describes the labels in this screen.

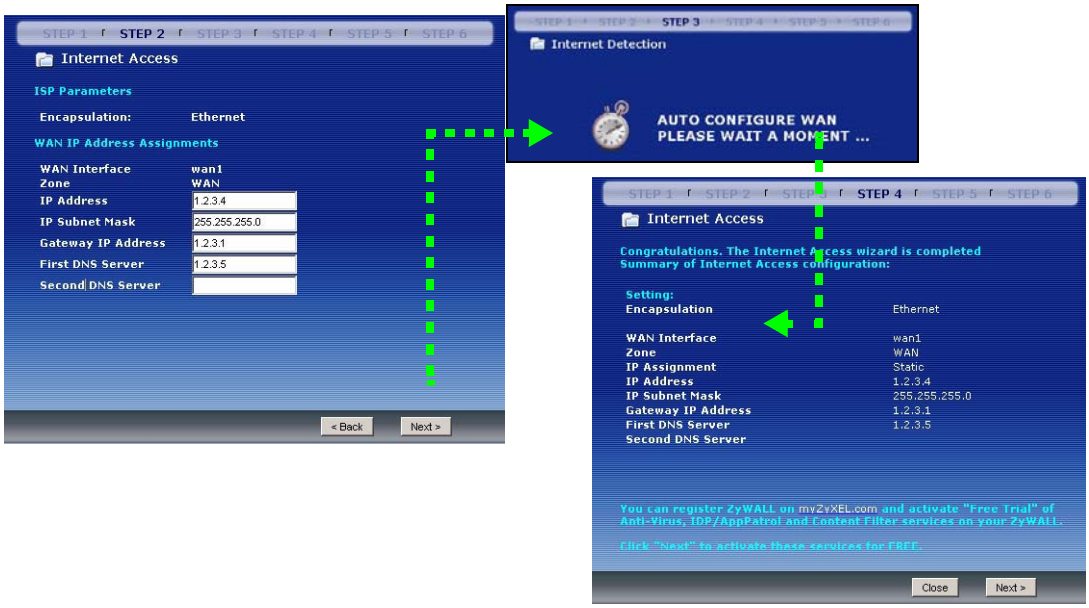
**Table 7** Internet Access: Step 1

| LABEL | DESCRIPTION |
|---|---|
| ISP Parameters | |
| Encapsulation | Choose the **Ethernet** option when the WAN port is used as a regular Ethernet.<br><br>Otherwise, choose **PPPoE** or **PPTP** for a dial-up connection according to the information from your ISP. |
| WAN IP Address Assignments | |
| WAN Interface | This is the interface you are configuring for Internet access. |
| Zone | This is the security zone to which this interface and Internet connection belong. |
| IP Address Assignment | Select **Auto** If your ISP did not assign you a fixed IP address.<br><br>Select **Static** If the ISP assigned a fixed IP address. |
| Back | Click **Back** to return to the previous screen. |
| Next | Click **Next** to continue. |

## 4.2.1 Internet Access: Ethernet Encapsulation

Configure your IP address settings and click **Next** to apply the configuration settings. This configures the ZyWALL to access the Internet.

**Figure 17** Internet Access: Ethernet Encapsulation



The following table describes the labels in this screen. This screen is read-only if you set the **IP Address Assignment** to **Static**.

**Table 8** Internet Access: Ethernet Encapsulation

| LABEL | DESCRIPTION |
|---|---|
| ISP Parameters | |
| Encapsulation | This displays the type of Internet connection you are configuring. |
| WAN IP Address Assignments | |
| WAN Interface | This displays the identity of the interface you configure to connect with your ISP. |
| Zone | This field displays to which security zone this interface and Internet connection will belong. |
| IP Address | Enter the IP address that your ISP gave you. This should be a static, public IP address. |
| IP Subnet Mask | Enter the subnet mask for the IP address. |
| Gateway IP Address | Enter the IP address of the router through which this WAN connection will send traffic (the default gateway). |
| First DNS Server<br><br>Second DNS Server | DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The ZyWALL uses a system DNS server (in the order you specify here) to resolve domain names for VPN, DDNS and the time server.<br><br>Enter the DNS server IP addresses. |
| Back | Click **Back** to return to the previous screen. |
| Next | Click **Next** to continue. |

## 4.2.2 Internet Access: PPPoE Encapsulation

Configure your PPPoE and IP address settings and click **Next** to apply the configuration settings. This configures the ZyWALL to access the Internet.

**Figure 18** Internet Access: PPPoE Encapsulation


The following table describes the labels in this screen.

**Table 9** Internet Access: PPPoE Encapsulation

| LABEL | DESCRIPTION |
|---|---|
| ISP Parameters | |
| Encapsulation | This displays the type of Internet connection you are configuring. |
| Service Name | Type the PPPoE service name given to you by your ISP. PPPoE uses a service name to identify and reach the PPPoE server. You can use alphanumeric and -_@$./ characters, and it can be up to 64 characters long. |

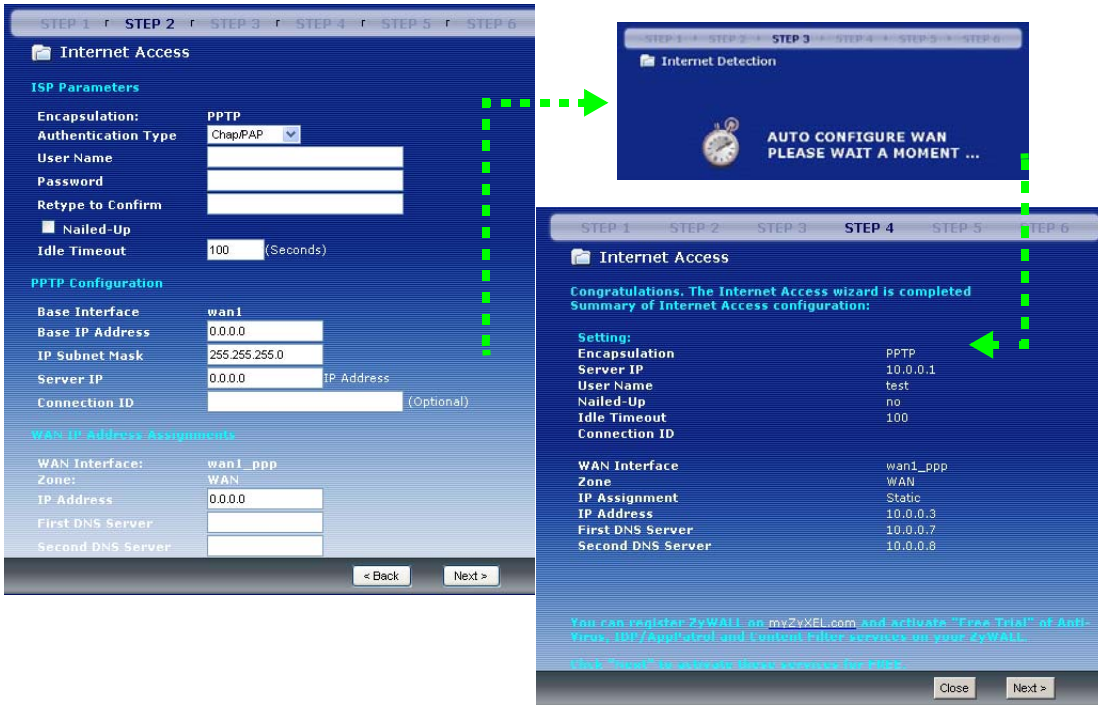
**Table 9** Internet Access: PPPoE Encapsulation (continued)

| LABEL | DESCRIPTION |
|---|---|
| Authentication Type | Use the drop-down list box to select an authentication protocol for outgoing calls. Options are:<br>**CHAP/PAP** - Your ZyWALL accepts either CHAP or PAP when requested by this remote node.<br>**CHAP** - Your ZyWALL accepts CHAP only.<br>**PAP** - Your ZyWALL accepts PAP only.<br>**MSCHAP** - Your ZyWALL accepts MSCHAP only.<br>**MSCHAP-V2** - Your ZyWALL accepts MSCHAP-V2 only. |
| User Name | Type the user name given to you by your ISP. You can use alphanumeric and -_@$./ characters, and it can be up to 31 characters long. |
| Password | Type the password associated with the user name above. Use up to 64 ASCII characters except the [] and ?. This field can be blank. |
| Retype to Confirm | Type your password again for confirmation. |
| Nailed-Up | Select **Nailed-Up** if you do not want the connection to time out. |
| Idle Timeout | Type the time in seconds that elapses before the router automatically disconnects from the PPPoE server. The default time is **100** seconds. |
| WAN IP Address Assignments | These fields are read-only if you selected **Auto** as the **IP Address Assignment** in the previous screen. |
| WAN Interface | This displays the identity of the interface you configure to connect with your ISP. |
| Zone | This field displays to which security zone this interface and Internet connection will belong. |
| IP Address | Enter your WAN IP address in this field. |
| First DNS Server<br>Second DNS Server | These fields displayd if you selected static IP address assignment. DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The ZyWALL uses a system DNS server (in the order you specify here) to resolve domain names for VPN, DDNS and the time server.<br>Enter the DNS server's IP address(es) in the field(s) to the right.<br>Leave the field as **0.0.0.0** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it. |
| Back | Click **Back** to return to the previous screen. |
| Next | Click **Next** to continue. |

## 4.2.3 Internet Access: PPTP Encapsulation

Configure your PPTP and IP address settings and click **Next** to apply the configuration settings. This configures the ZyWALL to access the Internet.

**Figure 19** Internet Access: PPTP Encapsulation




The following table describes the labels in this screen.

**Table 10** Internet Access: PPTP Encapsulation

| LABEL | DESCRIPTION |
|---|---|
| ISP Parameters | |
| Encapsulation | This displays the type of Internet connection you are configuring. |
| Authentication Type | Use the drop-down list box to select an authentication protocol for outgoing calls. Options are:<br>**CHAP/PAP** - Your ZyWALL accepts either CHAP or PAP when requested by this remote node.<br>**CHAP** - Your ZyWALL accepts CHAP only.<br>**PAP** - Your ZyWALL accepts PAP only.<br>**MSCHAP** - Your ZyWALL accepts MSCHAP only.<br>**MSCHAP-V2** - Your ZyWALL accepts MSCHAP-V2 only. |
| User Name | Type the user name given to you by your ISP. You can use alphanumeric and -_@$./ characters, and it can be up to 31 characters long. |
| Password | Type the password associated with the user name above. Use up to 64 ASCII characters except the [] and ?. This field can be blank. |

**Table 10** Internet Access: PPTP Encapsulation (continued)

| LABEL | DESCRIPTION |
|---|---|
| Retype to Confirm | Type your password again for confirmation. |
| Nailed-Up | Select **Nailed-Up** if you do not want the connection to time out. |
| Idle Timeout | Type the time in seconds that elapses before the router automatically disconnects from the PPTP server. |
| PPTP Configuration | |
| Base Interface | This displays the identity of the Ethernet interface you configure to connect with a modem or router. |
| Base IP Address | Type the (static) IP address assigned to you by your ISP. |
| IP Subnet Mask | Type the subnet mask assigned to you by your ISP (if given). |
| Server IP | Type the IP address of the PPTP server. |
| Connection ID | Enter the connection ID or connection name in this field. It must follow the "c:id" and "n:name" format. For example, C:12 or N:My ISP. This field is optional and depends on the requirements of your DSL modem.<br><br>You can use alphanumeric and -_: characters, and it can be up to 31 characters long. |
| WAN IP Address Assignments | These fields are read-only if you selected **Auto** as the **IP Address Assignment** in the previous screen. |
| WAN Interface | This displays the identity of the interface you configure to connect with your ISP. |
| Zone | This field displays to which security zone this interface and Internet connection will belong. |
| IP Address | Enter your WAN IP address in this field. |
| First DNS Server<br><br>Second DNS Server | These fields displayd if you selected static IP address assignment. DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The ZyWALL uses a system DNS server (in the order you specify here) to resolve domain names for VPN, DDNS and the time server.<br><br>Enter the DNS server's IP address(es) in the field(s) to the right.<br><br>Leave the field as **0.0.0.0** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it. |
| Back | Click **Back** to return to the previous screen. |
| Next | Click **Next** to continue. |

## 4.2.4 Internet Access - Finish

You have set up your ZyWALL to access the Internet.

Note: If you have not already done so, you can register your ZyWALL with myZyXEL.com and activate trials of services like IDP.

You can click **Next** and use the following screen to perform a basic registration (see Section 4.3 on page 63). If you want to do a more detailed registration or manage your account details, click **myZyXEL.com**.

Alternatively, click **Close** to exit the wizard.

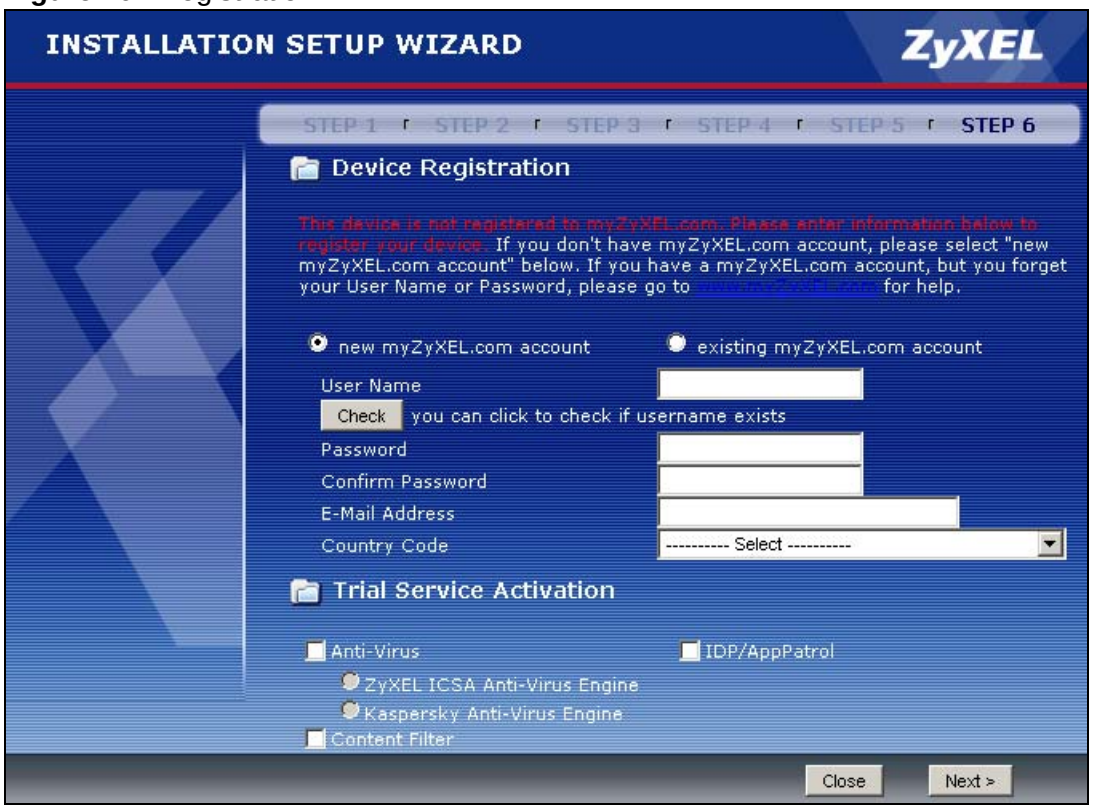
# 4.3 Device Registration

Use this screen to register your ZyWALL with myZXEL.com and activate trial periods of subscription security features if you have not already done so.

Note: You must be connected to the Internet to register.

This screen displays a read-only user name and password if the ZyWALL is already registered. It also shows which trial services are activated (if any). You can still select the unchecked trial service(s) to activate it after registration. Use the **Registration > Service** screen to update your service subscription status.

**Figure 20** Registration

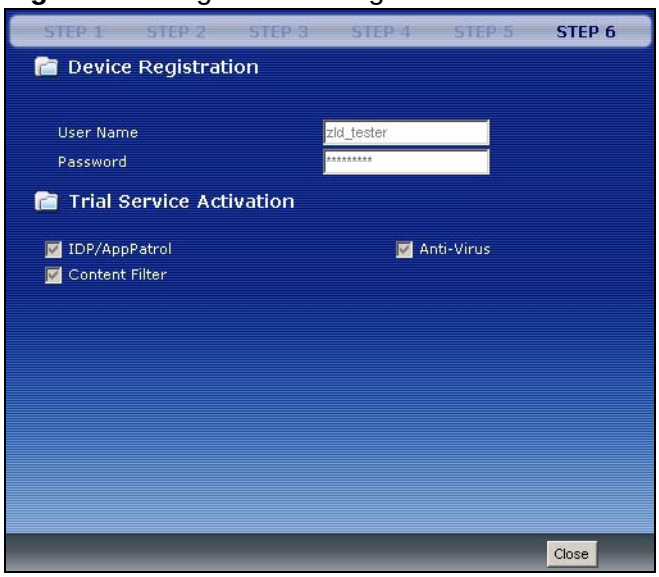


The following table describes the labels in this screen.

**Table 11** Registration

| LABEL | DESCRIPTION |
|---|---|
| Device Registration | If you select **existing myZyXEL.com account**, only the **User Name** and **Password** fields are available. |
| new myZyXEL.com account | If you haven't created an account at myZyXEL.com, select this option and configure the following fields to create an account and register your ZyWALL. |
| existing myZyXEL.com account | If you already have an account at myZyXEL.com, select this option and enter your user name and password in the fields below to register your ZyWALL. |
| UserName | Enter a user name for your myZyXEL.com account. The name should be from six to 20 alphanumeric characters (and the underscore). Spaces are not allowed. |
| Check | Click this button to check with the myZyXEL.com database to verify the user name you entered has not been used. |
| Password | Enter a password of between six and 20 alphanumeric characters (and the underscore). Spaces are not allowed. |
| Confirm Password | Enter the password again for confirmation. |
| E-Mail Address | Enter your e-mail address. You can use up to 80 alphanumeric characters (periods and the underscore are also allowed) without spaces. |
| Country Code | Select your country from the drop-down box list. |
| Trial Service Activation | You can try a trial service subscription. After the trial expires, you can buy an iCard and enter the license key in the **Registration Service** screen to extend the service. |
| IDP/AppPatrol<br>Anti-Virus<br>Content Filter | Select the check box to activate a trial. The trial period starts the day you activate the trial. |
| Close | Click **Close** to exit the wizard. |
| Next | Click **Next** to save your changes back to the ZyWALL and activate the selected services. |

**Figure 21** Registration: Registered Device

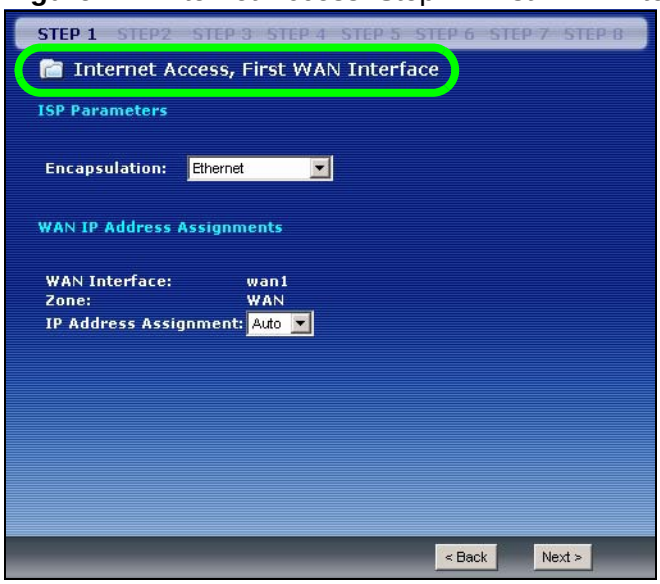



# 4.4 Installation Setup, Two Internet Service Providers

This wizard allows you to configure two interfaces for Internet access through either two different Internet Service Providers (ISPs) or two different accounts with the same ISP.

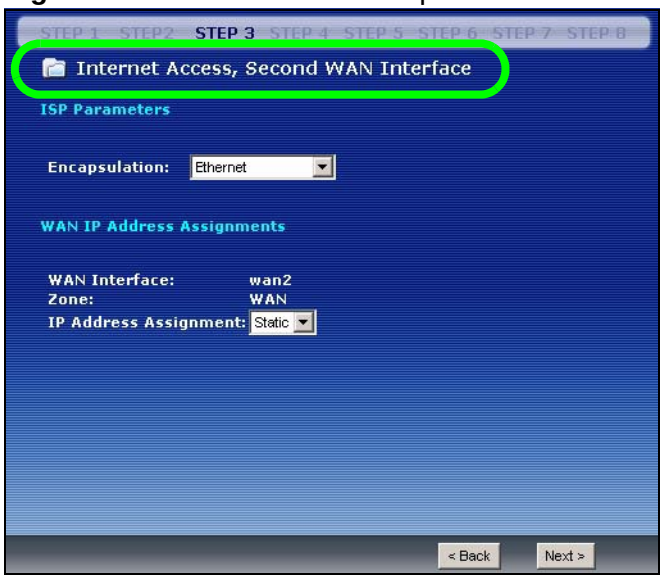
The configuration of the following screens is explained in Section 4.2 on page 56 section. Configure the **First WAN Interface** and click **Next**.

**Figure 22** Internet Access: Step 1: First WAN Interface



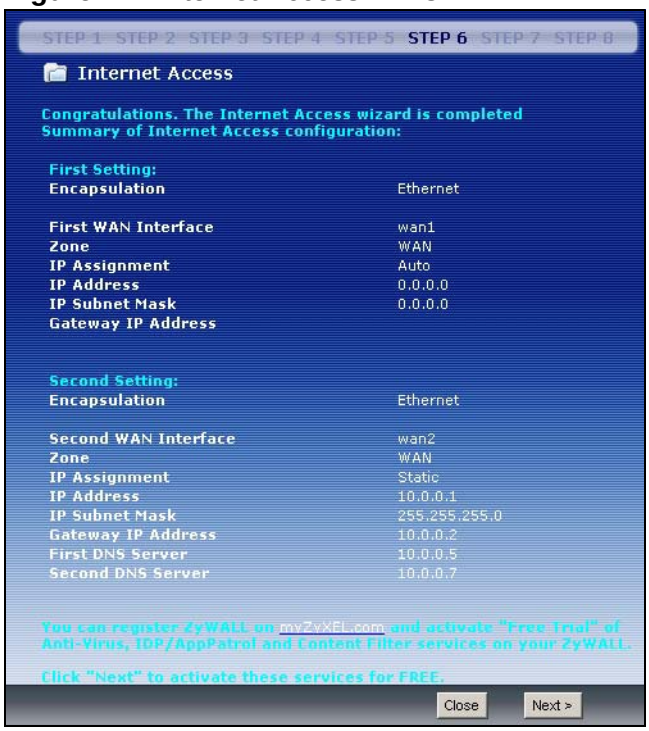
After you configure the **First WAN Interface**, you can configure the **Second WAN Interface**. Click **Next** to continue.

**Figure 23** Internet Access: Step 3: Second WAN Interface




After you configure the **Second WAN Interface**, a summary of configuration settings display for both WAN interfaces.

**Figure 24** Internet Access: Finish




Note: You can register your ZyWALL with myZyXEL.com and activate trials of services like IDP.

Use the myZyXEL.com link if you do already have a myZyXEL.com account. If you already have a myZyXEL.com account, you can click **Next** and use the following screen to register your ZyWALL and activate service trials (see Section 4.3 on page 63).

Alternatively, click **Close** to exit the wizard.

### 4.4.1 Internet Access Wizard Setup Complete

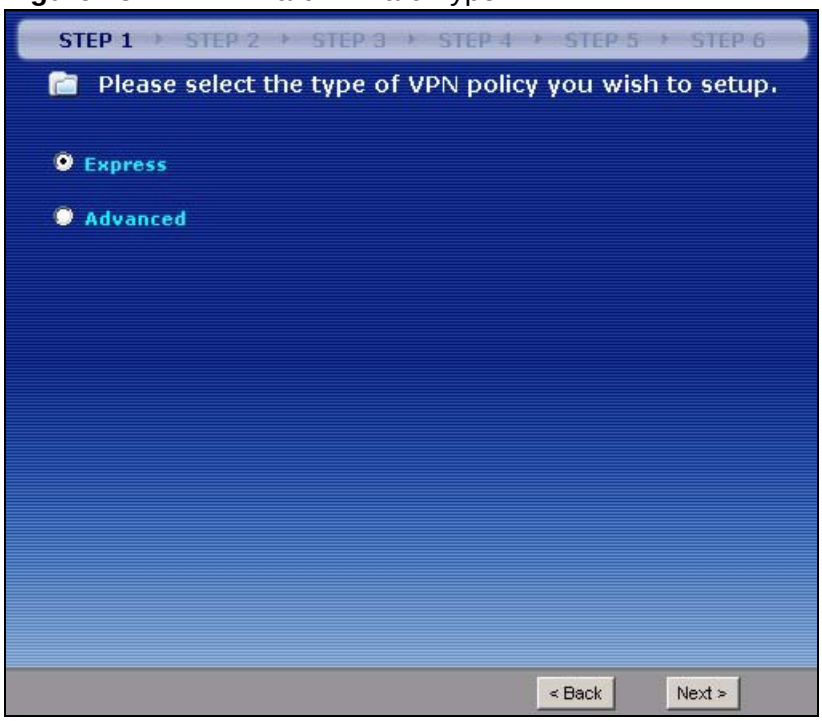
Well done! You have successfully set up your ZyWALL to access the Internet.

## 4.5 VPN Setup

The VPN wizard creates corresponding VPN connection and VPN gateway settings, a policy route and address objects that you can use later in configuring more VPN connections or other features.

Click **VPN SETUP** in the **Wizard Setup Welcome** screen (Figure 15 on page 55) to open the following screen. Use it to select which type of VPN settings you want to configure.

**Figure 25** VPN Wizard: Wizard Type



The following table describes the labels in this screen.

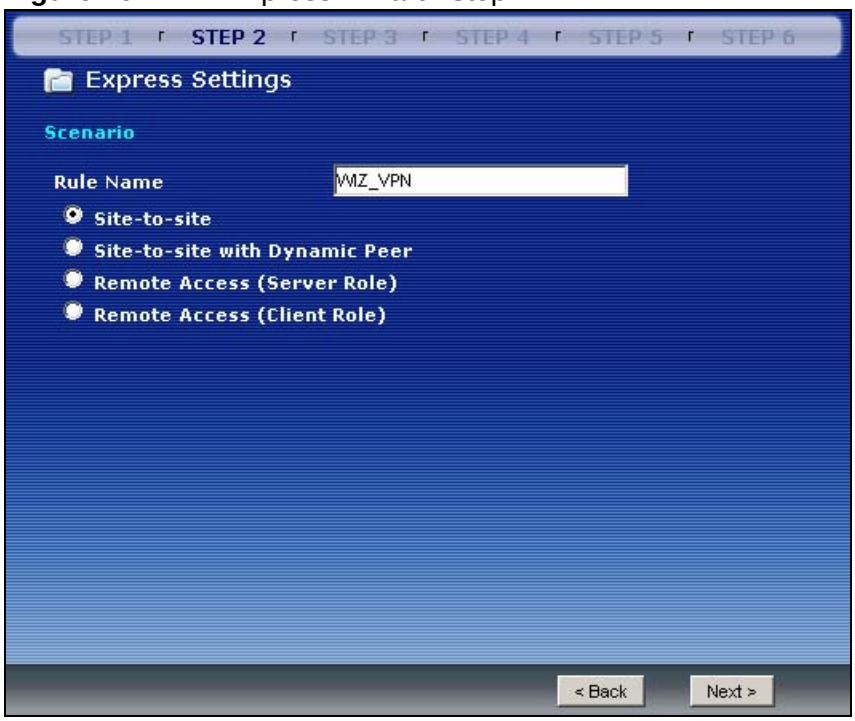
**Table 12** VPN Wizard: Step 1: Wizard Type

| LABEL | DESCRIPTION |
|---|---|
| Express | Use this wizard to create a VPN connection with another ZLD-based ZyWALL using a pre-shared key and default security settings. |
| Advanced | Use this wizard to configure detailed VPN security settings such as using certificates. The VPN connection can be to another ZLD-based ZyWALL or other IPSec device. |
| Back | Click **Back** to return to the previous screen. |
| Next | Click **Next** to continue. |

## 4.5.1 VPN Express Wizard

Click the **Express** radio button as shown in Figure 25 on page 67 to display the following screen.

**Figure 26** VPN Express Wizard: Step 2

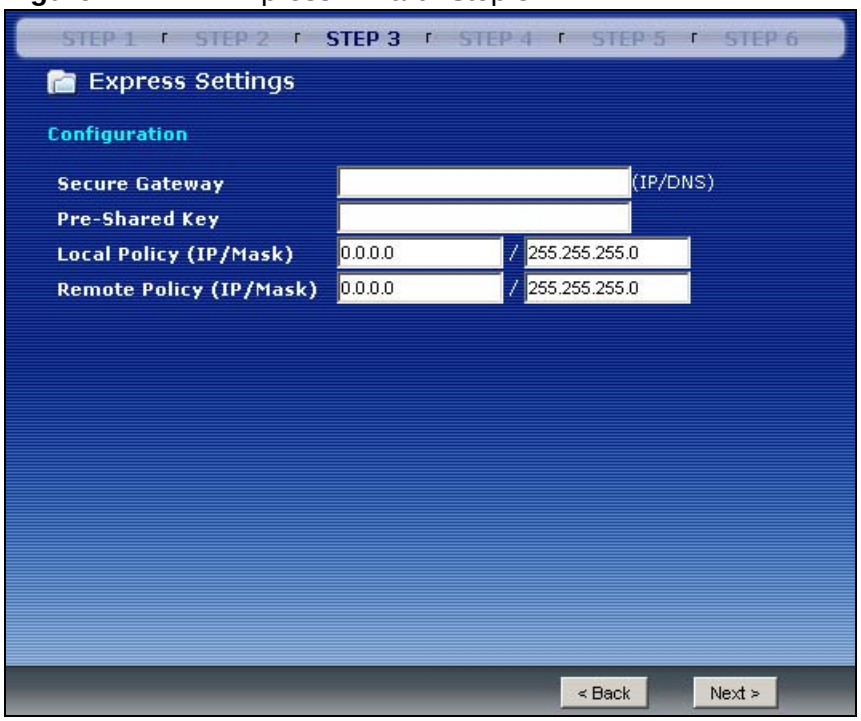


The following table describes the labels in this screen.

**Table 13** VPN Express Wizard: Step 2

| LABEL | DESCRIPTION |
|---|---|
| Rule Name | Type the name used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| Site-to-site | Choose this if the remote IPSec router has a static IP address or a domain name. This ZyWALL can initiate the VPN tunnel. |
| Site-to-site with Dynamic Peer | Choose this if the remote IPSec router has a dynamic IP address. Only the remote IPSec router can initiate the VPN tunnel. |
| Remote Access (Server Role) | Choose this to allow incoming connections from IPSec VPN clients. The clients have dynamic IP addresses and are also known as dial-in users. Only the clients can initiate the VPN tunnel. |
| Remote Access (Client Role) | Choose this to connect to an IPSec server. This ZyWALL is the client (dial-in user) and can initiate the VPN tunnel. |
| Back | Click **Back** to return to the previous screen. |
| Next | Click **Next** to continue. |

**Figure 27** VPN Express Wizard: Step 3

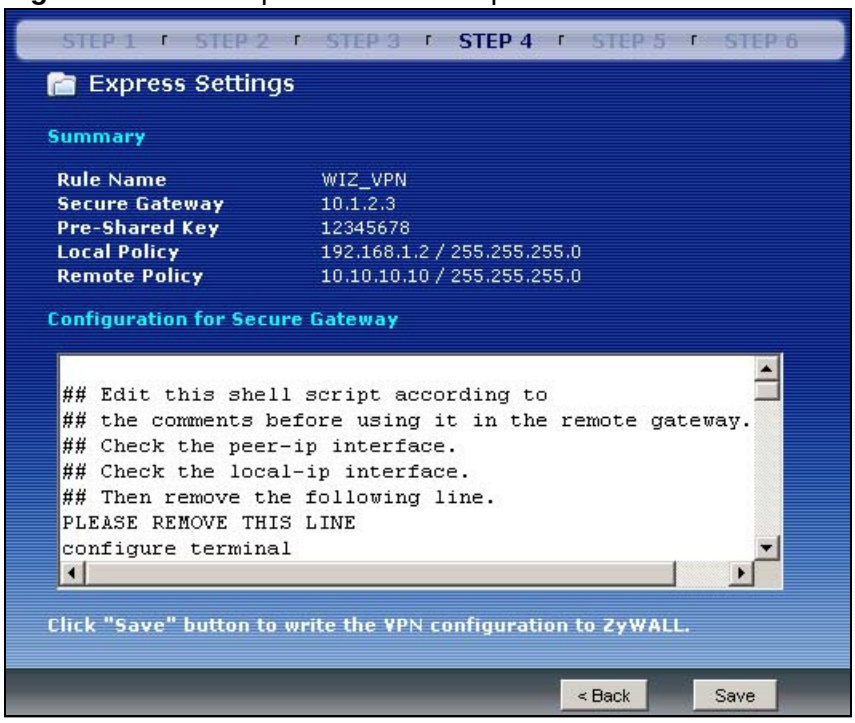


The following table describes the labels in this screen.

**Table 14** VPN Express Wizard: Step 3

| LABEL | DESCRIPTION |
|---|---|
| Secure Gateway | If **Any** displays in this field, it is not configurable for the chosen scenario.<br>If this field is configurable, enter the WAN IP address or domain name of the remote IPSec router (secure gateway) to identify the remote IPSec router by its IP address or a domain name. |
| Pre-Shared Key | Type your pre-shared key in this field. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection.<br>Type from 8 to 31 case-sensitive ASCII characters or 8 to 31 pairs of hexadecimal ("0-9", "A-F") characters. Precede a hexadecimal key with “0x”.<br>Both ends of the VPN tunnel must use the same pre-shared key. You will receive a PYLD_MALFORMED (payload malformed) packet if the same pre-shared key is not used on both ends. |
| Local Policy (IP/Mask) | Type a static local IP address that corresponds to the remote IPSec router's configured remote IP address (the remote IP address of the other ZyWALL).<br>To specify IP addresses on a network by their subnet mask, type the subnet mask of the LAN behind your ZyWALL. |
| Remote Policy (IP/ Mask) | If **Any** displays in this field, it is not configurable for the chosen scenario.<br>If this field is configurable, type a static local IP address that corresponds to the remote IPSec router's configured local IP address (the local IP address of the other ZyWALL).<br>To specify IP addresses on a network by their subnet mask, type the subnet mask of the LAN behind the remote gateway. |
| Back | Click **Back** to return to the previous screen. |
| Next | Click **Next** to continue. |

**Figure 28** VPN Express Wizard: Step 4




The following table describes the labels in this screen.

**Table 15** VPN Express Wizard: Step 4

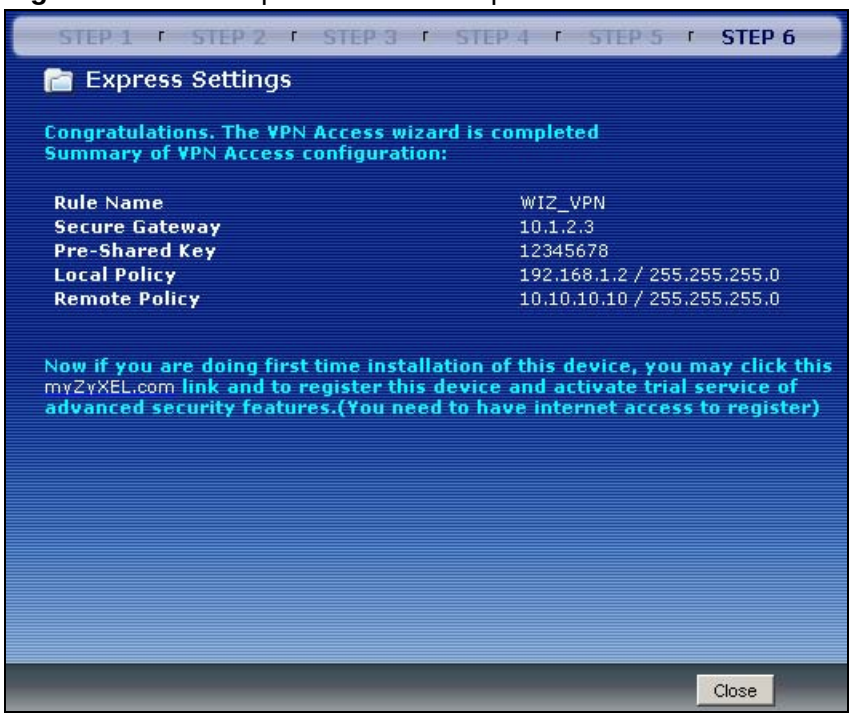
| LABEL | DESCRIPTION |
|---|---|
| Summary | |
| Rule Name | This is the name of the VPN connection (and VPN gateway). |
| Secure Gateway | This is the WAN IP address or domain name of the remote IPSec router. If this field displays **Any**, only the remote IPSec router can initiate the VPN connection. |
| Pre-Shared Key | This is a pre-shared key identifying a communicating party during a phase 1 IKE negotiation. |
| Local Policy | This is a (static) IP address and Subnet Mask on the LAN behind your ZyWALL. |
| Remote Policy | This is a (static) IP address and Subnet Mask on the network behind the remote IPSec router. If this field displays **Any**, only the remote IPSec router can initiate the VPN connection. |
| Configuration for Secure Gateway | These commands set the matching VPN connection settings for the remote gateway. If the remote gateway is a ZLD-based ZyWALL, you can copy and paste this list into its command line interface in order to configure it for the VPN tunnel.<br>You can also use a text editor to save these commands as a shell script file with a ".zysh" filename extension. Then you can use the file manager to run the script in order to configure the VPN connection.<br>See the commands reference guide for details on the commands displayed in this list. |

**Table 15** VPN Express Wizard: Step 4 (continued)

| LABEL | DESCRIPTION |
|---|---|
| Back | Click **Back** to return to the previous screen. |
| Save | Click **Save** to store the VPN settings on your ZyWALL. |

Now you can use the VPN tunnel.

**Figure 29** VPN Express Wizard: Step 6



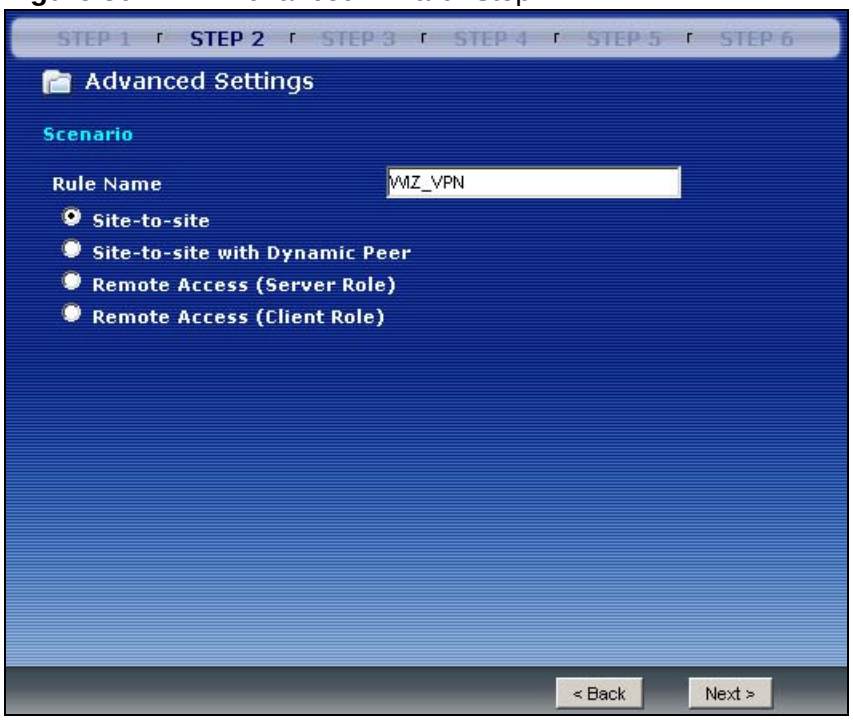

Note: If you have not already done so, use the myZyXEL.com link and register your ZyWALL with myZyXEL.com and activate trials of services like IDP.

Click **Close** to exit the wizard.

## 4.5.2 VPN Advanced Wizard

Click the **Advanced** radio button as shown in Figure 25 on page 67 to display the following screen.

**Figure 30** VPN Advanced Wizard: Step 2



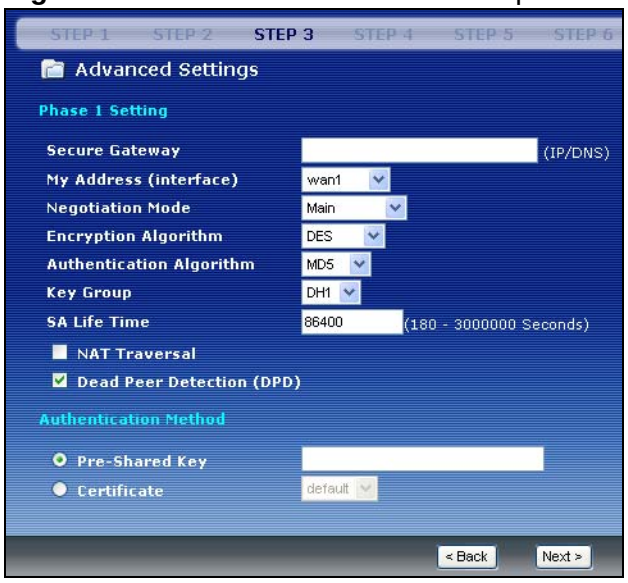

The following table describes the labels in this screen.

**Table 16** VPN Advanced Wizard: Step 2

| LABEL | DESCRIPTION |
|---|---|
| Rule Name | Type the name used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| Site-to-site | Choose this if the remote IPSec router has a static IP address or a domain name. This ZyWALL can initiate the VPN tunnel. |
| Site-to-site with Dynamic Peer | Choose this if the remote IPSec router has a dynamic IP address. Only the remote IPSec router can initiate the VPN tunnel. |
| Remote Access (Server Role) | Choose this to allow incoming connections from IPSec VPN clients. The clients have dynamic IP addresses and are also known as dial-in users. Only the clients can initiate the VPN tunnel. |
| Remote Access (Client Role) | Choose this to connect to an IPSec server. This ZyWALL is the client (dial-in user) and can initiate the VPN tunnel. |
| Back | Click **Back** to return to the previous screen. |
| Next | Click **Next** to continue. |

There are two phases to every IKE (Internet Key Exchange) negotiation – phase 1 (Authentication) and phase 2 (Key Exchange). A phase 1 exchange establishes an IKE SA (Security Association).

**Figure 31** VPN Advanced Wizard: Step 3




The following table describes the labels in this screen.

**Table 17** VPN Advanced Wizard: Step 3

| LABEL | DESCRIPTION |
|---|---|
| Phase 1 Setting | |
| Secure Gateway | If **Any** displays in this field, it is not configurable for the chosen scenario.<br><br>If this field is configurable, enter the WAN IP address or domain name of the remote IPSec router (secure gateway) in the field below to identify the remote IPSec router by its IP address or a domain name. Set this field to **0.0.0.0** if the remote IPSec router has a dynamic WAN IP address. |
| My Address (interface) | Select an interface from the drop-down list box to use on your ZyWALL. |
| Negotiation Mode | Select **Main** for identity protection. Select **Aggressive** to allow more incoming connections from dynamic IP addresses to use separate passwords.<br><br>Note: Multiple SAs (security associations) connecting through a secure gateway must have the same negotiation mode. |

**Table 17** VPN Advanced Wizard: Step 3 (continued)

| LABEL | DESCRIPTION |
|---|---|
| Encryption Algorithm | When **DES** is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The **DES** encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on **DES** that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. **AES128** uses a 128-bit key and is faster than **3DES**. **AES192** uses a 192-bit key and **AES256** uses a 256-bit key. Select **Null** to have no encryption. |
| Authentication Algorithm | **MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slower. Select **MD5** for minimal security and **SHA1** for maximum security. |
| Key Group | You must choose a key group for phase 1 IKE setup. **DH1** (default) refers to Diffie-Hellman Group 1 a 768 bit random number. **DH2** refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number. **DH5** refers to Diffie-Hellman Group 5 a 1536 bit random number. |
| SA Life Time (Seconds) | Define the length of time before an IKE SA automatically renegotiates in this field. The minimum value is 60 seconds.<br><br>A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected. |
| NAT Traversal | Select this check box to enable NAT traversal. NAT traversal allows you to set up a VPN connection when there are NAT routers between the two IPSec routers.<br><br>Note: The remote IPSec router must also have NAT traversal enabled. See Section on page 397 for more information. |
| Dead Peer Detection (DPD) | Select this check box if you want the ZyWALL to make sure the remote IPSec router is there before it transmits data through the IKE SA. If there has been no traffic for at least 15 seconds, the ZyWALL sends a message to the remote IPSec server. If the remote IPSec server responds, the ZyWALL transmits the data. If the remote IPSec server does not respond, the ZyWALL shuts down the IKE SA. |
| Authentication Method | |
| Pre-Shared Key | Type your pre-shared key in this field. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection.<br><br>Type from 8 to 31 case-sensitive ASCII characters or 8 to 31 pairs of hexadecimal ("0-9", "A-F") characters. Precede a hexadecimal key with “0x”.<br><br>Both ends of the VPN tunnel must use the same pre-shared key. You will receive a PYLD_MALFORMED (payload malformed) packet if the same pre-shared key is not used on both ends. |

**Table 17** VPN Advanced Wizard: Step 3 (continued)

| LABEL | DESCRIPTION |
|---|---|
| Certificate | Use the drop-down list box to select the certificate to use for this VPN tunnel. You must have certificates already configured in the **My Certificates** screen. Click **Certificate** under the **Object** menu to go to the **My Certificates** screen where you can view the ZyWALL's list of certificates. |
| Back | Click **Back** to return to the previous screen. |
| Next | Click **Next** to continue. |

Phase 2 in an IKE uses the SA that was established in phase 1 to negotiate SAs for IPSec.

**Figure 32** VPN Advanced Wizard: Step 4


The following table describes the labels in this screen.

**Table 18** VPN Advanced Wizard: Step 4

| LABEL | DESCRIPTION |
|---|---|
| Phase 2 Setting | |
| Active Protocol | Select the security protocols used for an SA.<br><br>Both **AH** and **ESP** increase ZyWALL processing requirements and communications latency (delay). |

**Table 18** VPN Advanced Wizard: Step 4 (continued)

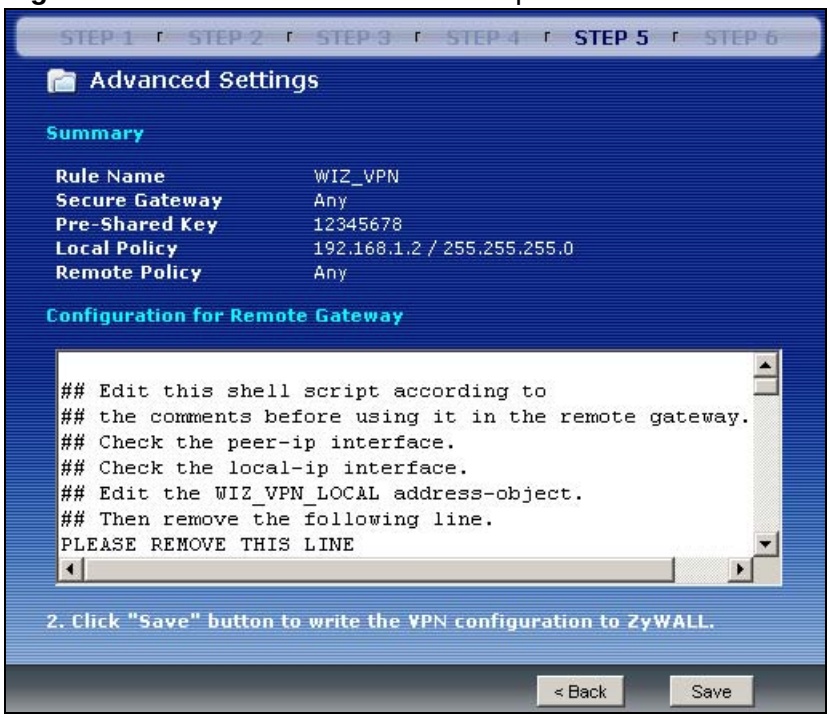
| LABEL | DESCRIPTION |
|---|---|
| Encapsulation | **Tunnel** is compatible with NAT, **Transport** is not.<br><br>**Tunnel** mode encapsulates the entire IP packet to transmit it securely. **Tunnel** mode is required for gateway services to provide access to internal systems. **Tunnel** mode is fundamentally an IP tunnel with authentication and encryption. **Transport** mode is used to protect upper layer protocols and only affects the data in the IP packet. In **Transport** mode, the IP packet contains the security protocol (AH or ESP) located after the original IP header and options, but before any upper layer protocols contained in the packet (such as TCP and UDP). |
| Encryption Algorithm | When **DES** is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The **DES** encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on **DES** that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. **AES128** uses a 128-bit key and is faster than **3DES**. **AES192** uses a 192-bit key and **AES256** uses a 256-bit key. Select **Null** to have no encryption. |
| SA Life Time (Seconds) | Define the length of time before an IKE SA automatically renegotiates in this field. The minimum value is 60 seconds.<br><br>A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected. |
| Perfect Forward Secret (PFS) | Perfect Forward Secret (PFS) is disabled (**None**) by default in phase 2 IPSec SA setup. This allows faster IPSec setup, but is not so secure.<br><br>Select **DH1**, **DH2** or **DH5** to enable PFS. **DH1** refers to Diffie-Hellman Group 1 a 768 bit random number. **DH2** refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number. **DH5** refers to Diffie-Hellman Group 5 a 1536 bit random number (more secure, yet slower). |
| Policy Setting | |
| Local Policy (IP/ Mask) | Type a static local IP address that corresponds to the remote IPSec router's configured remote IP address.<br><br>To specify IP addresses on a network by their subnet mask, type the subnet mask of the LAN behind your ZyWALL. |
| Incoming Interface | Select an interface from the drop-down list box to have packets encrypted by the remote IPSec router to enter the ZyWALL via this interface. |
| Remote Policy (IP/Mask) | If **Any** displays in this field, it is not configurable for the chosen scenario.<br><br>If this field is configurable, type a static local IP address that corresponds to the remote IPSec router's configured local IP address.<br><br>To specify IP addresses on a network by their subnet mask, type the subnet mask of the LAN behind the remote gateway. |

**Table 18** VPN Advanced Wizard: Step 4 (continued)

| LABEL | DESCRIPTION |
|---|---|
| Property | |
| Nailed-Up | This displays for the site-to-site and remote access client role scenarios. Select this to have the ZyWALL automatically renegotiate the IPSec SA when the SA life time expires. |
| Back | Click **Back** to return to the previous screen. |
| Next | Click **Next** to continue. |

This read-only screen shows the status of the current VPN setting. Use the summary table to check whether what you have configured is correct.

**Figure 33** VPN Advanced Wizard: Step 5




The following table describes the labels in this screen.

**Table 19** VPN Advanced Wizard: Step 5

| LABEL | DESCRIPTION |
|---|---|
| Summary | |
| Rule Name | This is the name of the VPN connection (and VPN gateway). |
| Secure Gateway | This is the WAN IP address or domain name of the remote IPSec router. If this field displays **Any**, only the remote IPSec router can initiate the VPN connection. |
| Pre-Shared Key | This is a pre-shared key identifying a communicating party during a phase 1 IKE negotiation. |

**Table 19** VPN Advanced Wizard: Step 5 (continued)

| LABEL | DESCRIPTION |
|---|---|
| Local Policy | This is a (static) IP address and Subnet Mask on the LAN behind your ZyWALL. |
| Remote Policy | This is a (static) IP address and Subnet Mask on the network behind the remote IPSec router. If this field displays **Any**, only the remote IPSec router can initiate the VPN connection. |
| Configuration for Remote Gateway | These commands set the matching VPN connection settings for the remote gateway. If the remote gateway is a ZLD-based ZyWALL, you can copy and paste this list into its command line interface in order to configure it for the VPN tunnel.<br><br>You can also use a text editor to save these commands as a shell script file with a ".zysh" filename extension. Then you can use the file manager to run the script in order to configure the VPN connection.<br><br>See the commands reference guide for details on the commands displayed in this list. |
| Back | Click **Back** to return to the previous screen. |
| Save | Click **Save** to store the VPN settings on your ZyWALL. |

## 4.5.3 VPN Advanced Wizard - Finish

Now you can use the VPN tunnel.

**Figure 34** VPN Wizard: Step 6: Advanced

Note: If you have not already done so, you can register your ZyWALL with myZyXEL.com and activate trials of services like IDP.

Click **Close** to exit the wizard.

# 5

# Configuration Basics

This section provides information to help you configure the ZyWALL effectively. Some of it is helpful when you are just getting started. Some of it is provided for your reference when you configure various features in the ZyWALL.

- Section 5.1 on page 81 introduces the ZyWALL's object-based configuration.
- Section 5.2 on page 82 introduces zones, interfaces, and port groups.
- Section 5.3 on page 85 introduces some differences in terminology and organization between the ZyWALL and other routers, particularly ZyNOS routers.
- Section 5.4 on page 86 identifies the features you should configure before and after you configure the main screens for each feature. For example, if you want to configure a trunk for load-balancing, you should configure the member interfaces before you configure the trunk. After you configure the trunk, you should configure a policy route for it as well. (You might also have to configure criteria for the policy route.)
- Section 5.5 on page 96 identifies the objects that store information used by other features.
- Section 5.6 on page 97 introduces some of the tools available for system management.

## 5.1 Object-based Configuration

The ZyWALL stores information or settings as objects. You use these objects to configure many of the ZyWALL's features and settings. Once you configure an object, you can reuse it in configuring other features.

When you change an object's settings, the ZyWALL automatically updates all the settings or rules that use the object. For example, if you create a schedule object, you can have firewall, application patrol, content filter, and other settings use it. If you modify the schedule, all the firewall, application patrol, content filter, and other settings that use the schedule automatically apply the updated schedule.

You can create address objects based on an interface's IP address, subnet, or gateway. The ZyWALL automatically updates every rule or setting that uses these objects whenever the interface's IP address settings change. For example, if you

change ge1's IP address, the ZyWALL automatically updates the rules or settings that use the ge1 interface-based, LAN subnet address object.

You can use the **Objects** screens to create objects before you configure features that use them. If you are in a screen that uses objects, you can also usually select **Create Object** to open a screen where you can configure a new object.

For a list of common objects, see Section 5.5 on page 96.

# 5.2 Zones, Interfaces, and Physical Ports

Zones (groups of interfaces and VPN tunnels) simplify security settings. Here is an overview of zones, interfaces, and physical ports in the ZyWALL.

**Figure 35** USG 100: Zones, Interfaces, and Physical Ethernet Ports

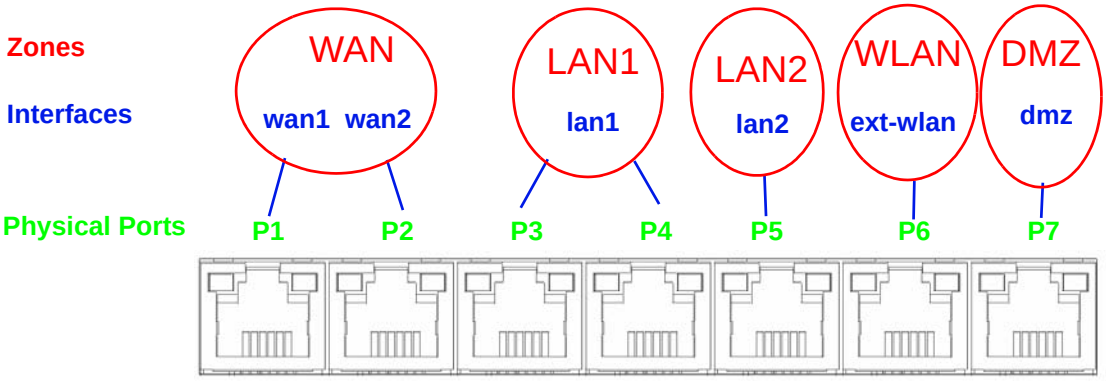



**Figure 36** USG 200: Zones, Interfaces, and Physical Ethernet Ports

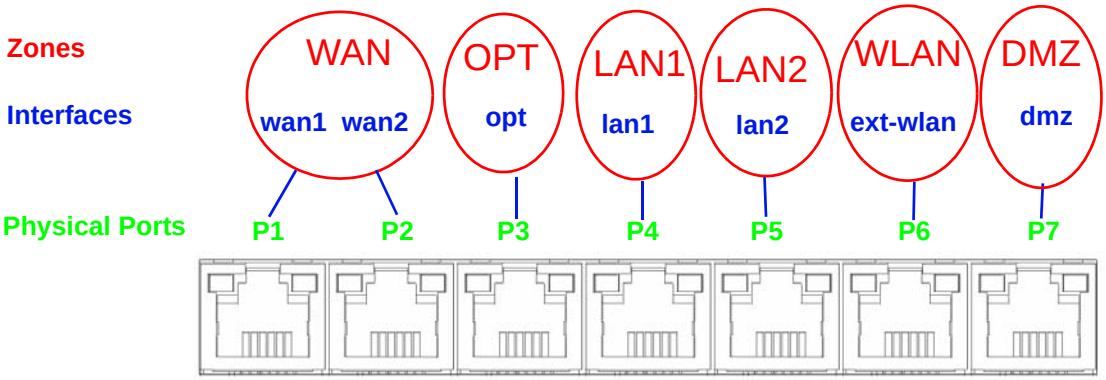


**Table 20** Zones, Interfaces, and Physical Ethernet Ports

| | |
|---|---|
| **Zones**<br><br>(WAN, OPT, LAN, DMZ) | A zone is a group of interfaces and VPN tunnels. Use zones to apply security settings such as firewall, IDP, remote management, anti-virus, and application patrol. You can change the **opt** interface to be part of a different zone. |
| **Interfaces**<br><br>(Ethernet, VLAN,...) | Interfaces are logical entities that (layer-3) packets pass through. Use interfaces in configuring VPN, zones, trunks, device HA, DDNS, policy routes, static routes, HTTP redirect, and virtual server.<br><br>Port roles combine physical ports into interfaces. |
| **Physical Ethernet Ports**<br><br>(P1, P2, ...) | The physical port is where you connect a cable. In configuration, you use physical ports when configuring port groups. You use interfaces and zones in configuring other features. |

## 5.2.1 Interface Types

There are many types of interfaces in the ZyWALL. In addition to being used in various features, interfaces also describe the network that is directly connected to the ZyWALL.

- **Ethernet interfaces** are the foundation for defining other interfaces and network policies. You also configure RIP and OSPF in these interfaces.
- **Port groups** create a hardware connection between physical ports at the layer-2 (data link, MAC address) level. Port groups are created when you use the **Interface > Port Roles** screen to set multiple physical ports to be part of the same (lan1, ext-wlan or dmz) interface.
- **PPP interfaces** support Point-to-Point Protocols (PPPoE or PPTP). ISP account settings are included.
- **VLAN interfaces** recognize tagged frames. The ZyWALL automatically adds or removes the tags as needed. Each VLAN can only be associated with one Ethernet interface.
- **Bridge interfaces** create a software connection between Ethernet or VLAN interfaces at the layer-2 (data link, MAC address) level. Then, you can configure the IP address and subnet mask of the bridge. It is also possible to configure zone-level security between the member interfaces in the bridge.
- **Virtual interfaces** increase the amount of routing information in the ZyWALL. There are three types: **virtual Ethernet interfaces** (also known as IP alias), **virtual VLAN interfaces**, and **virtual bridge interfaces**.
- The **auxiliary interface**, along with an external modem, provides an interface the ZyWALL can use to dial out. This interface can be used as a backup WAN interface, for example. The auxiliary interface controls the **AUX** port.

## 5.2.2 Default Interface and Zone Configuration

This section explains the ZyWALL's factory default zone and interface configuration. The following figure uses letters to denote public IP addresses or part of a private IP address.

**Figure 37** Default Network Topology

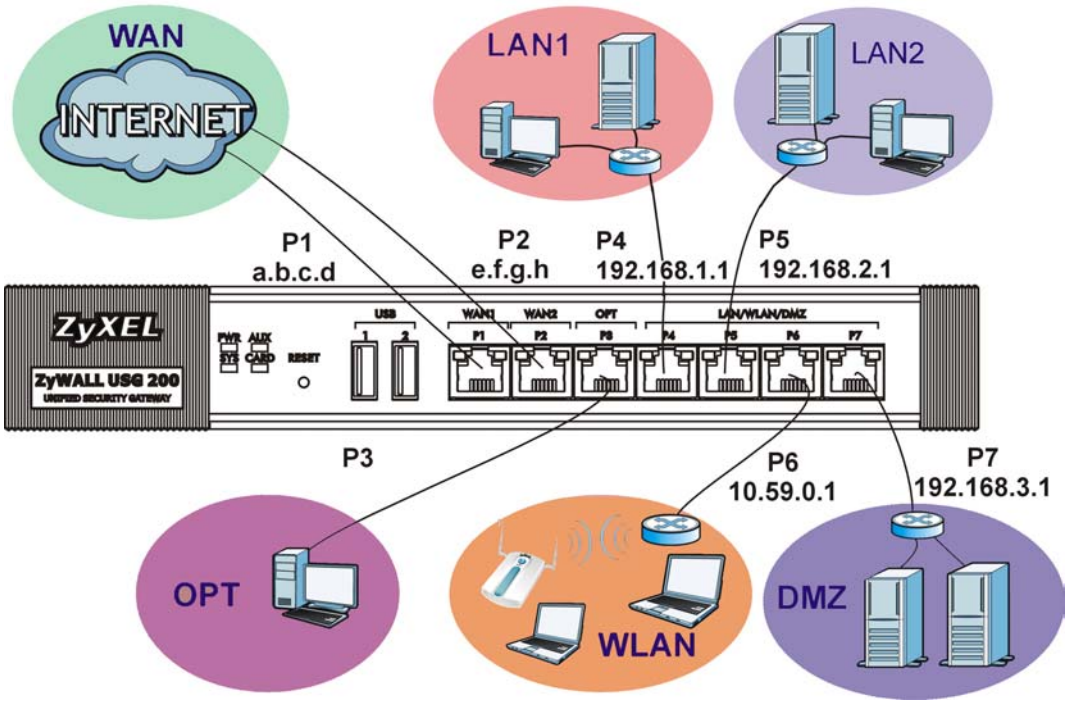



**Table 21** ZyWALL USG 200 Default Port, Interface, and Zone Configuration

| PORT | INTERFACE | ZONE | IP ADDRESS AND DHCP SETTINGS | SUGGESTED USE WITH DEFAULT SETTINGS |
|---|---|---|---|---|
| P1, P2 | wan1, wan2 | WAN | DHCP clients | Connections to the Internet |
| P3 | opt | OPT | None, DHCP server disabled | Third WAN, additional LAN, WLAN, or DMZ port or a separate network. |
| P4 | lan1 | LAN1 | 192.168.1.1, DHCP server enabled | Protected LAN |
| P5 | lan2 | LAN2 | 192.168.2.1, DHCP server enabled | Protected LAN |
| P6 | ext-wlan | WLAN | 10.59.0.1, DHCP server enabled | Wireless access points |
| P7 | dmz | DMZ | 192.168.3.1, DHCP server disabled | Public servers (such as web, e-mail and FTP) |
| AUX | aux | None | None | Auxiliary modem |
| CONSOLE | n/a | None | None | Local management |

**Table 22** ZyWALL USG 100 Default Port, Interface, and Zone Configuration

| PORT | INTERFACE | ZONE | IP ADDRESS AND DHCP SETTINGS | SUGGESTED USE WITH DEFAULT SETTINGS |
|---|---|---|---|---|
| **P1**, **P2** | wan1, wan2 | WAN | DHCP clients | Connections to the Internet |
| P3, P4 | lan1 | LAN1 | 192.168.1.1, DHCP server enabled | Protected LAN |
| P5 | lan2 | LAN2 | 192.168.2.1, DHCP server enabled | Protected LAN |
| P6 | ext-wlan | WLAN | 10.59.0.1, DHCP server enabled | Wireless access points |
| P7 | dmz | DMZ | 192.168.3.1, DHCP server enabled | Public servers (such as web, e-mail and FTP) |
| AUX | aux | None | None | Auxiliary modem |
| CONSOLE | n/a | None | None | Local management |

- The WAN zone contains the **wan1** and **wan2** interfaces (physical ports **P1** and **P2**). They use public IP addresses to connect to the Internet.
- OPT is specific to the ZyWALL USG 200 .The OPT zone contains the **opt** interface (physical port **P3**). The **opt** interface is the only default interface that you can change to be part of a different zone. The **opt** interface belongs to the OPT zone by default. The OPT zone is a separate zone and you can configure a different set of security policies for it.
- The LAN1 zone contains the **lan1** interface (a port group made up of physical ports **P4** and **P5** on the ZyWALL USG 200 or **P3**, **P4**, and **P5** on the ZyWALL USG 100). The LAN1 zone is a protected zone. The **lan1** interface uses 192.168.1.1 and the connected devices use IP addresses in the 192.168.1.2 to 192.168.1.254 range.
- The WLAN zone contains the **ext-wlan** interface (physical port **P6**). This is a second protected zone for connecting wireless access points. The **ext-wlan** interface uses private IP address 10.59.0.1 and the connected devices use IP addresses in the 10.59.0.2 to 10.59.0.254 range.
- The DMZ zone contains the **dmz** interface (physical port **P7**). The DMZ zone has servers that are available to the public. The **dmz** interface uses private IP address 192.168.3.1 and the connected devices use private IP addresses in the 192.168.3.2 to 192.168.3.254 range.

# 5.3 Terminology in the ZyWALL

This section highlights some differences in terminology or organization between the ZyWALL and other routers, particularly ZyNOS routers.

**Table 23** ZyWALL Terminology That is Different Than ZyNOS

| ZYNOS FEATURE / TERM | ZYWALL FEATURE / TERM |
|---|---|
| Port forwarding | Virtual server |
| IP alias | Virtual interface |

**Table 23** ZyWALL Terminology That is Different Than ZyNOS (continued)

| ZYNOS FEATURE / TERM | ZYWALL FEATURE / TERM |
|---|---|
| Gateway policy | VPN gateway |
| Network policy (IPSec SA) | VPN connection |
| Hub-and-spoke VPN | (VPN) concentrator |

**Table 24** ZyWALL Terminology That Might Be Different Than Other Products

| FEATURE / TERM | ZYWALL FEATURE / TERM |
|---|---|
| Destination NAT (DNAT) | Virtual server |
| Source NAT (SNAT) | Policy route |

**Table 25** NAT: Differences Between the ZyWALL and ZyNOS

| ZYNOS FEATURE / SCREEN | ZYWALL FEATURE / SCREEN |
|---|---|
| Port forwarding | Virtual server |
| Trigger port, port triggering | Policy route |
| Address mapping | Policy route |
| Address mapping (VPN) | IPSec VPN |

**Table 26** Bandwidth Management: Differences Between the ZyWALL and ZyNOS

| ZYNOS FEATURE / SCREEN | ZYWALL FEATURE / SCREEN |
|---|---|
| Interface bandwidth management (outbound) | Interface |
| OSI level-7 bandwidth management | Application patrol |
| General bandwidth management | Policy route |

# 5.4 Feature Configuration Overview

This section provides information about configuring the main features in the ZyWALL. The features are listed in the same sequence as the menu item(s) in the Web Configurator. Each feature is organized as shown below.

## 5.4.1 Feature

This provides a brief description. See the appropriate chapter(s) in this User's Guide for more information about any feature.

| | |
|---|---|
| **MENU ITEM(S)** | This shows you the sequence of menu items and tabs you should click to find the main screen(s) for this feature. See the web help or the related User's Guide chapter for information about each screen. |

| | |
|---|---|
| **PREREQUISITES** | These are other features you should configure before you configure the main screen(s) for this feature.<br><br>If you did not configure one of the prerequisites first, you can often select an option to create a new object. After you create the object you return to the main screen to finish configuring the feature.<br><br>You may not have to configure everything in the list of prerequisites. For example, you do not have to create a schedule for a policy route unless time is one of the criterion. |
| **WHERE USED** | There are two uses for this.<br><br>These are other features you should usually configure or check right after you configure the main screen(s) for this feature. For example, you should usually create a policy route for a VPN tunnel.<br><br>You have to delete the references to this feature before you can delete any settings. For example, you have to delete (or modify) all the policy routes that refer to a VPN tunnel before you can delete the VPN tunnel. |

**Example:** This provides a simple example to show you how to configure this feature. The example is usually based on the network topology in Figure 37 on page 84.

Note: **PREQUISITES** or **WHERE USED** does not appear if there are no prerequisites or references in other features to this one. For example, no other features reference DDNS entries, so there is no **WHERE USED** entry.

## 5.4.2 Interface

See Section 5.2 on page 82 for background information.

Note: When you create an interface, there is no security applied on it until you assign it to a zone.

Most of the features that use interfaces support Ethernet, PPPoE/PPTP, cellular, wireless LAN, VLAN, and bridge interfaces.

| | |
|---|---|
| **MENU ITEM(S)** | **Network > Interface** (except **Network > Interface > Trunk**) |
| **PREREQUISITES** | Port groups (configured in the **Interface > Port Grouping** screen) |
| **WHERE USED** | Zones, trunks, IPSec VPN, device HA, DDNS, policy routes, static routes, HTTP redirect, virtual server, application patrol |

**Example:** The **dmz** interface is in the DMZ zone and uses a private IP address. To configure **dmz**'s settings, click **Network > Interface > Ethernet** and then the **dmz**'s **Edit** icon.

### 5.4.3 Trunks

Use trunks to set up load balancing using two or more interfaces.

| | |
|---|---|
| **MENU ITEM(S)** | **Network > Interface > Trunk** |
| **PREREQUISITES** | Interfaces |
| **WHERE USED** | Policy routes |

**Example:** See Chapter 6 on page 101.

### 5.4.4 IPSec VPN

Use IPSec VPN to provide secure communication between two sites over the Internet or any insecure network that uses TCP/IP for communication. The ZyWALL also offers hub-and-spoke VPN.

| | |
|---|---|
| **MENU ITEM(S)** | **VPN > IPSec VPN**; you can also use the **VPN Setup Wizard**, which handles most of the prerequisites for you. |
| **PREREQUISITES** | Interfaces, certificates (authentication), authentication methods (extended authentication), addresses (local network, remote network, NAT), to-ZyWALL firewall, firewall |
| **WHERE USED** | Policy routes, zones, L2TP VPN |

**Example:** See Chapter 6 on page 101.

### 5.4.5 SSL VPN

Use SSL VPN to provide secure network access to remote users.

| | |
|---|---|
| **MENU ITEM(S)** | **VPN > SSL VPN** |
| **PREREQUISITES** | Interfaces, SSL application, users, user groups, addresses (network list, IP pool for assigning to clients, DNS and WINS server addresses), to-ZyWALL firewall, firewall |
| **WHERE USED** | Policy routes, zones |

**Example:** See Chapter 6 on page 101.

### 5.4.6 L2TP VPN

Use L2TP VPN to let remote users use the L2TP and IPSec client software included with their computers' operating systems to securely connect to the network behind the ZyWALL.

| | |
|---|---|
| **MENU ITEM(S)** | **VPN > L2TP VPN** |

| | |
|---|---|
| **PREREQUISITES** | Interfaces, IPSec VPN connection, certificates (authentication), authentication methods (extended authentication), addresses (local network, remote network, NAT, IP pool for assigning to clients, DNS and WINS server addresses), to-ZyWALL firewall, firewall |
| **WHERE USED** | The IPSec VPN connection used for L2TP VPN can be used in policy routes and zones |

**Example:** See Chapter 28 on page 447.

## 5.4.7 Zones

See Section 5.2 on page 82 for background information. A zone is a group of interfaces and VPN tunnels. The ZyWALL uses zones, not interfaces, in many security settings, such as firewall rules and remote management.

Zones cannot overlap. Each interface and VPN tunnel can be assigned to at most one zone. Virtual interfaces are automatically assigned to the same zone as the interface on which they run.

| | |
|---|---|
| **MENU ITEM(S)** | **Network > Zone** |
| **PREREQUISITES** | Interfaces, IPSec VPN, SSL VPN |
| **WHERE USED** | Firewall, IDP, remote management, anti-virus, ADP, application patrol |

**Example:** For example, to change the OPT port to being in the LAN1 zone, click **Network > Zone** and then the **OPT Edit** icon. Remove the OPT interface from the OTP zone and click **Apply**. Then click the **LAN1 Edit** icon and add the OPT interface and click **Apply**.

## 5.4.8 Device HA

To increase network reliability, device HA lets a backup ZyWALL automatically take over if a master ZyWALL fails.

| | |
|---|---|
| **MENU ITEM(S)** | **Device HA** |
| **PREREQUISITES** | Interfaces (with a static IP address), to-ZyWALL firewall |

**Example:** See Chapter 6 on page 101.

## 5.4.9 DDNS

Dynamic DNS maps a domain name to a dynamic IP address. The ZyWALL helps maintain this mapping.

| | |
|---|---|
| **MENU ITEM(S)** | **Network > DDNS** |

| PREREQUISITES | Interface |
|---|---|

## 5.4.10 Policy Routes

Use policy routes to control the routing of packets through the ZyWALL's interfaces, trunks, and send traffic through VPN connections. You also use policy routes for bandwidth management (out of the ZyWALL), port triggering, and general NAT on the source address. You have to set up the criteria, next-hops, and NAT settings in other screens first.

| MENU ITEM(S) | **Network > Routing > Policy Route** |
|---|---|
| PREREQUISITES | Criteria: users, user groups, interfaces (incoming), IPSec VPN (incoming), addresses (source, destination), address groups (source, destination), schedules, services, service groups<br><br>Next-hop: addresses (HOST gateway), IPSec VPN, SSL VPN, trunks, interfaces<br><br>NAT: addresses (translated address), services and service groups (port triggering) |

**Example:** You have an FTP server connected to **ge4** (in the DMZ zone). You want to limit the amount of FTP traffic that goes out from the FTP server through your WAN connection.

1 Create an address object for the FTP server (**Object > Address**).

2 Click **Network > Routing > Policy Route** to go to the policy route configuration screen. Add a policy route.

3 Name the policy route.

4 Select the interface that the traffic comes in through (**ge4** in this example).

5 Select the FTP server's address as the source address.

6 You don't need to specify the destination address or the schedule.

7 For the service, select **FTP**.

8 For the **Next Hop** fields, select **Interface** as the **Type** if you have a single WAN connection or **Trunk** if you have multiple WAN connections.

9 Select the interface that you are using for your WAN connection (**ge2** and **ge3** are the default WAN interfaces). If you have multiple WAN connections, select the trunk.

10 Specify the amount of bandwidth FTP traffic can use. You may also want to set a low priority for FTP traffic.

Note: The ZyWALL checks the policy routes in the order that they are listed. So make sure that your custom policy route comes before any other routes that would also match the FTP traffic.

## 5.4.11 Static Routes

Use static routes to tell the ZyWALL about networks not directly connected to the ZyWALL.

| | |
|---|---|
| **MENU ITEM(S)** | **Network > Routing > Static Route** |
| **PREREQUISITES** | Interfaces |

## 5.4.12 Firewall

The firewall controls the travel of traffic between or within zones. You can also configure the firewall to control traffic for virtual server (port forwarding) and policy routes (NAT). You can configure firewall rules based on schedules, specific users (or user groups), source or destination addresses (or address groups) and services (or service groups). Each of these objects must be configured in a different screen.

To-ZyWALL firewall rules control access to the ZyWALL. Configure to-ZyWALL firewall rules for remote management. By default, the firewall only allows mangement connections from the LAN, WLAN, or WAN zone.

| | |
|---|---|
| **MENU ITEM(S)** | **Firewall** |
| **PREREQUISITES** | Zones, schedules, users, user groups, addresses (source, destination), address groups (source, destination), services, service groups |

**Example:** Suppose you have a SIP proxy server connected to the DMZ zone for VoIP calls. You could configure a firewall rule to allow VoIP sessions from the SIP proxy server on DMZ to the LAN so VoIP users on the LAN can receive calls.

1 Create a VoIP service object for UDP port 5060 traffic (**Object > Service**).

2 Create an address object for the VoIP server (**Object > Address**).

3 Click **Firewall** to go to the firewall configuration.

4 Select from the **DMZ** zone to the **LAN1** zone, and add a firewall rule using the items you have configured.

- You don't need to specify the schedule or the user.
- In the **Source** field, select the address object of the VoIP server.
- You don't need to specify the destination address.
- Leave the **Access** field set to **Allow** and the **Log** field set to **No**.

Note: The ZyWALL checks the firewall rules in order. Make sure each rule is in the correct place in the sequence.

## 5.4.13 Application Patrol

Use application patrol to control which individuals can use which services through the ZyWALL (and when they can do so). You can also specify allowed amounts of bandwidth and priorities. You must subscribe to use application patrol. You can subscribe using the **Licensing > Registration** screens or one of the wizards.

| MENU ITEM(S) | AppPatrol |
|---|---|
| PREREQUISITES | Registration, zones, Schedules, users, user groups, addresses (source, destination), address groups (source, destination). These are only used as criteria in exceptions and conditions. |

**Example:** Suppose you want to allow vice president Bob to use BitTorrent and block everyone else from using it.

1 Create a user account for Bob (**User/Group**).

2 Click **AppPatrol > Peer to Peer** to go to the application patrol configuration screen. Click the BitTorrent application patrol entry's **Edit** icon.

- Set the default policy's access to **Drop**.
- Add another policy.
- Select the user account that you created for Bob.
- You can leave the source, destination and log settings at the default.

Note: With this example, Bob would have to log in using his account. If you do not want him to have to log in, you might create an exception policy with Bob's computer IP address as the source.

## 5.4.14 Anti-Virus

Use anti-virus to detect and take action on viruses. You must subscribe to use anti-virus. You can subscribe using the **Licensing > Registration** screens or one of the wizards.

| MENU ITEM(S) | Anti-X > AV |
|---|---|

| PREREQUISITES | Registration, zones |
|---|---|

## 5.4.15 IDP

Use IDP to detect and take action on malicious or suspicious packets. You must subscribe to use IDP. You can subscribe using the **Licensing > Registration** screens or one of the wizards.

| MENU ITEM(S) | **Anti-X > IDP** |
|---|---|
| PREREQUISITES | Registration, zones |

## 5.4.16 ADP

Use ADP to detect and take action on traffic and protocol anomalies.

| MENU ITEM(S) | **Anti-X > ADP** |
|---|---|
| PREREQUISITES | Zones |

## 5.4.17 Content Filter

Use content filtering to block or allow access to specific categories of web site content, individual web sites and web features (such as cookies). You can define which user accounts (or groups) can access what content and at what times. You must have a subscription in order to use the category-based content filtering. You can subscribe using the menu item or one of the wizards.

| MENU ITEM(S) | **Anti-X > Content Filter** |
|---|---|
| PREREQUISITES | Registration, addresses (source), schedules, users, user groups |

**Example:** You can configure a policy that blocks Bill's access to arts and entertainment web pages during the workday. You must have already subscribed to the content filter service.

1. Create a user account for Bill if you have not done so already (**User/Group**).
2. Create a schedule for the work day (**Object > Schedule**).
3. Click **Anti-X > Content Filter > Filter Profile**. Click the **Add** icon to go to the screen where you can configure a category-based profile.
4. Name the profile and enable it.
5. Enable the external web filter service.

6 Decide what to do for matched web sites (**Block** in this example), unrated web sites and what to do when the category-based content filtering service is not available.

7 Select the **Arts/Entertainment** category (you need to click **Advanced** to display it).

8 Click **OK**.

9 Click **General** to go to the content filter general configuration screen.

10 Enable the content filter.

11 Add a policy that uses the schedule, the filtering profile and the user that you created.

## 5.4.18 Anti-Spam

Use anti-spam to detect and take action on spam mail.

| | |
|---|---|
| **MENU ITEM(S)** | **Anti-X > Anti-Spam** |
| **PREREQUISITES** | Zones |

## 5.4.19 Virtual Server (Port Forwarding)

Use this to change the address and/or port number of packets coming in from a specified interface. This is also known as port forwarding.

The ZyWALL does not check to-ZyWALL firewall rules for packets that are redirected by virtual server. It does check regular (through-ZyWALL) firewall rules.

| | |
|---|---|
| **MENU ITEM(S)** | **Network > Virtual Server** |
| **PREREQUISITES** | Interfaces, addresses (HOST) |

**Example:** Suppose you have an FTP server with a private IP address connected to a DMZ port. You could configure a virtual server rule to forwards FTP sessions from the WAN to the DMZ.

1 Click **Network > Virtual Server** to configure the virtual server. Add an entry.

2 Name the entry.

3 Select the WAN interface that the FTP traffic is to come in through.

4 Specify the public WAN IP address where the ZyWALL will receive the FTP packets.

5 In the **Mapped IP field**, list the IP address of the FTP server. The ZyWALL will forward the packets received for the original IP address.

6 In **Mapping Type**, select **Port**.

7 Enter 21 in both the **Original** and the **Mapped Port** fields.

## 5.4.20 HTTP Redirect

Configure this feature to have the ZyWALL transparently forward HTTP (web) traffic to a proxy server. This can speed up web browsing because the proxy server keeps copies of the web pages that have been accessed so they are readily available the next time one of your users needs to access that page.

The ZyWALL does not check to-ZyWALL firewall rules for packets that are redirected by HTTP redirect. It does check regular (through-ZyWALL) firewall rules.

| | |
|---|---|
| **MENU ITEM(S)** | **Network > HTTP Redirect** |
| **PREREQUISITES** | Interfaces |

**Example:** Suppose you want HTTP requests from your LAN to go to a HTTP proxy server at IP address 192.168.3.80.

1 Click **Network > HTTP Redirect**.

2 Add an entry.

3 Name the entry.

4 Select the interface from which you want to redirect incoming HTTP requests (**lan1**).

5 Specify the IP address of the HTTP proxy server.

6 Specify the port number to use for the HTTP traffic that you forward to the proxy server.

### 5.4.21 ALG

The ZyWALL's Application Layer Gateway (ALG) allows VoIP and FTP applications to go through NAT on the ZyWALL. You can also specify additional signaling port numbers.

| MENU ITEM(S) | Network > ALG |
|---|---|

## 5.5 Objects

Objects store information and are referenced by other features. If you update this information in response to changes, the ZyWALL automatically propagates the change through the features that use the object.

The following table introduces the objects. You can also use this table when you want to delete an object because you have to delete references to the object first.

**Table 27** Objects Overview

| OBJECT | WHERE USED |
|---|---|
| user/group | See the User/Group section for details on users and user groups. |
| address | VPN connections (local / remote network, NAT), policy routes (criteria, next-hop [HOST], NAT), firewall, application patrol (source, destination), content filter, virtual server (HOST), user settings (force user authentication), address groups, remote management (System) |
| address group | Policy routes (criteria), firewall, application patrol (source, destination), content filter, user settings (force user authentication), address groups, remote management (System) |
| service, service group | Policy routes (criteria, port triggering), firewall, service groups, log (criteria) |
| schedule | Policy routes (criteria), firewall, application patrol, content filter, user settings (force user authentication) |
| AAA server | Authentication methods |
| authentication methods | VPN gateways (extended authentication), WWW (client authentication), L2TP VPN |
| certificates | VPN gateways, WWW, SSH, FTP |
| SSL Application | SSL VPN |

### 5.5.1 User/Group

Use these screens to configure the ZyWALL's administrator and user accounts. The ZyWALL provides the following user types.

**Table 28** User Types

| TYPE | ABILITIES |
|---|---|
| Admin | Change ZyWALL configuration (web, CLI) |
| Limited-Admin | Look at ZyWALL configuration (web) |
| User | Access network services, browse user-mode commands (CLI) |
| Guest | Access network services |
| Ext-User | The same as a User or a Guest. The ZyWALL looks for the specific type in an external authentication server. If the type is not available, the ZyWALL applies default settings. |

If you want to force users to log in to the ZyWALL before the ZyWALL routes traffic for them, you might have to configure prerequisites first.

| | |
|---|---|
| **MENU ITEM(S)** | **Object > User/Group** |
| **PREREQUISITES** | Addresses, address groups, schedules. The prerequisites are only used in policies to force user authentication |
| **WHERE USED** | Policy routes, firewall, application patrol, content filter, user groups, VPN |

## 5.6 System Management and Maintenance

This section introduces some of the management and maintenance features in the ZyWALL. Use **Host Name** to configure the system and domain name for the ZyWALL. Use **Date/Time** to configure the current date, time, and time zone in the ZyWALL. Use **Console Speed** to set the console speed. Use **Language** to select a language for the Web Configurator screens.

### 5.6.1 DNS, WWW, SSH, TELNET, FTP, SNMP, Dial-in Mgmt, Vantage CNM

Use these screens to set which services or protocols can be used to access the ZyWALL through which zone and from which addresses (address objects) the access can come. Use **Dial-in Mgmt** for a remote management connection through an external serial modem connected to the **AUX** port.

| | |
|---|---|
| **MENU ITEM(S)** | **System > DNS, WWW, SSH, TELNET, FTP, SNMP, Dial-in Mgmt, Vantage CNM, Language** |

| PREREQUISITES | To-ZyWALL firewall, zones, addresses, address groups, certificates (WWW, SSH, FTP, Vantage CNM), authentication methods (WWW) |
|---|---|

**Example:** Suppose you want to allow an administrator to use HTTPS to manage the ZyWALL from the WAN.

1 Create an administrator account (**User/Group**).

2 Create an address object for the administrator's computer (**Object > Address**).

3 Click **System > WWW** to configure the HTTP management access. Enable HTTPS and add an administrator service control entry.

- Select the address object for the administrator's computer.
- Select the **WAN** zone.
- Set the action to **Accept**.

## 5.6.2 File Manager

Use these screens to upload, download, delete, or run scripts of CLI commands. You can manage

- Configuration files. Use configuration files to back up and restore the complete configuration of the ZyWALL. You can store multiple configuration files in the ZyWALL and switch between them without restarting.
- Shell scripts. Use shell scripts to run a series of CLI commands. These are useful for large, repetitive configuration changes (for example, creating a lot of VPN tunnels) and for troubleshooting.

You can edit configuration files and shell scripts in any text editor.

| MENU ITEM(S) | **Maintenance > File Manager** |
|---|---|

## 5.6.3 Licensing Registration

Use these screens to register your ZyWALL and subscribe to services like anti-virus, IDP and application patrol, more SSL VPN tunnels, and content filtering. You must have Internet access to myZyXEL.com.

| MENU ITEM(S) | **Licensing > Registration** |
|---|---|
| PREREQUISITES | Internet access to myZyXEL.com |

## 5.6.4 Licensing Update

Use these screens to update the ZyWALL's signature packages for the anti-virus, IDP and application patrol, and system protect features. You must have a valid subscription to update the anti-virus and IDP/application patrol signatures You must have Internet access to myZyXEL.com.

| | |
|---|---|
| **MENU ITEM(S)** | **Licensing > Update** |
| **PREREQUISITES** | Registration (for anti-virus and IDP/application patrol), Internet access to myZyXEL.com |

## 5.6.5 Logs and Reports

The ZyWALL provides a system log, offers two e-mail profiles to which to send log messages, and sends information to four syslog servers. It also provides statistical reports to track user activity, web site hits, virus traffic and intrusions and can e-mail them to you on a daily basis.

| | |
|---|---|
| **MENU ITEM(S)** | **Maintenance > Log, Report** |

## 5.6.6 Diagnostics

The ZyWALL can generate a file containing the ZyWALL's configuration and diagnostic information.

| | |
|---|---|
| **MENU ITEM(S)** | **Maintenance > Diagnostics** |

# 6

# Tutorials

This chapter provides some examples of using the Web Configurator to set up features in the ZyWALL. See also Chapter 28 on page 447 for an example of configuring L2TP.

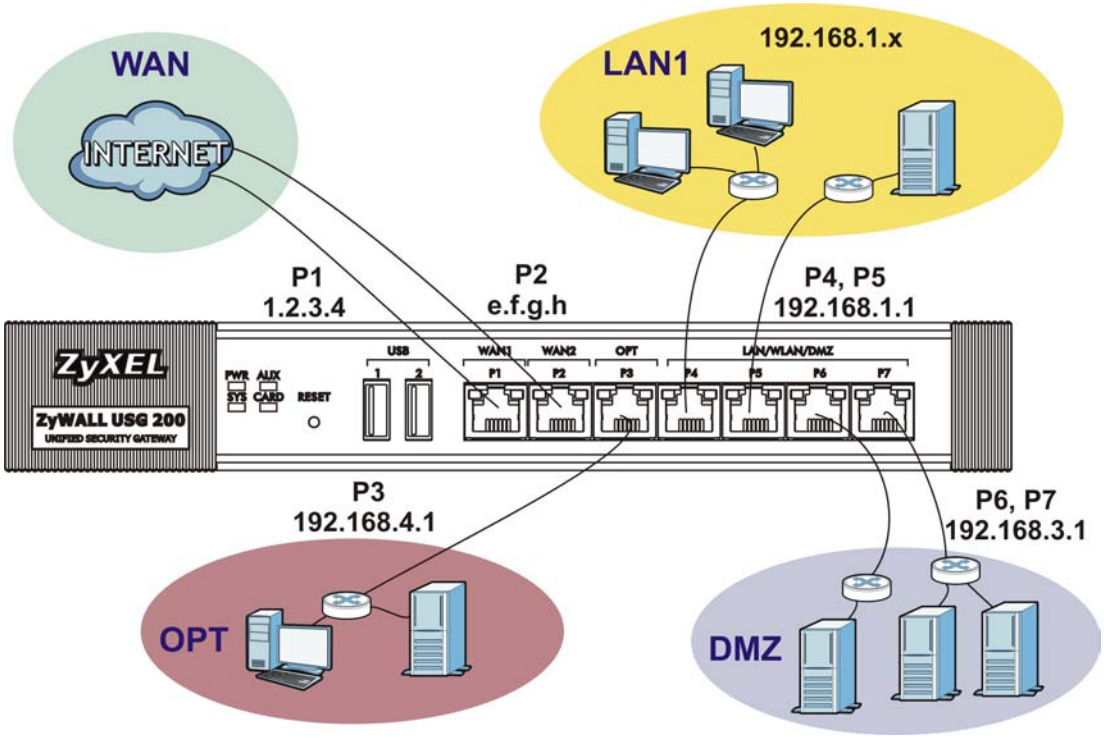
## 6.1 How to Configure Interfaces, Port Roles, and Zones

This tutorial shows how to configure Ethernet interfaces, port roles, and zones for the following example configuration (see Section 5.2.2 on page 84 for the default configuration).

- The **wan1** interface uses a static IP address of 1.2.3.4.
- The **opt** interface is used for a protected local network. It uses IP address 192.168.4.1 and has a DHCP server. Add it to the LAN zone so all of the LAN zone's security policies apply to it.

- This example does not use the **ext-wlan** interface (for Ethernet-connected APs) so you remove port **P6** from the **ext-wlan** interface and add it to the **dmz** interface instead.

**Figure 38** Ethernet Interface, Port Roles, and Zone Configuration Example

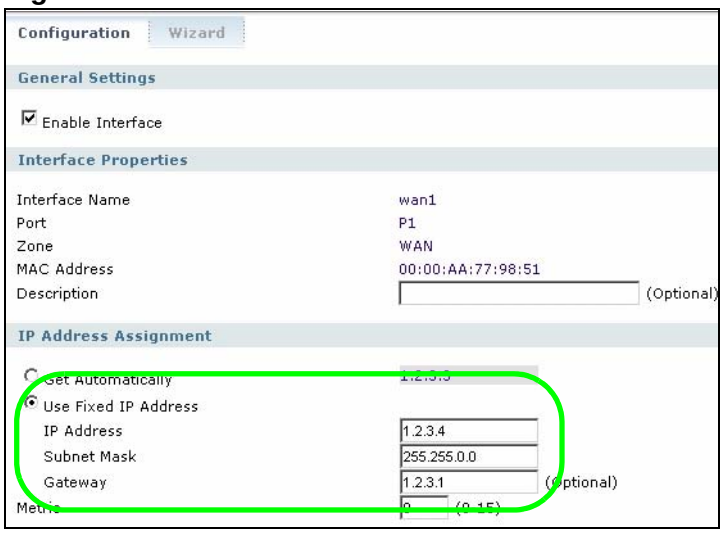



## 6.1.1 Configure a WAN Ethernet Interface

You need to assign the ZyWALL's **wan1** interface a static IP address of 1.2.3.4.

Click **Network > Interface > Ethernet** and the **wan1** interface's **Edit** icon. Configure the IP address, subnet mask, and default gateway settings as follows and click **OK**.

**Figure 39** Network > Interface > Ethernet > Edit wan1

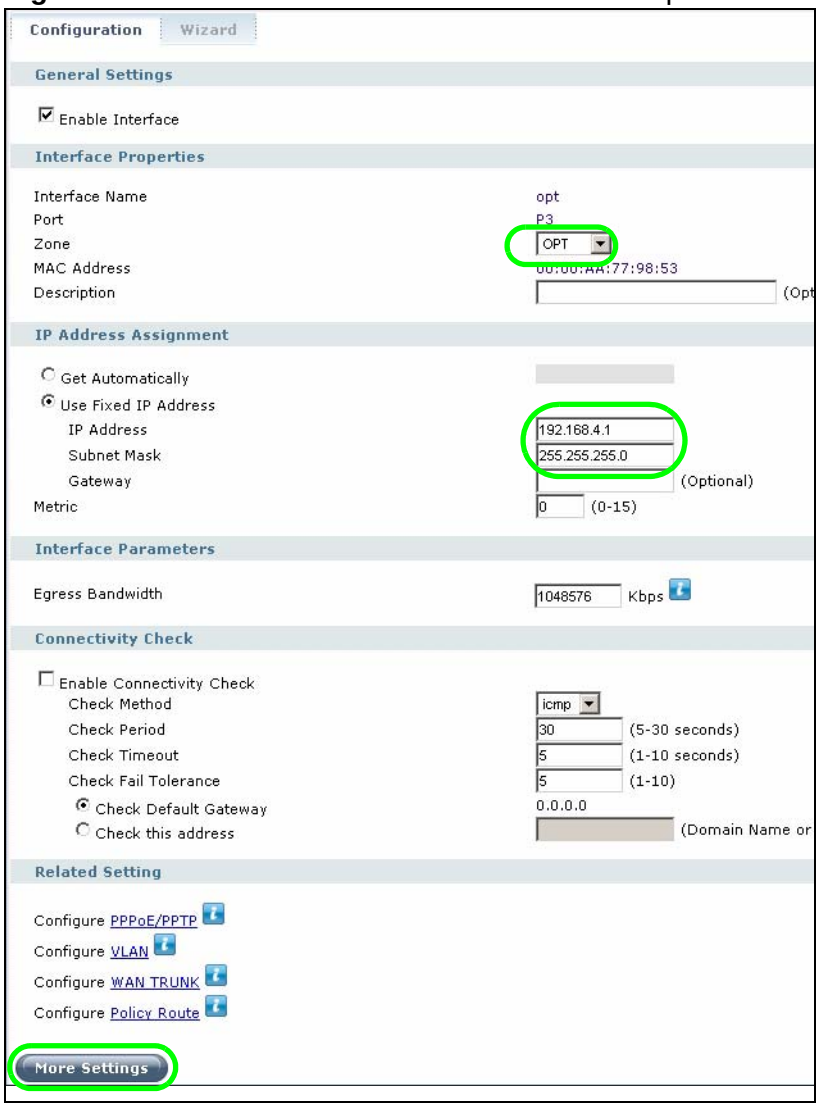



## 6.1.2 Configure the OPT Interface for a Local Network

Here is how to set the **opt** interface for a separate local network. It uses 192.168.4.1 as its IP address and has a DHCP server to distribute IP addresses to connected DHCP clients.

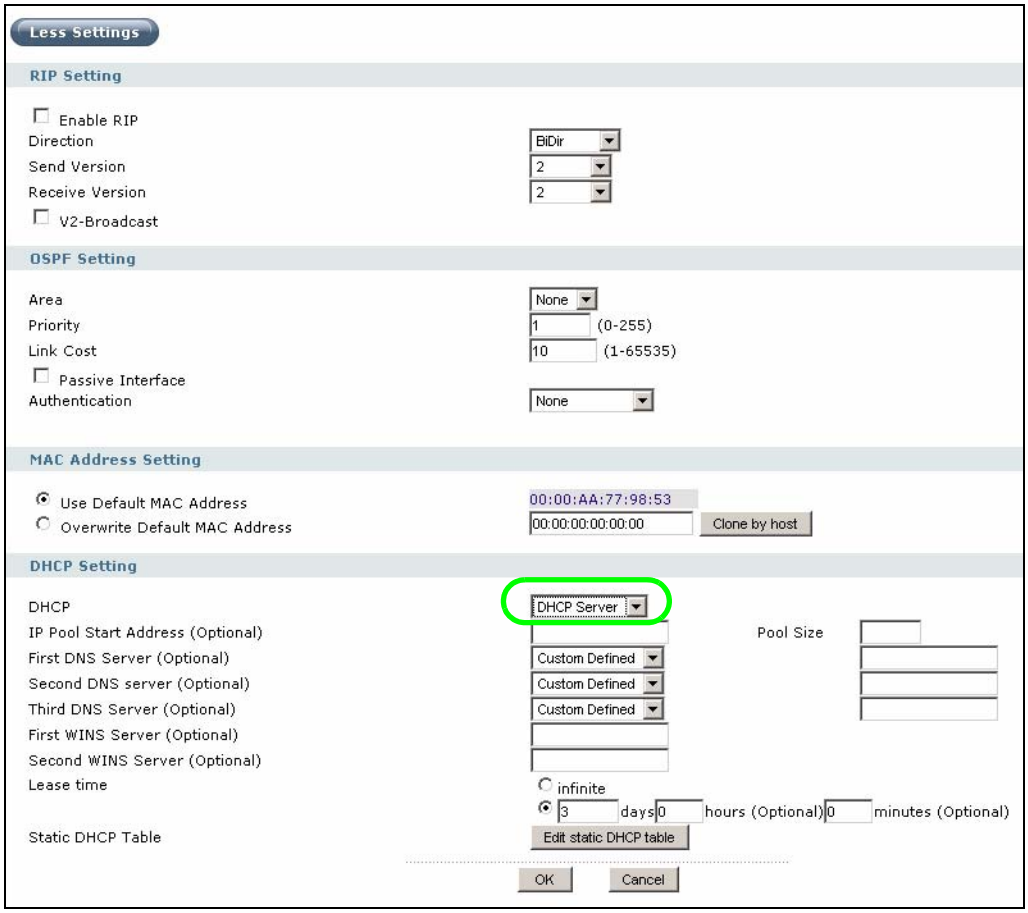
1 Click **Network > Interface > Ethernet** and the **opt** interface's **Edit** icon. Set the **IP Address** to 192.168.4.1, the **Subnet Mask** to 255.255.255.0, and the **Zone** to **LAN** as shown next. Then click **More Settings**.

**Figure 40** Network > Interface > Ethernet > Edit opt



2 Set **DHCP** to **DHCP Server** and click **OK**.

**Figure 41** Network > Interface > Ethernet > Edit opt > More Settings



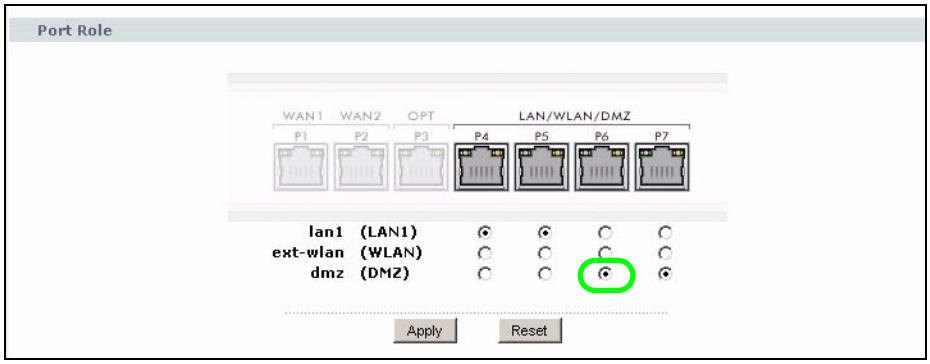

## 6.1.3 Configure Port Roles

Here is how to remove port **P6** from the ext-wlan interface and add it to the dmz interface.

1 Click **Network > Interface > Role**.

2 Under **P6** select the **dmz (DMZ)** radio button and click **Apply**.

**Figure 42** Network > Interface > Port Roles Example




# 6.2 How to Configure a Cellular Interface

Use 3G cards for cellular WAN (Internet) connections. Table 275 on page 835 lists the compatible 3G devices. In this example you install or connect the 3G card before you configure the cellular interfaces but is also possible to reverse the sequence.

1 Make sure the 3G device's SIM card is installed.

2 Install the 3G device in the ZyWALL's PCIMCIA slot or connect it to one of the ZyWALL's USB ports.

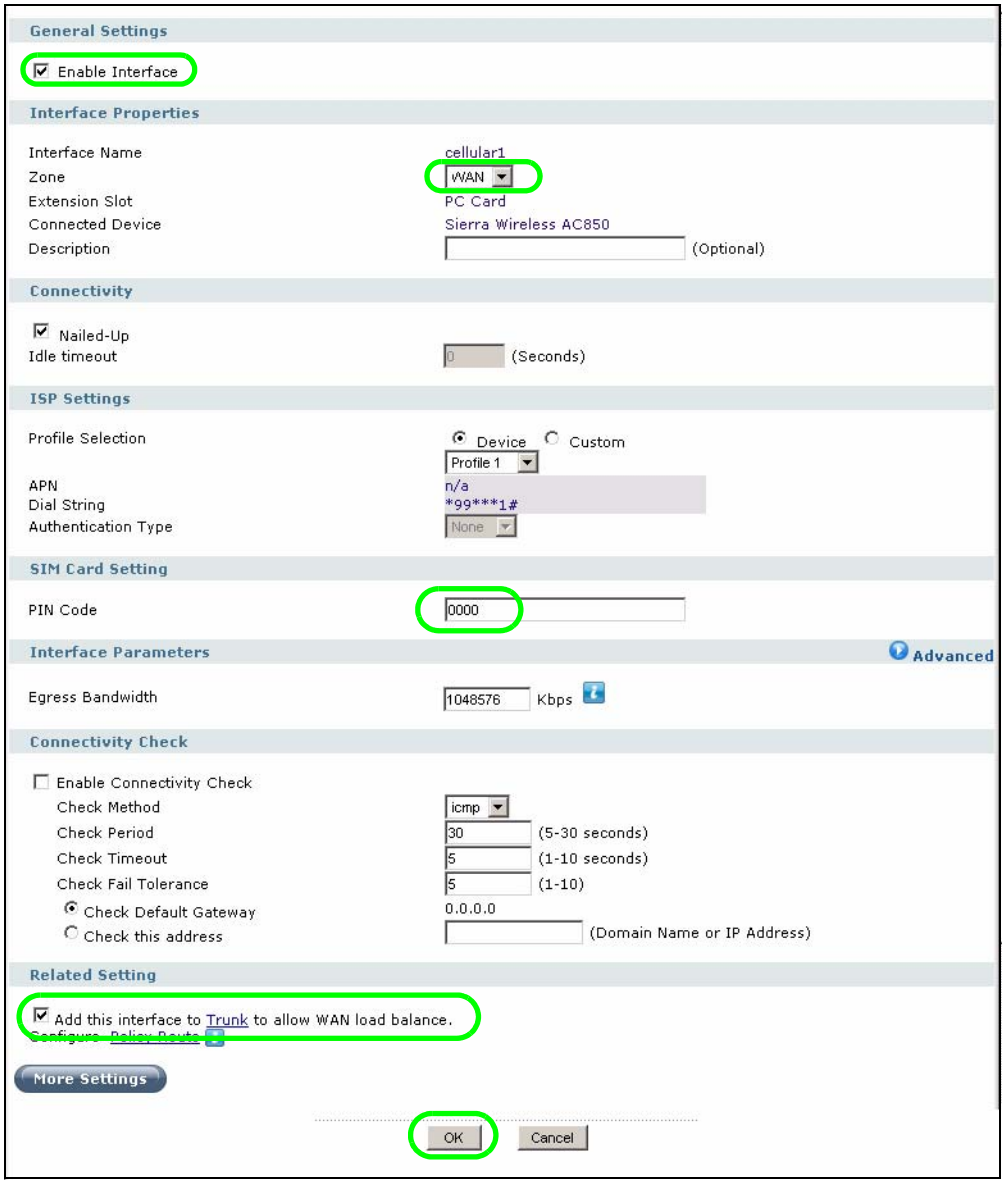
3 Click **Network > Interface > Cellular**. Click the 3G card's **Edit** icon.

**Figure 43** Network > Interface > Cellular

4 Enable the interface and add it to a zone. It is highly recommended that you set the **Zone** to **WAN** to apply your WAN zone security settings to this 3G connection. Leaving **Zone** blank has the ZyWALL not apply any security settings to the 3G connection. Enter the **PIN Code** provided by the cellular 3G service provider (0000 in this example).

In **Related Setting**, keep **Add this interface to Trunk to allow WAN load balance** selected. Click **OK**.

**Figure 44** Network > Interface > Cellular > Edit




5 Go to the **Status** screen. The **Interface Status Summary** section should contain a “cellular” entry. When its connection status is “Connected” you can use the 3G connection to access the Internet.

**Figure 45** Status

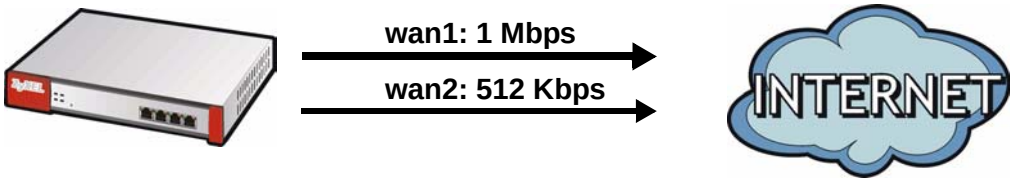
The ZyWALL automatically balances the traffic load amongst the available WAN connections. This enhances overall network throughput. Plus, if a WAN connection goes down, the ZyWALL sends traffic through the remaining WAN connections. For a simple test, disconnect all of the ZyWALL's wired WAN connections. If you can still access the Internet, your cellular interface is properly configured and your cellular device is working.

To fine-tune the load balancing configuration, see Chapter 11 on page 263. See also Section 6.3 on page 108 for an example.

# 6.3 How to Configure Load Balancing

This example shows how to configure a trunk for two WAN connections (to the Internet). The available bandwidth for the connections is 1Mbps (**wan1**) and 512 Kbps (**wan2**) respectively. As these connections have different bandwidth, use the **Weighted Round Robin** algorithm to send traffic to wan1 and wan2 in a 2:1 ratio.

**Figure 46** Trunk Example



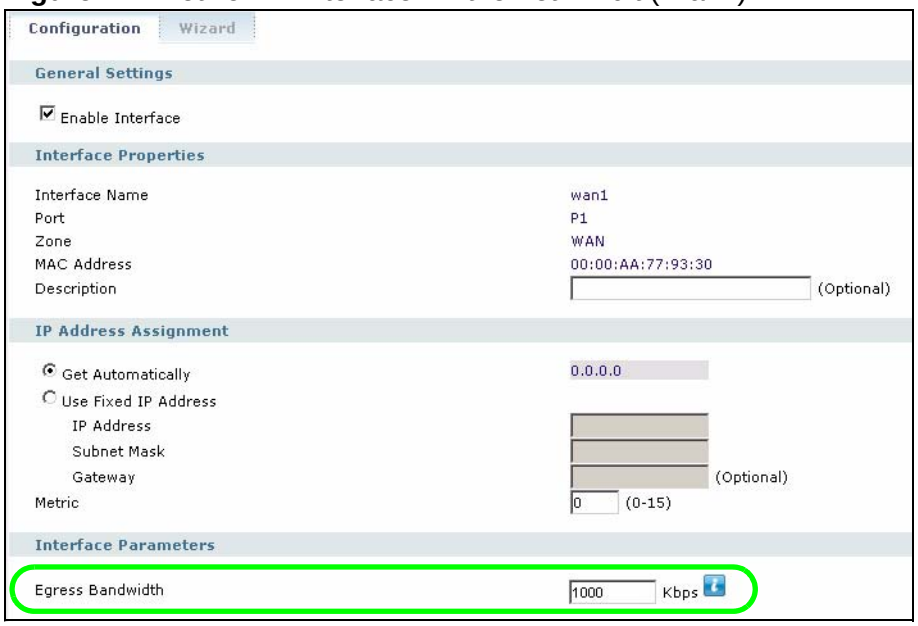

You do not have to change many of the ZyWALL's settings from the defaults to set up this trunk. You only have to set up the outgoing bandwidth on each of the WAN interfaces and configure the WAN_TRUNK trunk's load balancing settings.

## 6.3.1 Set Up Available Bandwidth on Ethernet Interfaces

Here is how to set a limit on how much traffic the ZyWALL tries to send out through each WAN interface.

1 Click **Network > Interface > Ethernet** and the **wan1 Edit** icon. Enter the available bandwidth (1000 kbps) in the **Egress Bandwidth** field. Click **OK**.

**Figure 47** Network > Interface > Ethernet > Edit ( wan1)




2 Repeat the process to set the egress bandwidth for **ge3** to (512 Kbps).

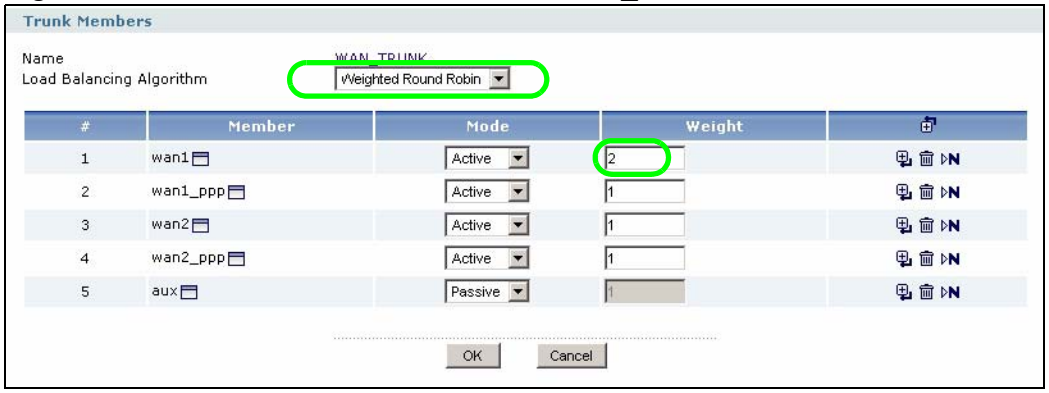
## 6.3.2 Configure the WAN Trunk

1 Click **Network > Interface > Trunk**. Click the **WAN_TRUNK Edit** icon.

2 In the **Load Balancing Algorithm** field, select **Spillover**. After the screen refreshes, click the **Add** icon at the top of the right-hand column.

3 In the **Load Balancing Algorithm** field, select **Weighted Round Robin**. After the screen refreshes, enter 2 in the **Weight** column for **wan1**. Click **OK**.

**Figure 48** Network > Interface > Trunk > WAN_TRUNK > Edit



# 6.4 How to Set Up a WLAN Interface

You can install a wireless LAN card (IEEE 802.11b/g) in the PCIMCIA slot (see Table 275 on page 835 for the supported cards). You can configure different interfaces to use on the wireless LAN card. This lets you have different wireless LAN networks using different SSIDs. You can configure the WLAN interfaces before or after you install the wireless LAN card. This example shows how to create a WLAN interface that uses WPA or WPA2 security and the ZyWALL's local user database for authentication.

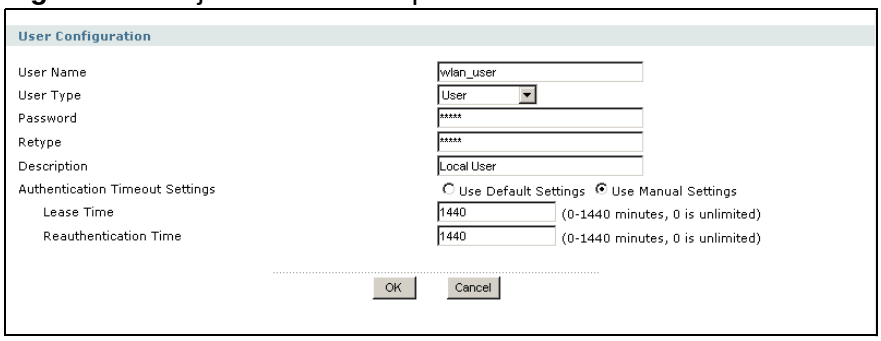
## 6.4.1 Set Up User Accounts

The ZyWALL supports TTLS using PAP so you can use the ZyWALL's local user database with WPA or WPA2 instead of needing an external RADIUS server. For each WLAN user, set up a user account containing the user name and password the WLAN user needs to enter to connect to the wireless LAN.

1 Click **Object > User/Group > User** and the **Add wlan_user Edit** icon.

2 Set the **User Name** to **wlan_user**. Enter (and re-enter) the user's password. Click **OK**.

**Figure 49** Object > User/Group > User > Add




3 Use the **Add** icon in the **Object > User/Group > User** screen to set up the remaining user accounts in similar fashion.

## 6.4.2 Create the WLAN Interface

1 Click **Network > Interface > WLAN > Add** to open the **WLAN Edit** screen.

2 Edit this screen as follows.

A (internal) name for the WLAN interface displays. You can modify it if you want to.

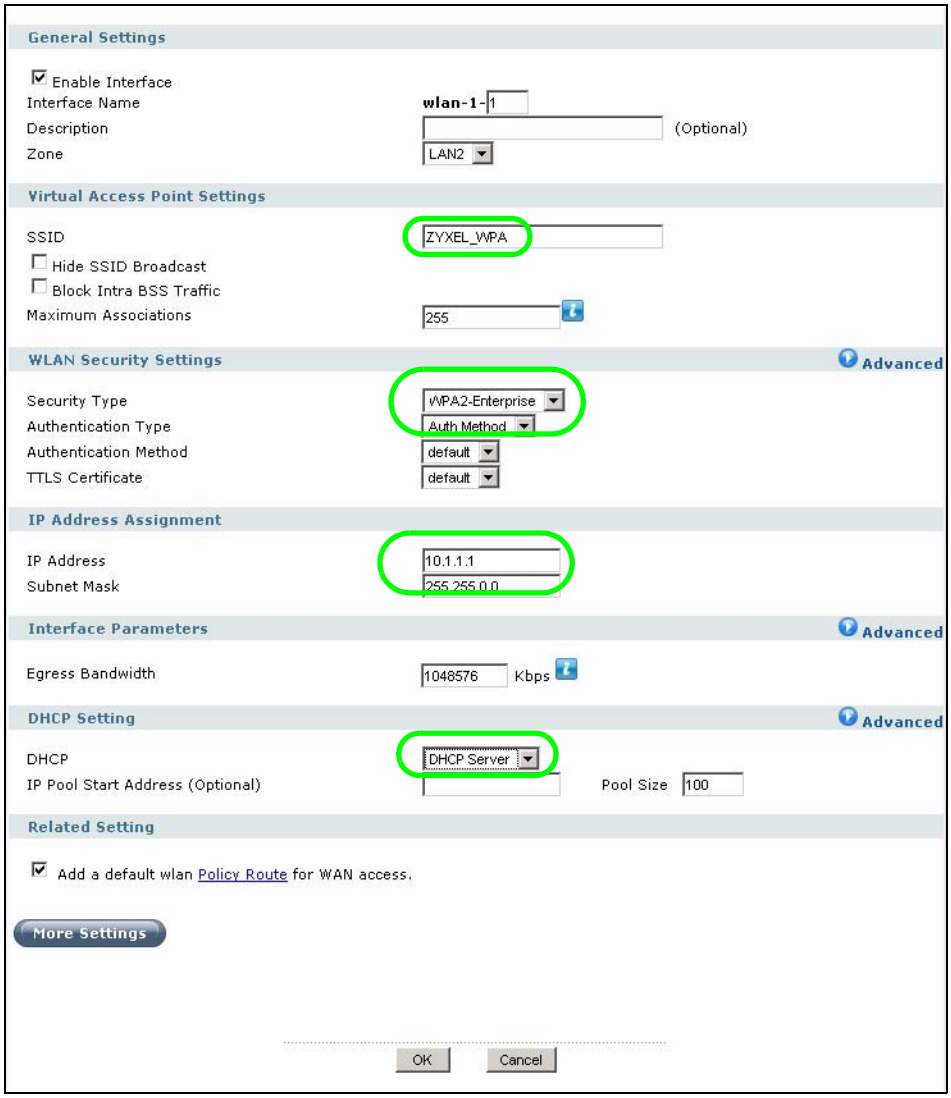
The ZyWALL's security settings are configured by zones. Select to which security zone you want the WLAN interface to belong (the WLAN zone in this example). This determines which security settings the ZyWALL applies to the WLAN interface.

Configure the **SSID** (ZYXEL_WPA in this example).

If all of your wireless clients support WPA2, select **WPA2-Enterprise** as the **Security Type**, otherwise select **WPA-Enterprise**. Set the **Authentication Type** to **Auth Method**. The ZyWALL can use its default authentication method (the local user database) and its default certificate to authenticate the users.

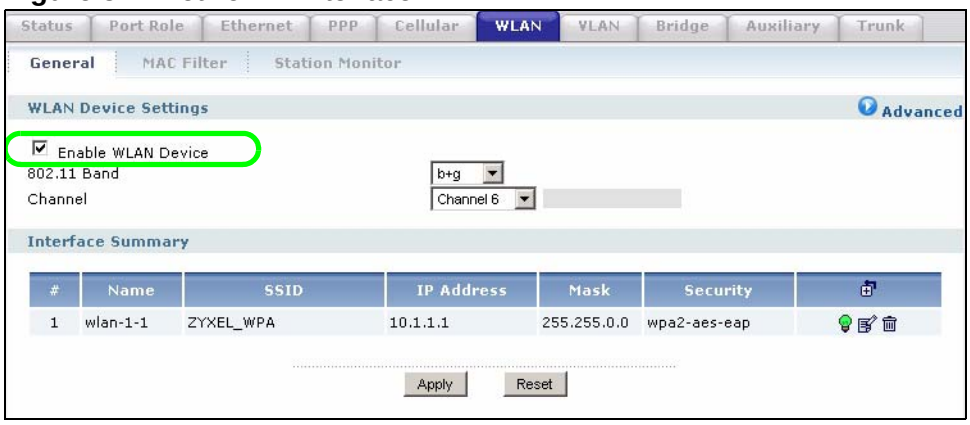
Configure the interface's IP address and set it to **DHCP Server**. Click **OK**.

**Figure 50** Network > Interface > WLAN > Add (WPA/WPA2 Security)



3 Turn on the wireless LAN and click **Apply**.

**Figure 51** Network > Interface > WLAN




## 6.4.3 Set Up the Wireless Clients to Use the WLAN Interface

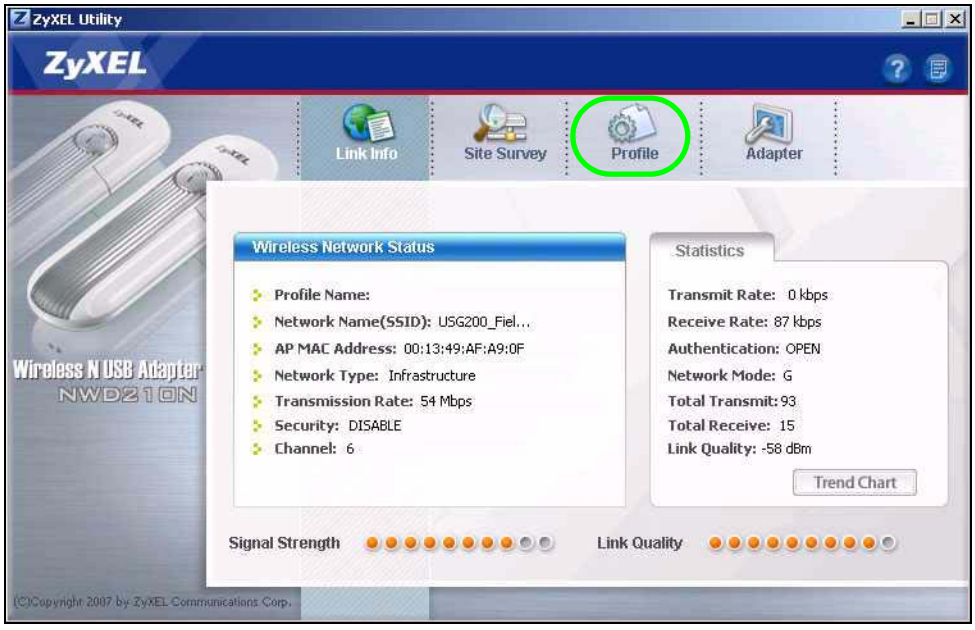
The following sections show you how to have a wireless client (not included with the ZyWALL) use the wireless network.

### 6.4.3.1 Configure the ZyXEL Wireless Client Utility

This example shows how to configure ZyXEL's wireless client utility (not included with the ZyWALL) to use the WLAN interface. See Section 6.4.3.2 on page 116 instead for how to use Funk Odyssey's wireless client software if you want the wireless client to validate the ZyWALL's certificate (for added protection against connecting to a rogue AP).

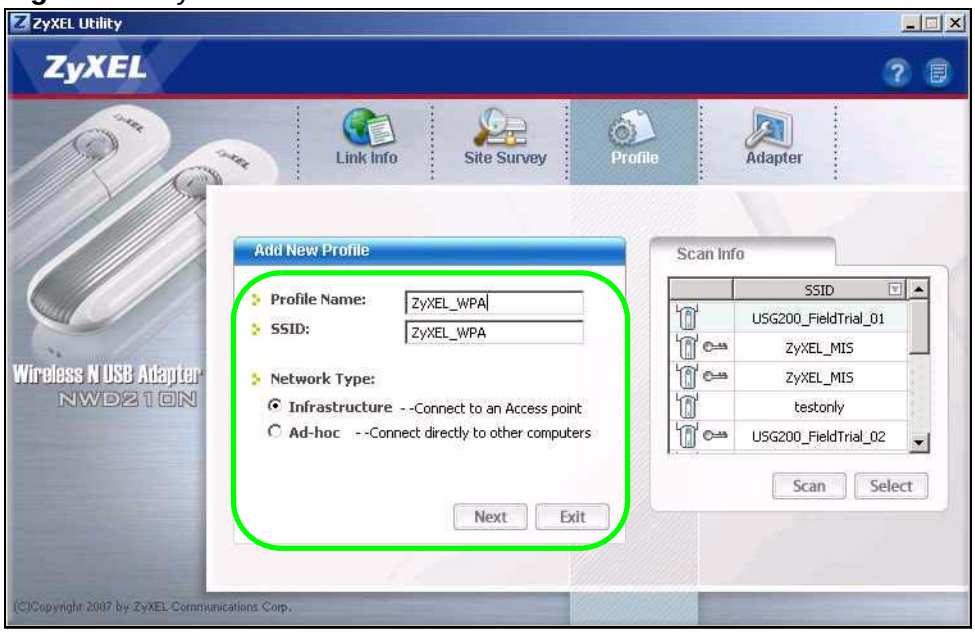
1 Open the wireless client utility and click **Profile**.

**Figure 52** ZyXEL Wireless Client



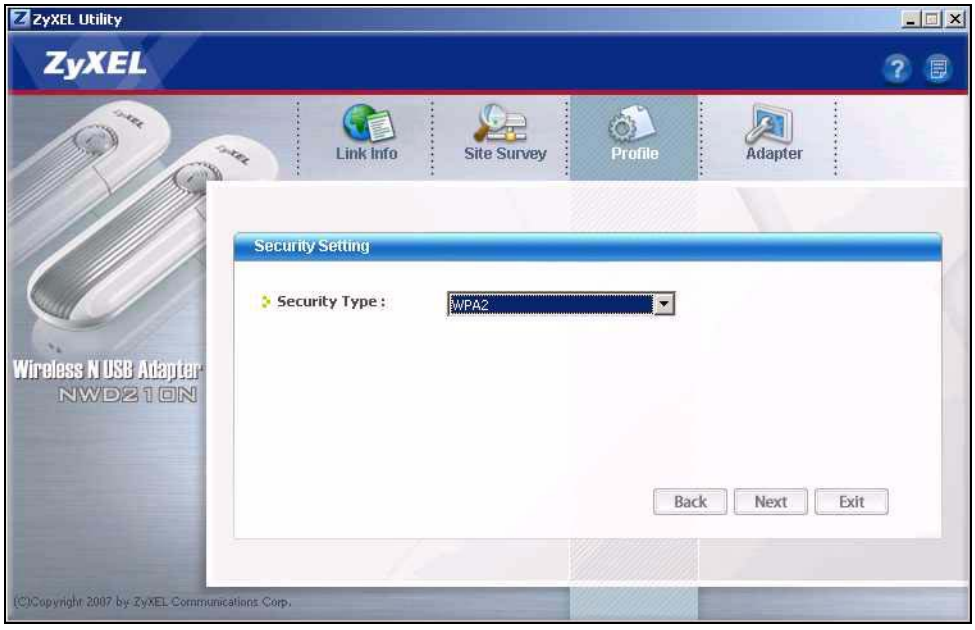

2 Add a new profile. This example uses “ZYXEL_WPA” as the name. It is also the SSID (name) of the wireless network. Select **Infrastructure** and click **Next**.

**Figure 53** ZyXEL Wireless Client > Profile



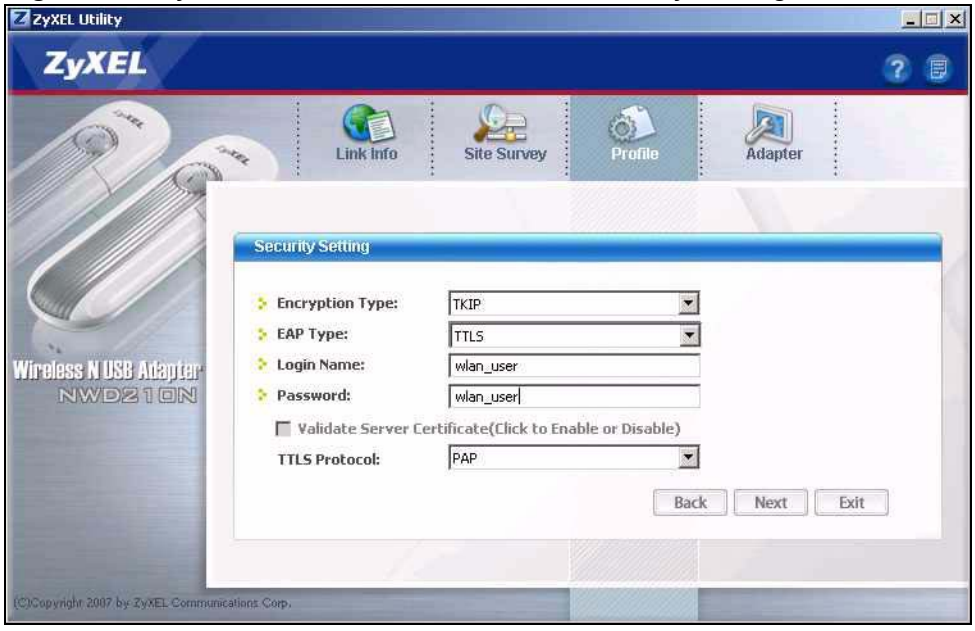
3 Select **WPA2** as the security type and click **Next**.

**Figure 54** ZyXEL Wireless Client > Profile: Security Type



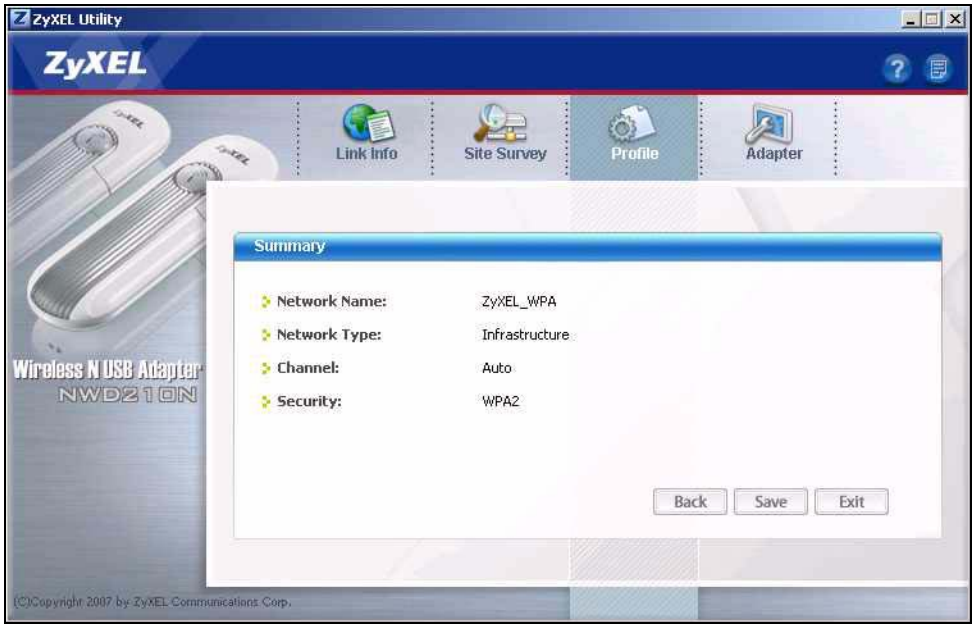

4 Set the encryption type to **TKIP** and the EAP type to **TTLS**. Configure **wlan_user** as the **Login Name** and enter the account's password (also **wlan_user** in this example. In **TTLS Protocol**, select **PAP**. Click **Next**.

**Figure 55** ZyXEL Wireless Client > Profile: Security Settings



5 Confirm your settings and click **Save**.

**Figure 56** ZyXEL Wireless Client > Profile: Save

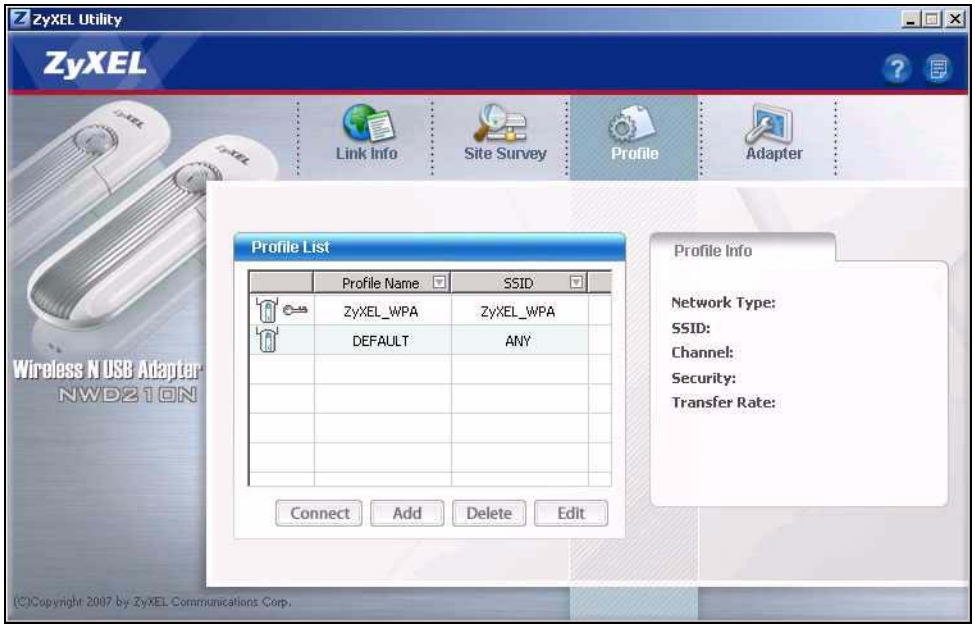



6 Click **Activate Now**.

**Figure 57** ZyXEL Wireless Client > Profile: Activate

7 The **ZYXEL_WPA** profile displays in your list of profiles.

**Figure 58** ZyXEL Wireless Client > Profile: Activate



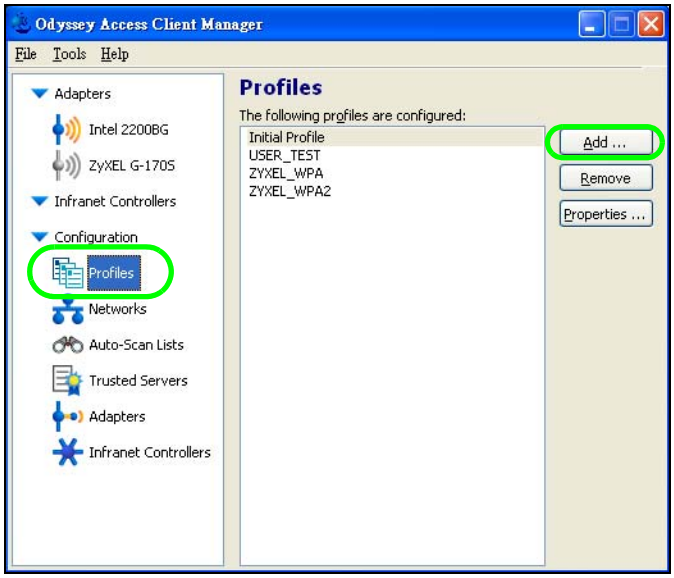

Since the ZyXEL utility does not have the wireless client validate the ZyWALL's certificate, you can go to Section 6.4.3.4 on page 123.

## 6.4.3.2 Configure the Funk Odyssey Wireless Client

This example shows how to configure Funk's Odyssey Access Client Manager wireless client software (not included with the ZyWALL) to use the WLAN interface.

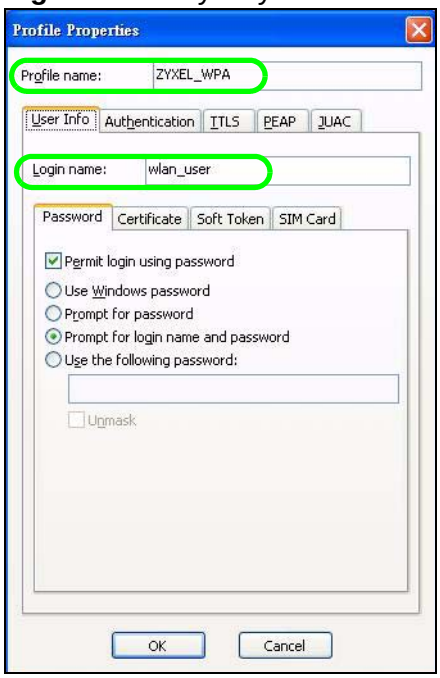
1 Open the Odyssey wireless client software and click **Profiles > Add**.

**Figure 59** Odyssey Access Client Manager > Profiles



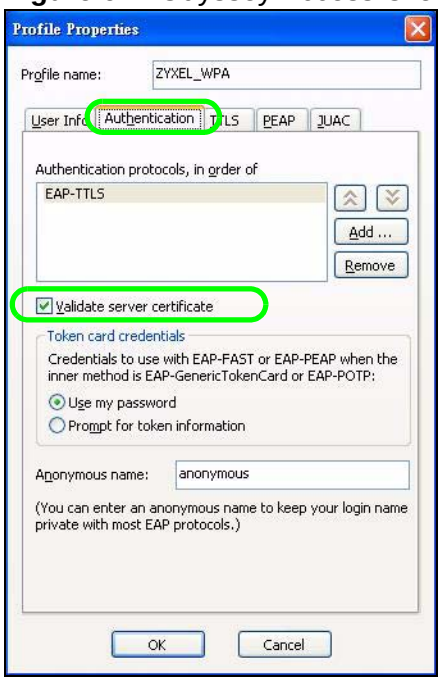
2 Name the profile (this example uses **ZYXEL_WPA**). In the **User Info** tab, configure **wlan_user** as the **Login name**. In the **Password** sub-tab, select **Prompt for long name and password**.

**Figure 60** Odyssey Access Client Manager > Profiles > User Info




3 Click the **Authentication** tab and select **Validate server certificate**.

**Figure 61** Odyssey Access Client Manager > Profiles > Authentication

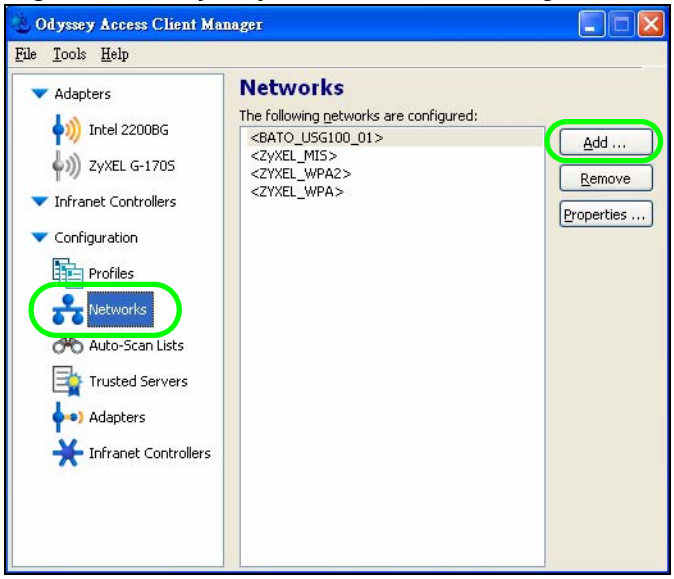


4 Click the **TTLS** tab and select **PAP**. Then click **OK**.

**Figure 62** Odyssey Access Client Manager > Profiles > Authentication

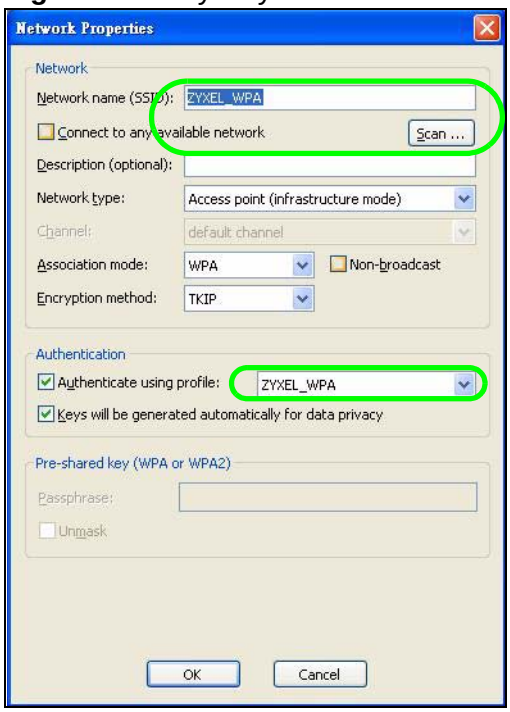

5 Click **Networks > Add**.

**Figure 63** Odyssey Access Client Manager > Networks



6 Enter the name of the wireless network (“ZYXEL_WPA” in this example) or click **Scan** to look for it. Then select **Authenticate using profile** and select the profile you configured (“ZYXEL_WPA” in this example). Click **OK**.

**Figure 64** Odyssey Access Client Manager > Networks > Add



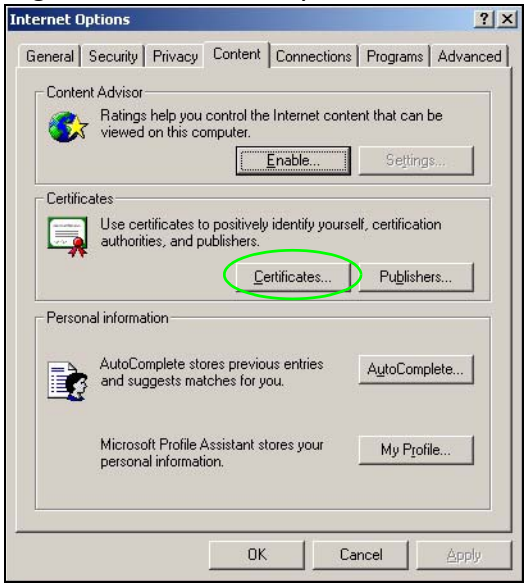

Use the next section to import the ZyWALL’s certificate into the wireless client.

### 6.4.3.3 Wireless Clients Import the ZyWALL’s Certificate

You must import the ZyWALL’s certificate into the wireless clients if they are to validate the ZyWALL’s certificate. Use the **My Certificate Edit** screen (see Section 43.2.2 on page 709) to export the certificate the ZyWALL is using for the WLAN interface. Then do the following to import the certificate into each wireless client.

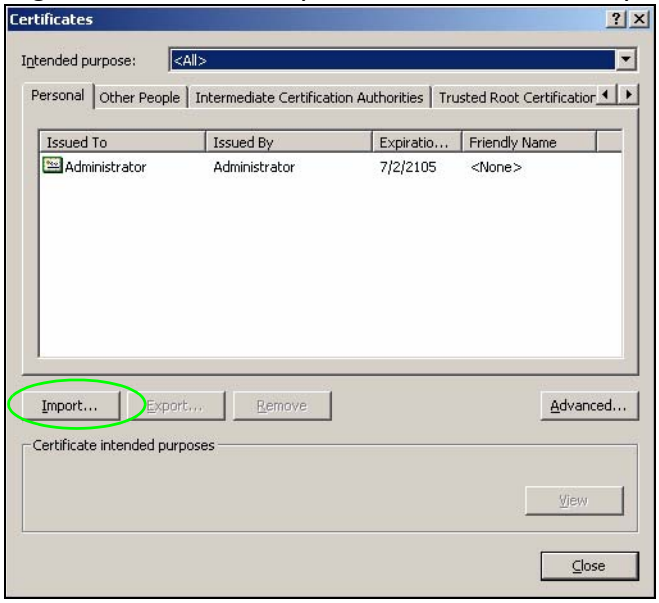
1 In Internet Explorer, click **Tools > Internet Options > Content** and click the **Certificates** button.

**Figure 65** Internet Explorer: Tools > Internet Options > Content



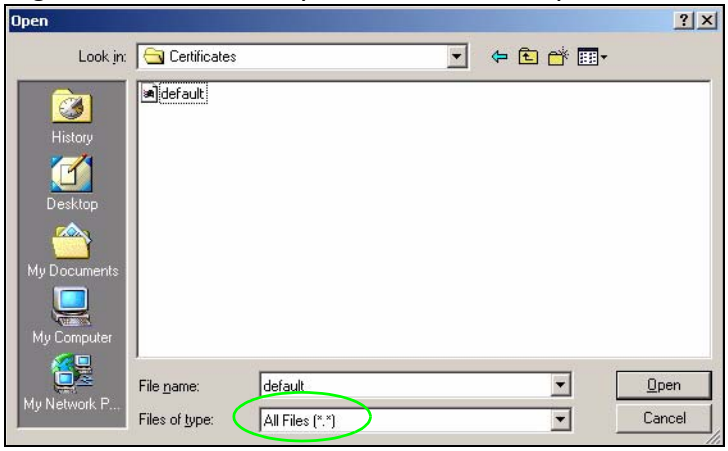

2 Click **Import**.

**Figure 66** Internet Explorer: Tools > Internet Options > Content > Certificates



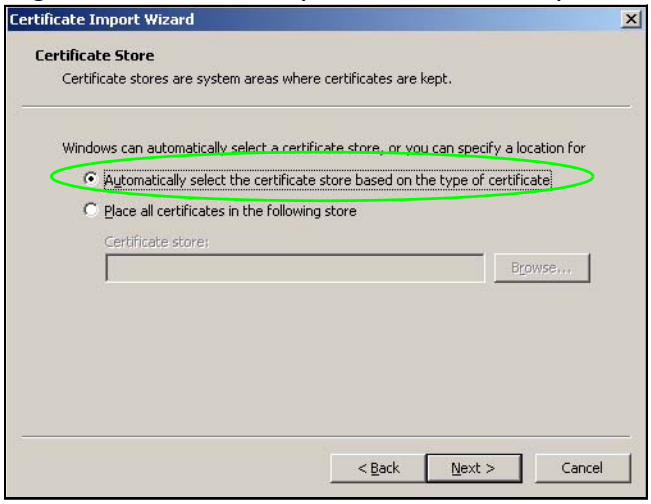
3 Use the wizard screens to import the certificate. You may need to change the **Files of Type** setting to **All Files** in order to see the certificate file.

**Figure 67** Internet Explorer Certificate Import Wizard File Open Screen



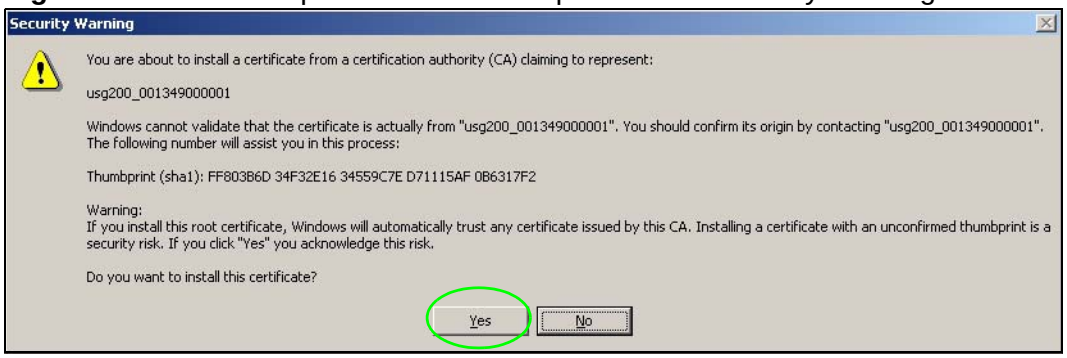

4 When you get to the **Certificate Store** screen, you can just leave it at the default setting.

**Figure 68** Internet Explorer Certificate Import Wizard Certificate Store Screen



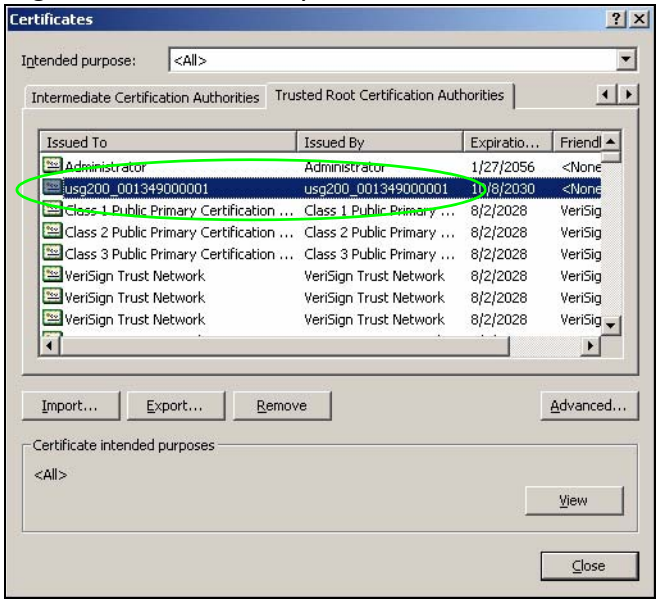

5 If you get a security warning screen, click **Yes** to proceed.

**Figure 69** Internet Explorer Certificate Import Wizard Security Warning Screen



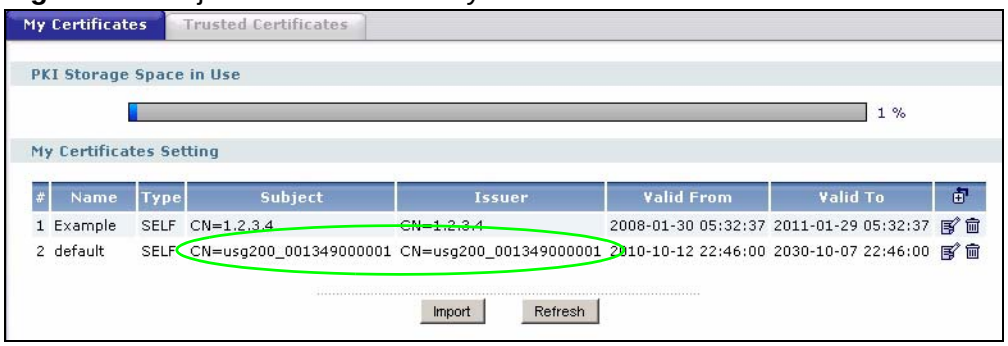
6 The **Internet Explorer Certificates** screen remains open after the import is done. You can see the newly imported certificate listed in the **Trusted Root Certification Authorities** tab. The values in the **Issued To** and **Issued By** fields should match those in the ZyWALL's **My Certificates** screen's **Subject** and **Issuer** fields (respectively).

**Figure 70** Internet Explorer: Trusted Root Certification Authorities




As shown here, the **My Certificates** screen uses a prefix, followed by a hyphen, to indicate what type of information is being displayed, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).

**Figure 71** Object > Certificate > My Certificates




Repeat the steps to import the certificate into each wireless client that is to validate the ZyWALL's certificate when using the WLAN interface.

### 6.4.3.4 Wireless Clients Use the WLAN Interface

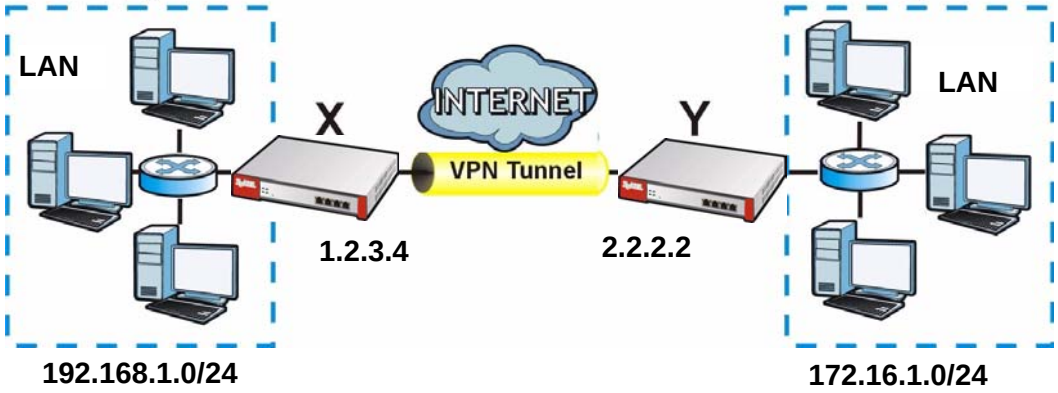
A login screen displays when the wireless client attempts to connect to the wireless interface. Enter the username and password and click **OK**.

**Figure 72** Funk Odyssey Access Wireless Client Login Example


# 6.5 How to Set Up an IPSec VPN Tunnel

This example shows how to create the following VPN tunnel.

**Figure 73** VPN Example




In this example, the ZyWALL is router **X** (1.2.3.4), and the remote IPSec router is router **Y** (2.2.2.2). Create the VPN tunnel between ZyWALL **X**'s LAN subnet (192.168.1.0/24**)** and the LAN subnet behind peer IPSec router **Y** (172.16.1.0/24).

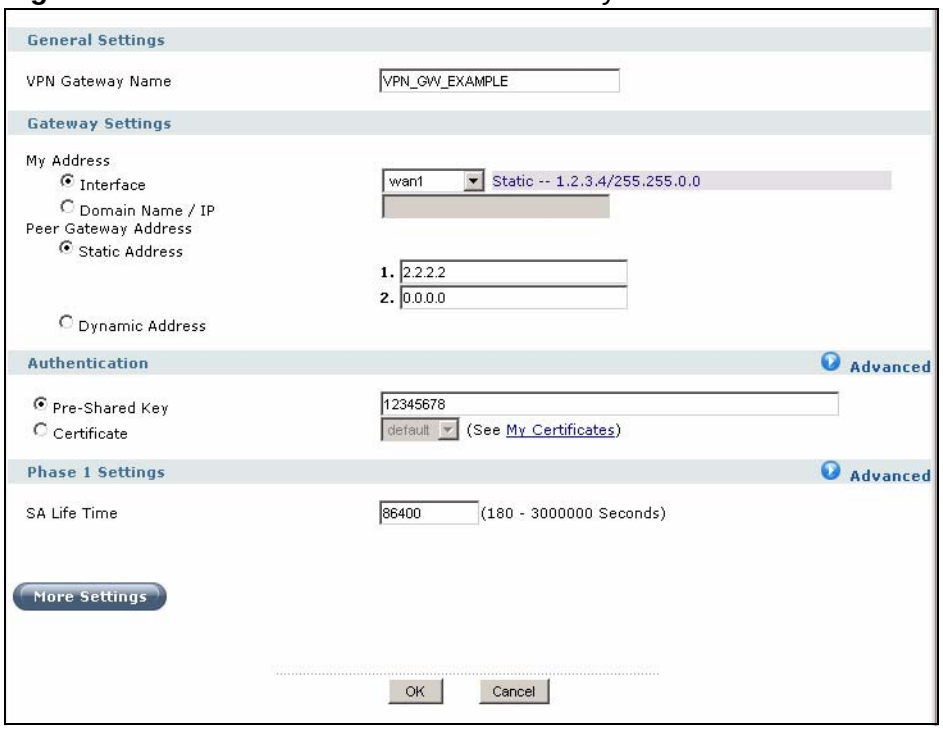
## 6.5.1 Set Up the VPN Gateway

The VPN gateway manages the IKE SA. You do not have to set up any other objects before you configure the VPN gateway because this VPN tunnel does not use any certificates or extended authentication.

1 Click **VPN > IPSec VPN > VPN Gateway**, and then click the **Add** icon.

2 Give the VPN gateway a name (“VPN_GW_EXAMPLE”). For **My Address**, select **Interface** and **wan1**. For the **Peer Gateway Address**, select **Static Address** and enter 2.2.2.2 in field **1**. For the **Authentication**, Select **Pre-Shared Key** and enter 12345678. Click **OK**.

**Figure 74** VPN > IPSec VPN > VPN Gateway > Add



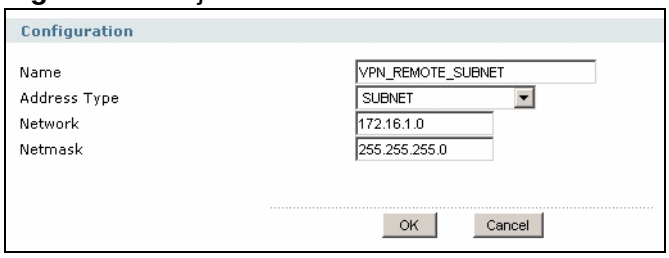

## 6.5.2 Set Up the VPN Connection

The VPN connection manages the IPSec SA. You have to set up the address objects for the local network and remote network before you can set up the VPN connection.

1 Click **Object > Address**. Click the **Add** icon.

2 Give the new address object a name (“VPN_REMOTE_SUBNET”), change the **Address Type** to **SUBNET**. Set up the **Network** field to 172.16.1.0 and the **Netmask** to 255.255.255.0. Click **OK**.

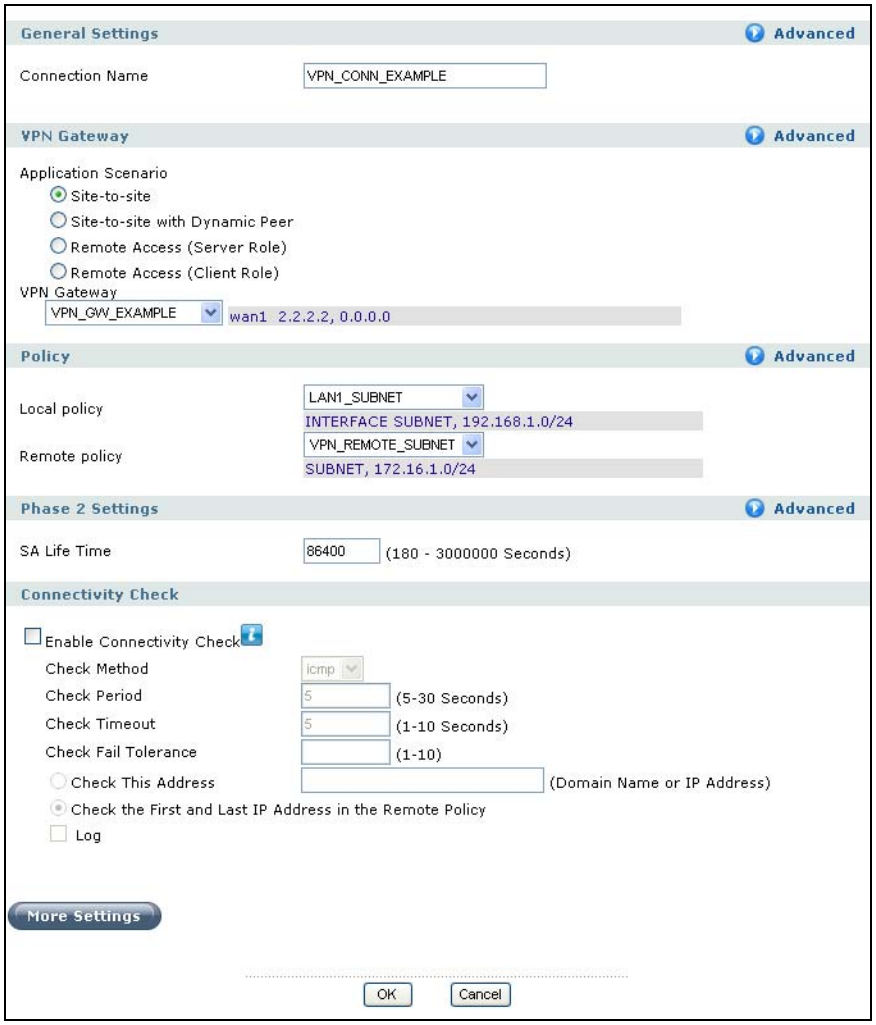
**Figure 75** Object > Address > Add




3 Click **VPN > IPSec VPN > VPN Connection**. Click the **Add** icon.

4 Give the VPN connection a name (“VPN_CONN_EXAMPLE”). Under **VPN Gateway** select **Site-to-site** and the VPN gateway (**VPN_GW_EXAMPLE**). Under **Policy**, select **LAN1_SUBNET** for the local network and **VPN_REMOTE_SUBNET** for the remote. Click **OK**.

**Figure 76** VPN > IPSec VPN > VPN Connection > Add

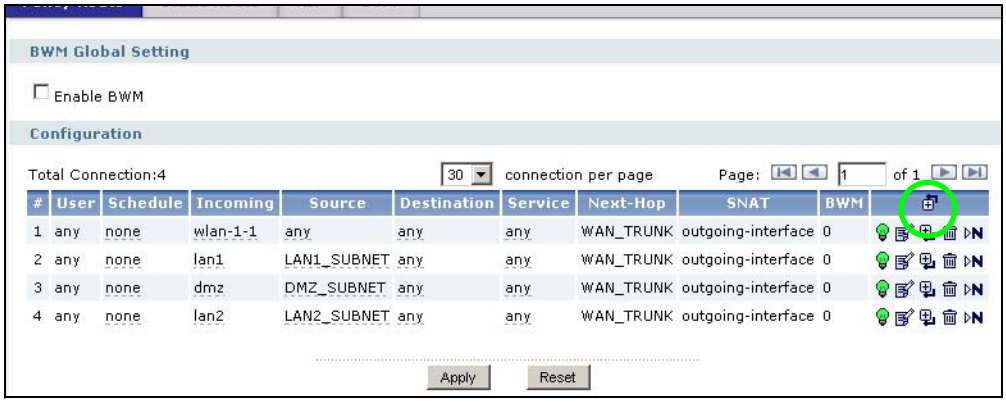


## 6.5.3 Set Up the Policy Route for the VPN Tunnel

Do the following to create a policy route to have the ZyWALL send traffic through the VPN tunnel.

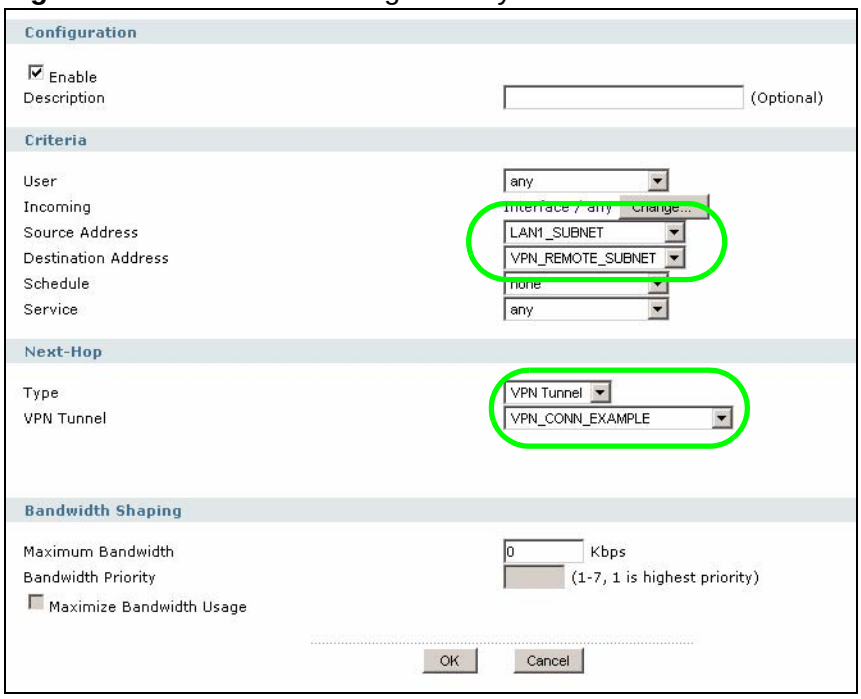
1 Click **Network > Routing > Policy Route**. You want this policy route to have higher priority than the default policy route for the trunk, so click the **Add** icon at the top of the column, not the one next to the existing policy route.

**Figure 77** Network > Routing > Policy Route




2 Configure the policy route as shown next. This policy route applies to traffic from the LAN1 subnet. Use the VPN connection's local and remote objects as the source address and destination address objects here. The next-hop is the VPN connection that you created. Click **OK**.

**Figure 78** Network > Routing > Policy Route > Add



3 Now set up the VPN settings on the peer IPSec router and try to establish the VPN tunnel. To trigger the VPN, either try to connect to a device on the peer IPSec router's LAN or click **VPN > IPSec VPN > VPN Connection** and use the VPN connection screen's **Connect** icon.

### 6.5.4 Configure Security Policies for the VPN Tunnel

You configure security policies based on zones. The new VPN connection was assigned to the IPSec_VPN zone. By default, there are no security restrictions on the IPSec_VPN zone, so, next, you should set up security policies (firewall rules, IDP, and so on) that apply to the IPSec_VPN zone. Make sure all firewalls between the ZyWALL and remote IPSec router allow UDP port 500 (IKE) and IP protocol 50 (AH) or 51 (ESP). If you enable NAT traversal, all firewalls between the ZyWALL and remote IPSec router should also allow UDP port 4500.

## 6.6 How to Configure User-aware Access Control

You can configure many policies and security settings for specific users or groups of users. This is illustrated in the following example, where you will set up the following policies. This is a simple example that does not include priorities for different types of traffic. See Bandwidth Management on page 479 for more on bandwidth management.

**Table 29** User-aware Access Control Example

| GROUP (USER) | WEB SURFING | WEB BANDWIDTH | MSN | LAN-TO-DMZ ACCESS |
|---|---|---|---|---|
| Finance (Leo) | Yes | 200K | No | Yes |
| Engineer (Steven) | Yes | 100K | No | No |
| Sales (Debbie) | Yes | 100K | Yes (M-F, 08:30~18:00) | Yes |
| Boss (Andy) | Yes | 100K | Yes | Yes |
| Guest (guest) | Yes | 50K | No | No |
| Others | No | --- | No | No |

The users are authenticated by an external RADIUS server at 192.168.1.200.

First, set up the user accounts and user groups in the ZyWALL. Then, set up user authentication using the RADIUS server. Finally, set up the policies in the table above.

The ZyWALL has its default settings.

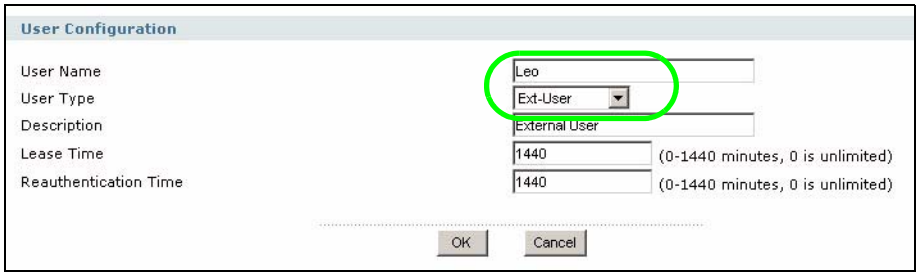
## 6.6.1 Set Up User Accounts

Set up one user account for each user account in the RADIUS server. If it is possible to export user names from the RADIUS server to a text file, then you might create a script to create the user accounts instead. This example uses the Web Configurator.

1 Click **Object > User/Group > User**. Click the **Add** icon.

2 Enter the same user name that is used in the RADIUS server, and set the **User Type** to **Ext-User** because this user account is authenticated by an external server. Click **OK**.

**Figure 79** Object > User/Group > User > Add




3 Repeat this process to set up the remaining user accounts.

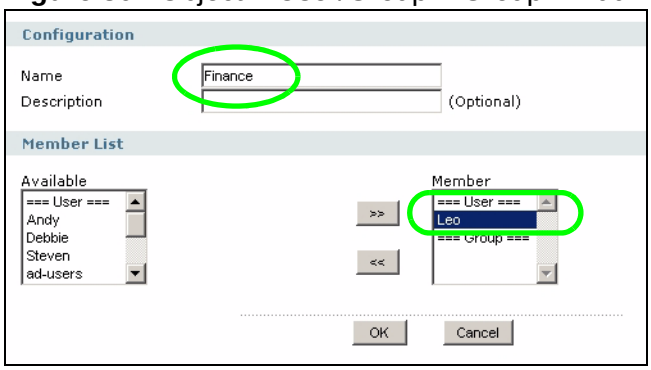
## 6.6.2 Set Up User Groups

Set up the user groups and assign the users to the user groups.

1 Click **Object > User/Group > Group**. Click the **Add** icon.

2 Enter the name of the group that is used in Table 29 on page 127. In this example, it is “Finance”. Then, select **User/Leo** and click the right arrow to move him to the **Member** list. This example only has one member in this group, so click **OK**. Of course you could add more members later.

**Figure 80** Object > User/Group > Group > Add



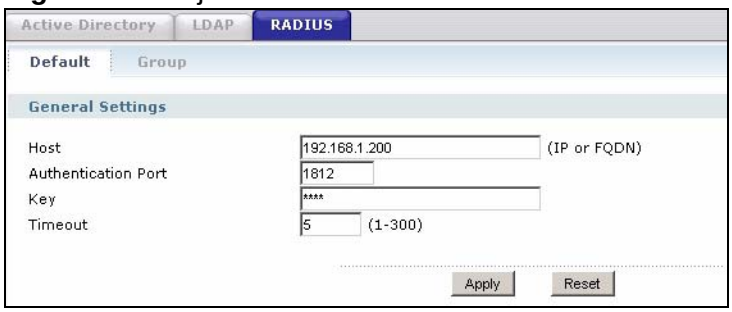
3 Repeat this process to set up the remaining user groups.

## 6.6.3 Set Up User Authentication Using the RADIUS Server

This step sets up user authentication using the RADIUS server. First, configure the settings for the RADIUS server. Then, set up the authentication method, and configure the ZyWALL to use the authentication method. Finally, force users to log in to the ZyWALL before it routes traffic for them.

1 Click **Object > AAA Server > RADIUS > Default**. Configure the RADIUS server, and click **Apply**.

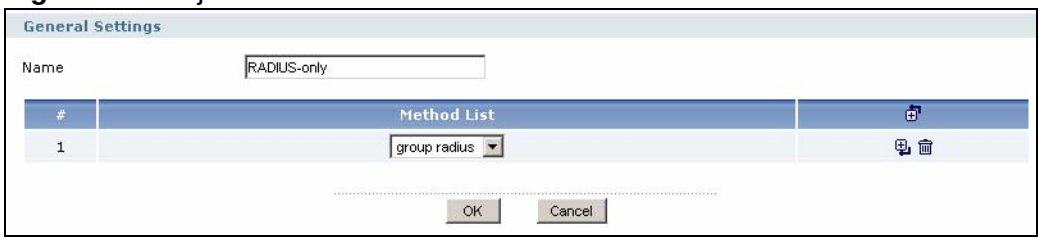
**Figure 81** Object > AAA Server > RADIUS > Default




2 Click **Object > Auth. method**. Click the **Add** icon.

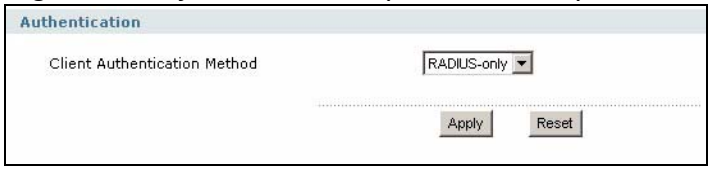
3 Give the new authentication method object a descriptive name, and click the **Add** icon. Select **group radius** because the ZyWALL should use the specified RADIUS server for authentication. Click **OK**.

**Figure 82** Object > Auth. method > Add




4 Click **System > WWW**. In the **Authentication** section, select the new authentication method in the **Client Authentication Method** field. Click **Apply**.

**Figure 83** System > WWW (Authentication)

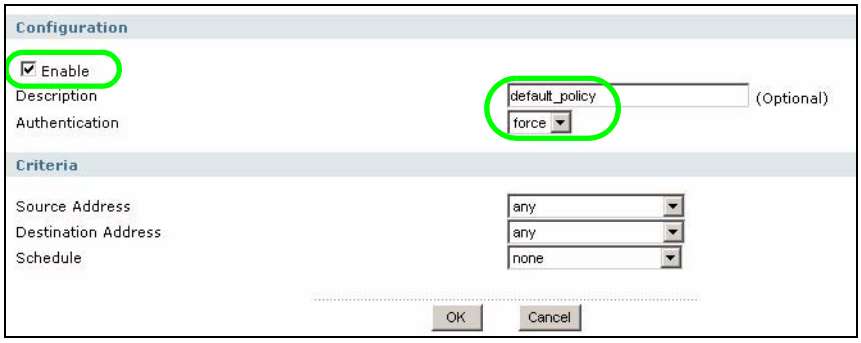



5 Click **Object > User/Group > Setting**. In the **Force User Authentication Policy** section, click the **Add** icon.

6 Set up a default policy that forces every user to log in to the ZyWALL before the ZyWALL routes traffic for them. Select **Enable**. Then, select **force** in the **Authentication** field. Keep the rest of the default settings, and click **OK**.

Note: The users will have to log in using the Web Configurator login screen before they can use HTTP or MSN.

**Figure 84** Object > User/Group > Setting > Add (Force User Authentication Policy)



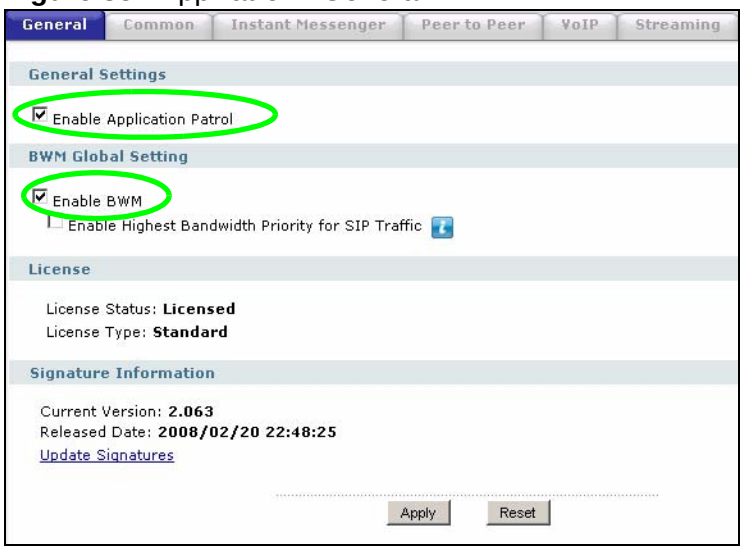

When the users try to browse the web (or use any HTTP/HTTPS application), the **Login** screen appears. They have to log in using the user name and password in the RADIUS server.

## 6.6.4 Set Up Web Surfing Policies With Bandwidth Restrictions

Use application patrol (AppPatrol) to enforce the web surfing and MSN policies. You must have already subscribed for the application patrol service. You can subscribe using the **Licensing > Registration** screens or using one of the wizards.

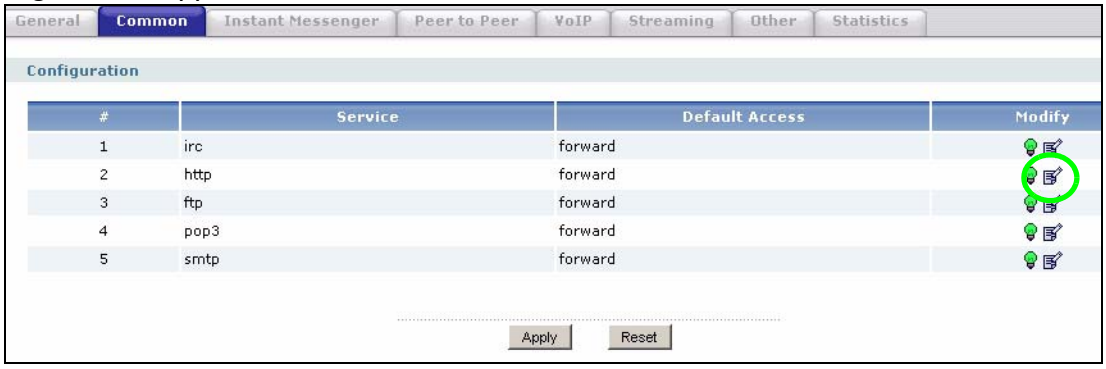
1 Click **AppPatrol**. If application patrol and bandwidth management are not enabled, enable them, and click **Apply**.

**Figure 85** AppPatrol > General



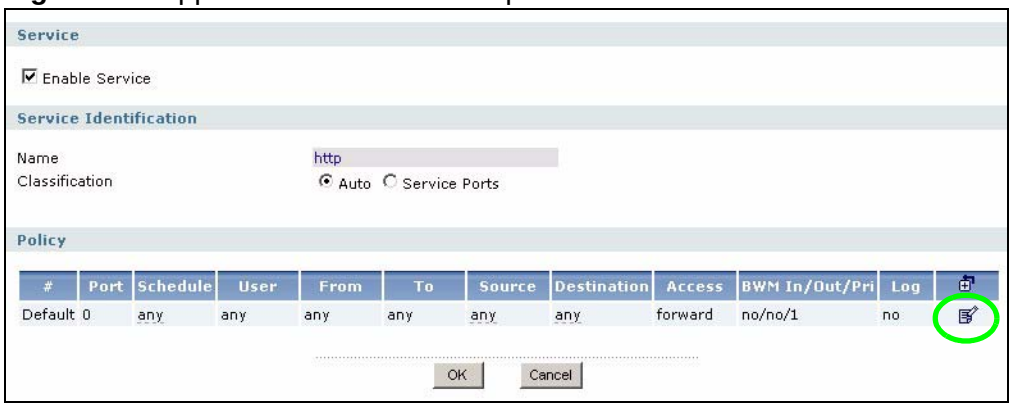

2 Click the **Common** tab and then the **Edit** icon next to the default **http** service.

**Figure 86** AppPatrol > Common



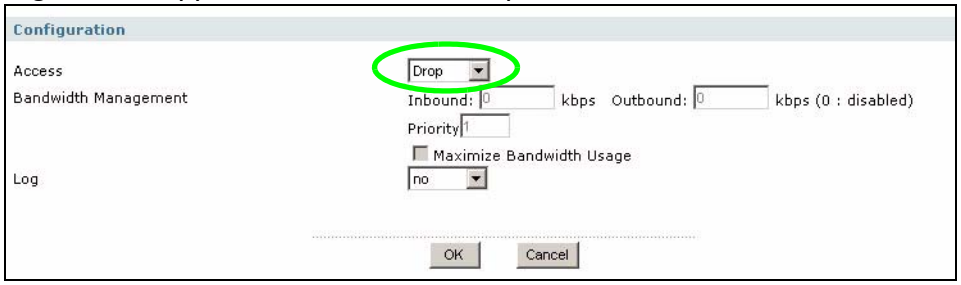

3 Click the **Default** policy's **Edit** icon.

**Figure 87** AppPatrol > Common > http



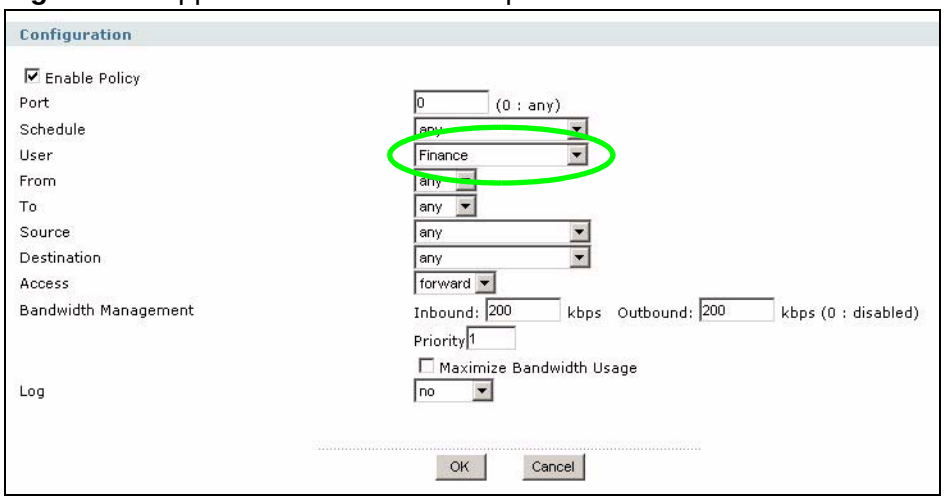
4 Change the access to **Drop** because you do not want anyone except authorized user groups to browse the web. Click **OK**.

**Figure 88** AppPatrol > Common > http > Edit Default




5 Click the **Add** icon in the policy list. In the new policy, select one of the user groups that is allowed to browse the web and set the corresponding bandwidth restriction in the **Inbound** and **Outbound** fields. Click **OK**. Repeat this process to add exceptions for all the other user groups that are allowed to browse the web.

**Figure 89** AppPatrol > Common> http > Edit Default



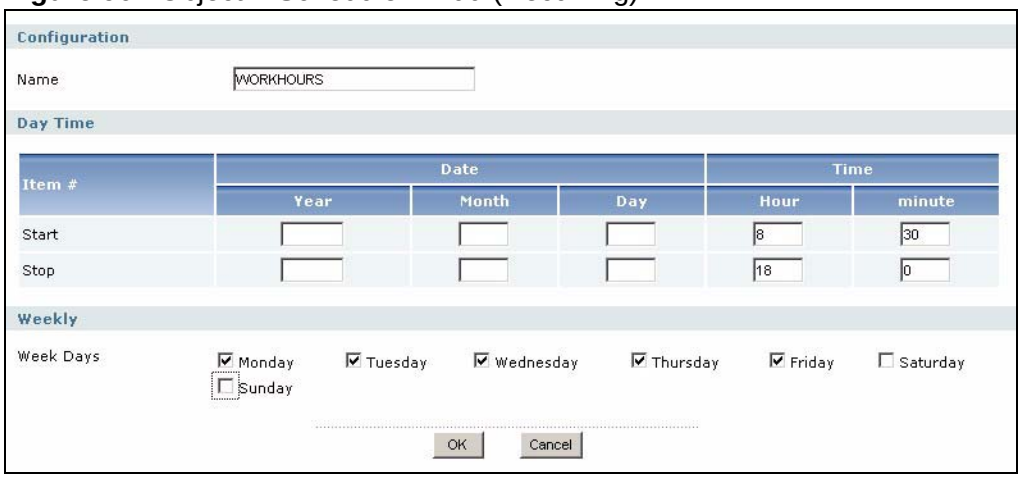

## 6.6.5 Set Up MSN Policies

Set up a recurring schedule object first because Sales can only use MSN during specified times on specified days.

1 Click **Object > Schedule**. Click the **Add** icon for recurring schedules.

2 Give the schedule a descriptive name. Set up the days (Monday through Friday) and the times (8:30 - 18:00) when Sales is allowed to use MSN. Click **OK**.

**Figure 90** Object > Schedule > Add (Recurring)



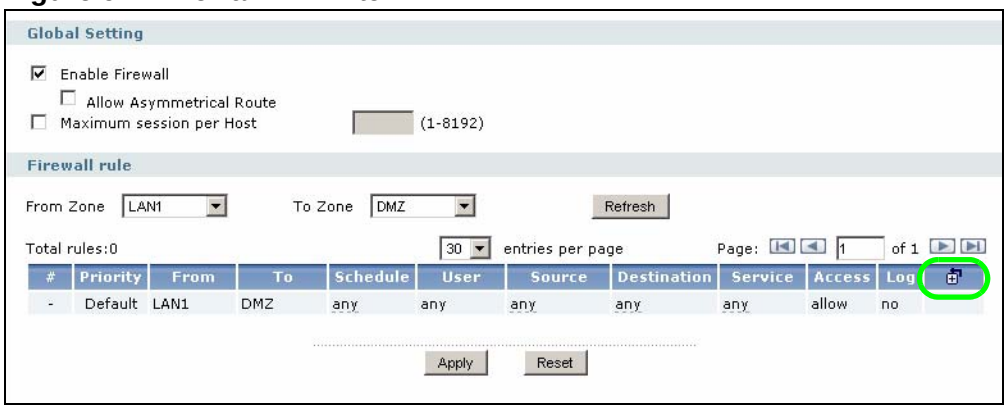

3 Follow the steps in Section 6.6.4 on page 130 to set up the appropriate policies for MSN in application patrol. Make sure to specify the schedule when you configure the policy for the Sales group's MSN access.

## 6.6.6 Set Up Firewall Rules

Use the firewall to control access from LAN to the DMZ.

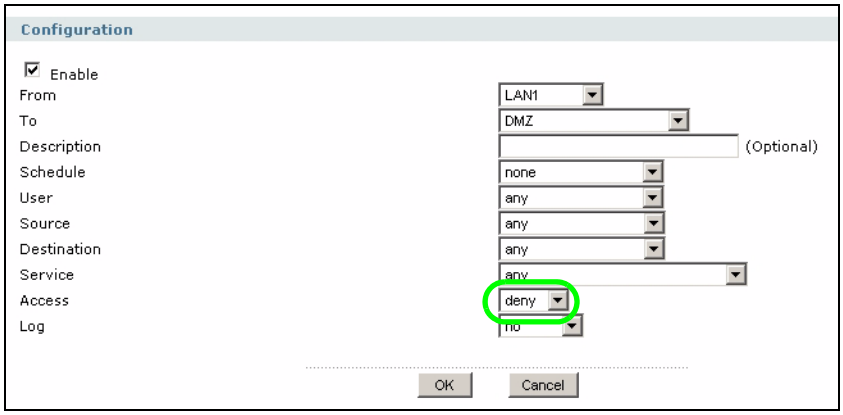
1 Click **Firewall**. In **From Zone**, select **LAN1**; in **To Zone**, select **DMZ** and click **Refresh**. The default rule for LAN1-to-DMZ traffic allows all traffic. You want to limit access to specific groups, so change the default rule first. Click the **Add** icon next to it.

**Figure 91** Firewall > LAN to DMZ



2 Set the **Access** field to **deny**, and click **OK**.

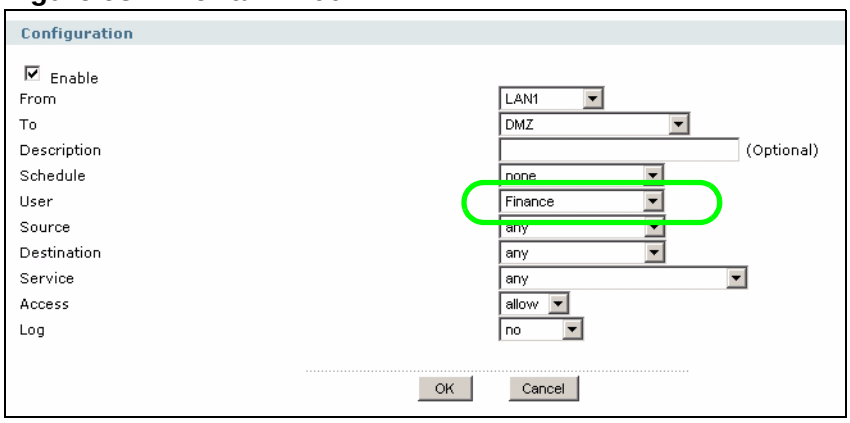
**Figure 92** Firewall > LAN to DMZ > Add




3 Click the **Add** icon at the top of the rule list to create a rule for one of the user groups that is allowed to access the DMZ.

4 Select one of the user groups that is allowed to access the DMZ, and click **OK**.

**Figure 93** Firewall > Add




5 Repeat this process to set up firewall rules for the other user groups that are allowed to access the DMZ.

# 6.7 How to Configure Service Control

Service control lets you configure rules that control HTTP and HTTPS management access (to the Web Configurator) and separate rules that control HTTP and HTTPS user access (logging into SSL VPN for example). See Chapter 45 on page 731 for more on service control.

The To-ZyWALL firewall rules apply to any kind of HTTP or HTTPS connection to the ZyWALL. They do not distinguish between administrator management access and user access. If you configure service control to allow management or user

HTTP or HTTPS access, make sure the firewall is not configured to block that access.

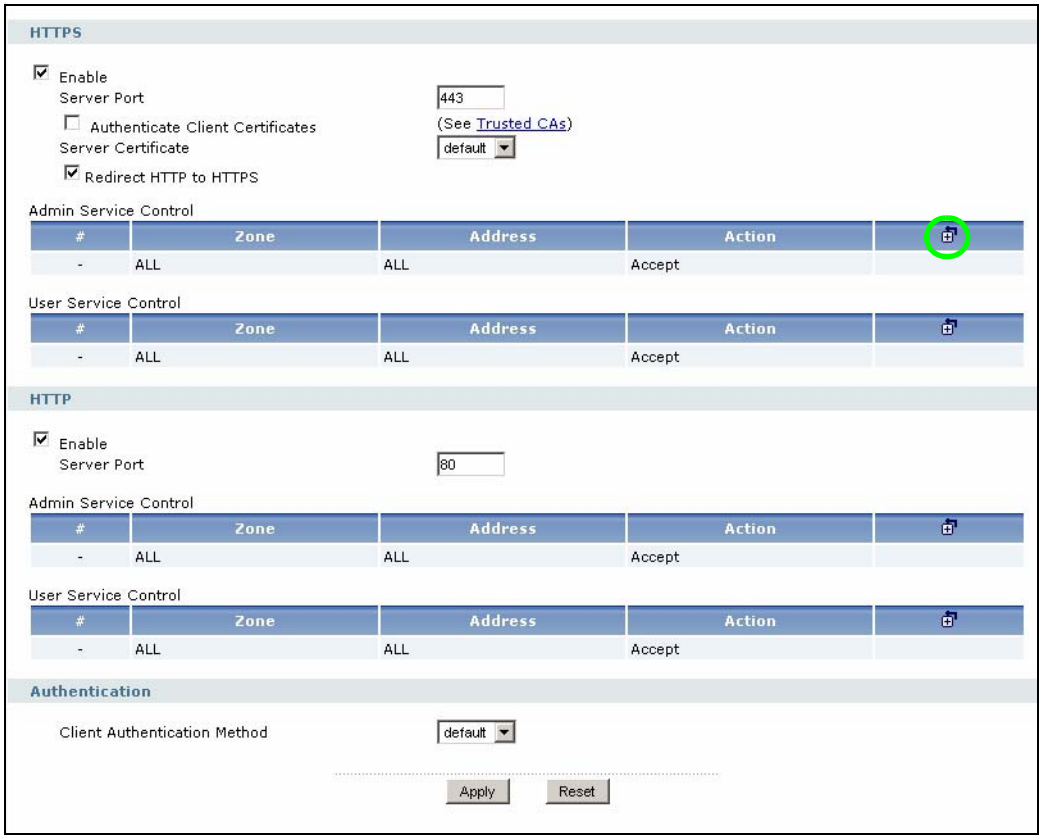
## 6.7.1 Allow HTTPS Administrator Access Only From the LAN

This example configures service control to block administrator HTTPS access from all zones except the LAN1.

1 Click **System > WWW**.

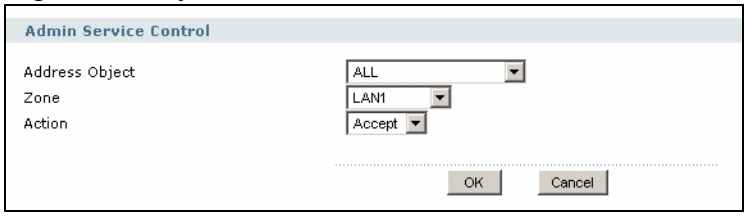
2 In HTTPS **Admin Service Control,** click the **Add** icon.

**Figure 94** System > WWW



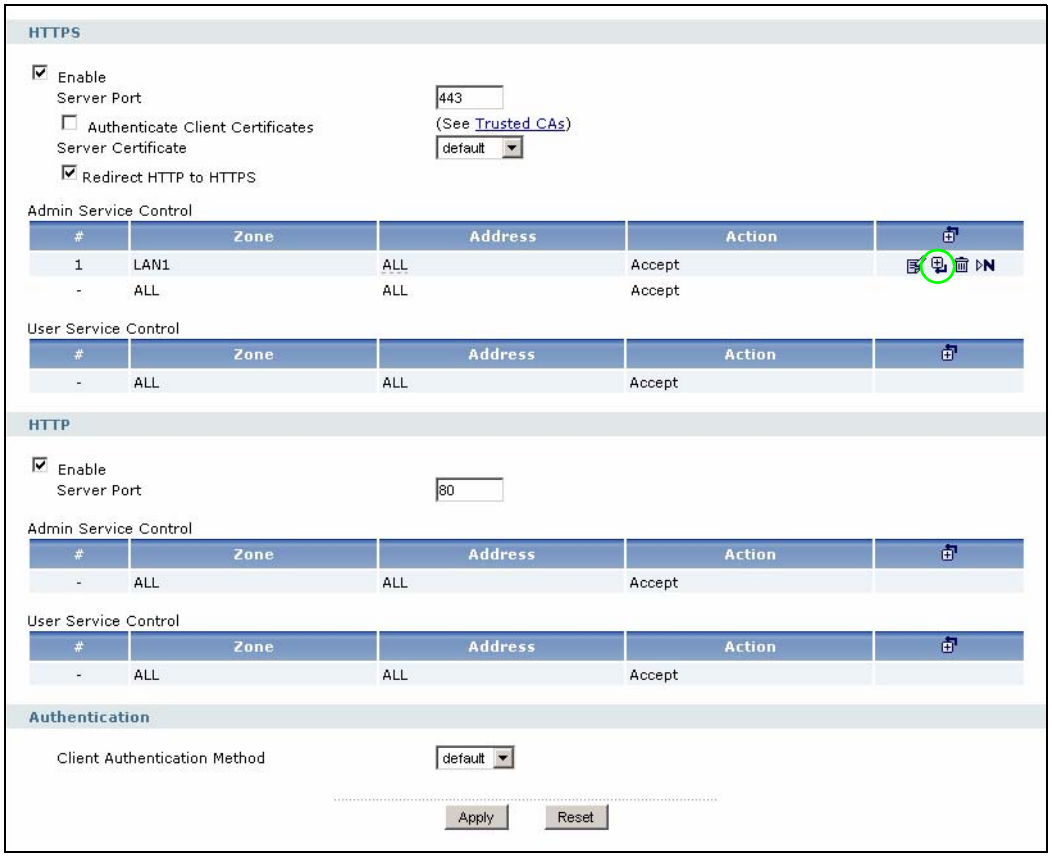

3 In the **Zone** field select **LAN1** and click **OK**.

**Figure 95** System > WWW > Service Control Rule Edit



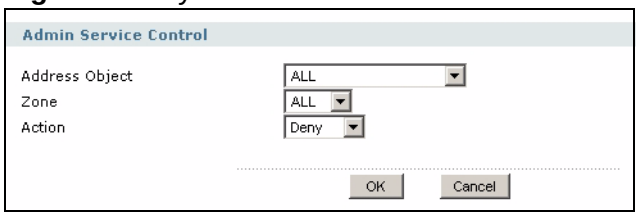
4 Click the new rule's **Add** icon.

**Figure 96** System > WWW (First Example Admin Service Rule Configured)



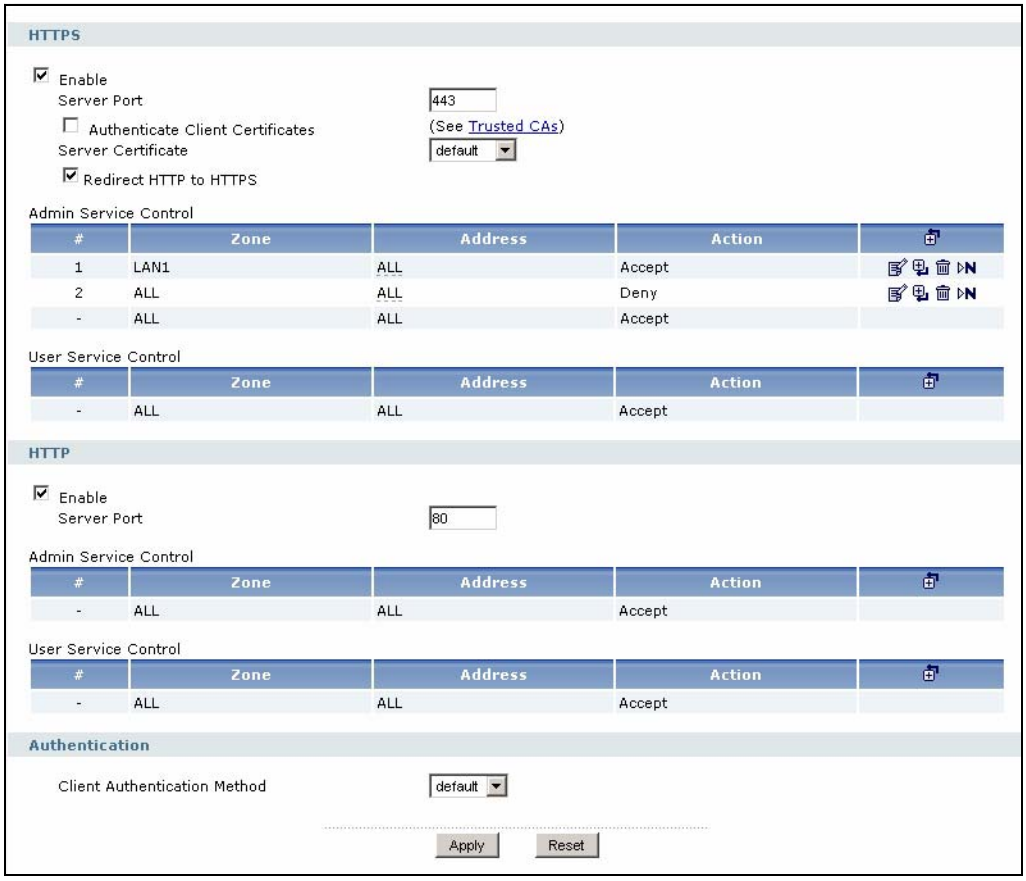

5 In the **Zone** field select **ALL** and set the **Action** to **Deny**. Click **OK**.

**Figure 97** System > WWW > Service Control Rule Edit



6 Click **Apply**.

**Figure 98** System > WWW (Second Example Admin Service Rule Configured)




Now administrator access to the Web Configurator can only come from the LAN1 zone. Non-admin users can still use HTTPS to log into the ZyWALL from any of the ZyWALL's zones (to use SSL VPN for example).

# 6.8 How to Allow Incoming H.323 Peer-to-peer Calls

Suppose you have a H.323 device on the LAN1 for VoIP calls and you want it to be able to receive peer-to-peer calls from the WAN. Here is an example of how to configure virtual server (port forwarding) and firewall rules to have the ZyWALL

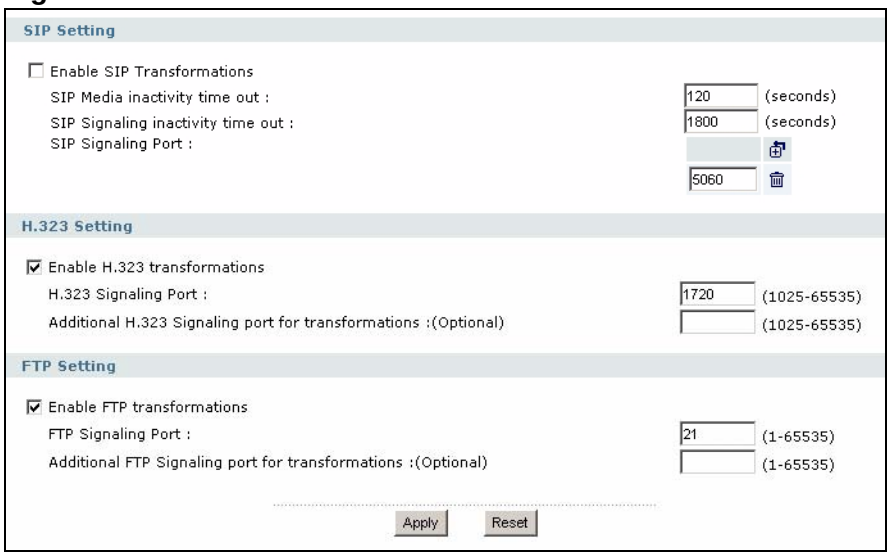
forward H.323 traffic destined for wan1 IP address 10.0.0.8 to a H.323 device located on the LAN and using IP address 192.168.1.56.

**Figure 99** WAN to LAN H.323 Peer-to-peer Calls Example


## 6.8.1 Turn On the ALG

Click **Network > ALG**. Select **Enable H.323 transformations** and click **Apply**.

**Figure 100** Network > ALG

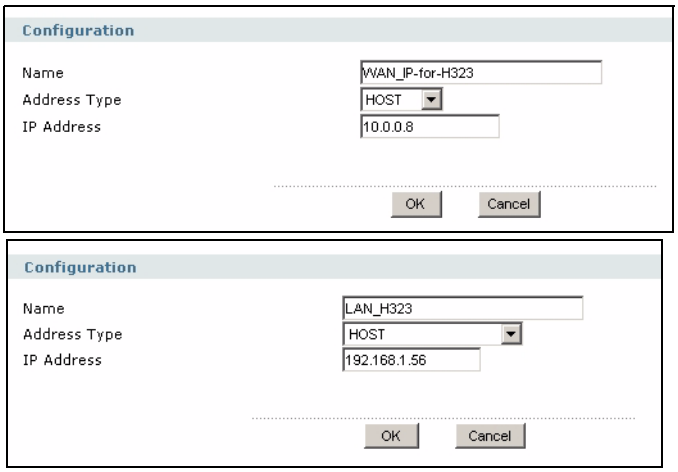



## 6.8.2 Set Up a Virtual Server Policy For H.323

In this example, you need a virtual server policy to forward H.323 (TCP port 1720) traffic received on the ZyWALL's 10.0.0.8 WAN IP address to LAN1 IP address 192.168.1.56.

1 Use **Object > Address > Add** to create address objects for the private and public IP addresses (WAN_IP-for-H323 and LAN_H323) as shown next.

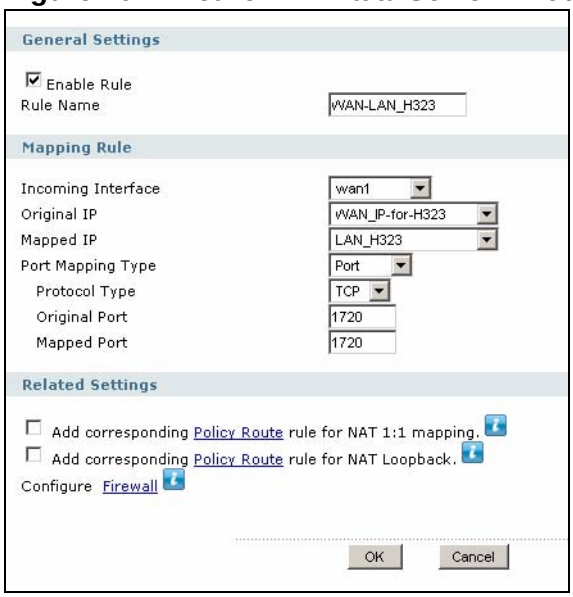
**Figure 101** Create Address Objects




2 Click **Network > Virtual Server > Add.**

3 Configure the screen as follows and click **OK**.

**Figure 102** Network > Virtual Server > Add



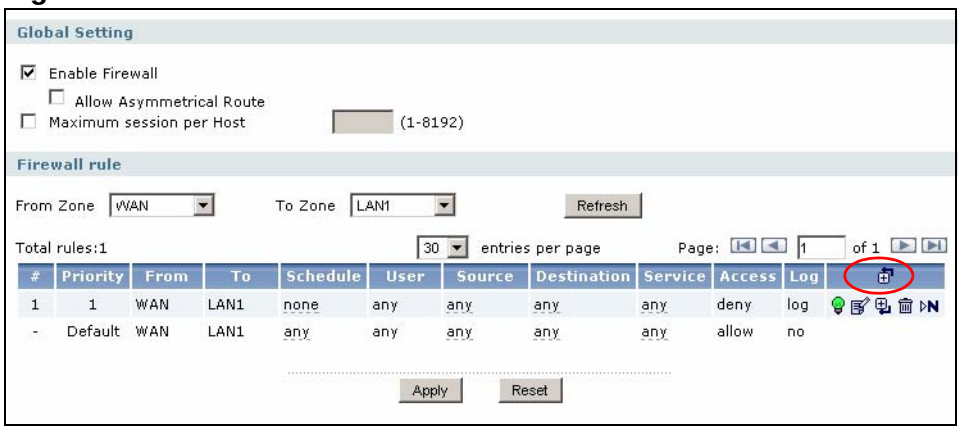

## 6.8.3 Set Up a Firewall Rule For H.323

Here is how to configure a firewall rule to allow H.323 (TCP port 1720) traffic received on the WAN_IP-for-H323 IP address to go to LAN1 IP address 192.168.1.56.

1 Click **Firewall**. In **From Zone**, select **WAN**; in **To Zone**, select **LAN1.**

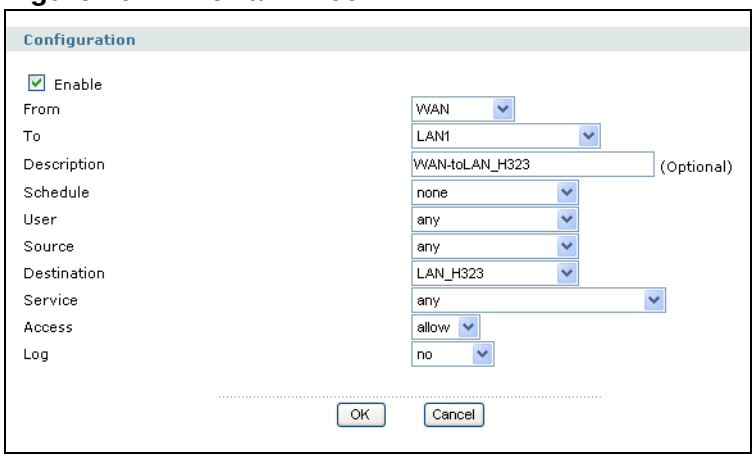
2 The default rule for WAN-to-LAN traffic drops all traffic. You want to allow H.323 access through IP address 10.0.0.8, so add a rule before the default rule. Click the **Add** icon at the top of the column.

**Figure 103** Firewall: WAN to LAN




3 Configure the screen as follows and click **OK**. LAN_H323 is the destination because the ZyWALL applies the virtual server to traffic before applying the firewall rule.

**Figure 104** Firewall > Add



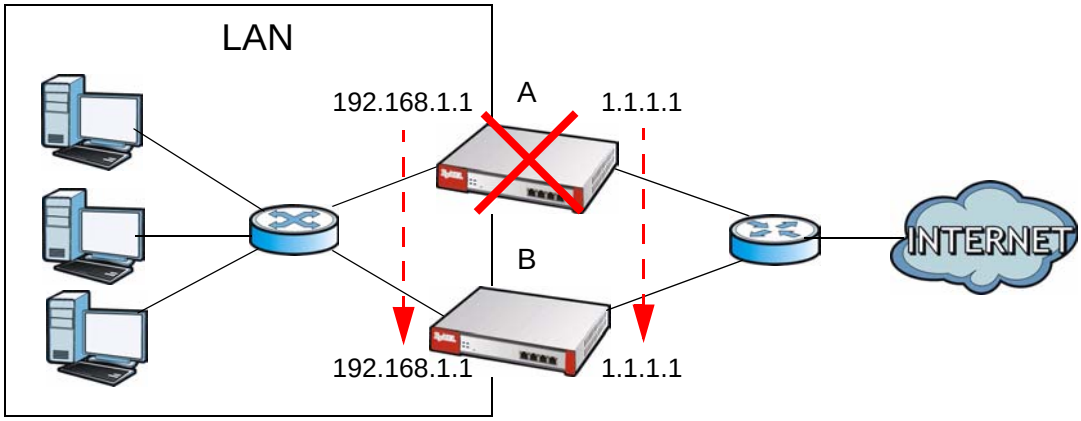

# 6.9 How to Use Active-Passive Device HA

Here is an example of using device HA (High Availability) to backup ZyWALL **A** (the master) with ZyWALL **B**. ZyWALL **B** automatically takes over all of **A**'s functions if **A** fails or loses its **lan1** or **wan1** connection.

An Ethernet switch connects both ZyWALLs' **lan1** interfaces to the LAN. Whichever ZyWALL is functioning as the master uses the default gateway IP address of the LAN computers (192.168.1.1) for its **lan1** interface and the static public IP address (1.1.1.1) for its **wan1** interface. If ZyWALL **A** recovers (has both its **lan1**

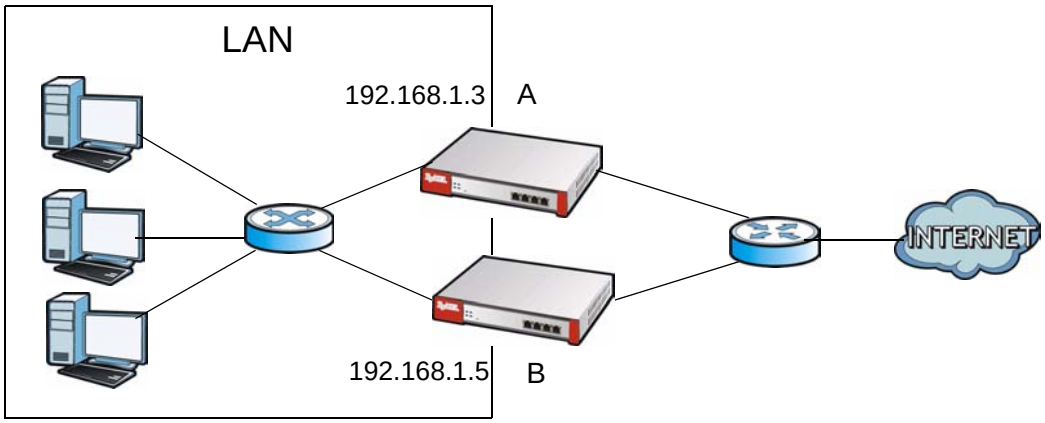
and **wan1** interfaces connected), it resumes its role as the master and takes over all of its functions again.

**Figure 105** Device HA: Master Fails and Backup Takes Over




Each ZyWALL's **lan1** interface also has a separate management IP address that stays the same whether the ZyWALL functions as the master or a backup. ZyWALL **A**'s management IP address is 192.168.1.3 and ZyWALL **B**'s is 192.168.1.5.

**Figure 106** Device HA: Management IP Addresses




## 6.9.1 Before You Start

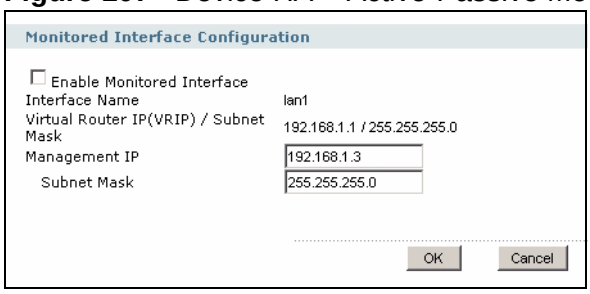
ZyWALL **A** should already be configured. You will use device HA to copy ZyWALL **A**'s settings to **B** later (in Section 6.9.3 on page 143). To avoid an IP address conflict, do not connect ZyWALL **B** to the LAN subnet until after you configure its device HA settings and the instructions tell you to deploy it (in Section 6.9.4 on page 144).

## 6.9.2 Configure Device HA on the Master ZyWALL

1 Log into ZyWALL **A** (the master ) and click **Device HA > Active-Passive Mode**. Click **lan1**'s **Edit** icon.

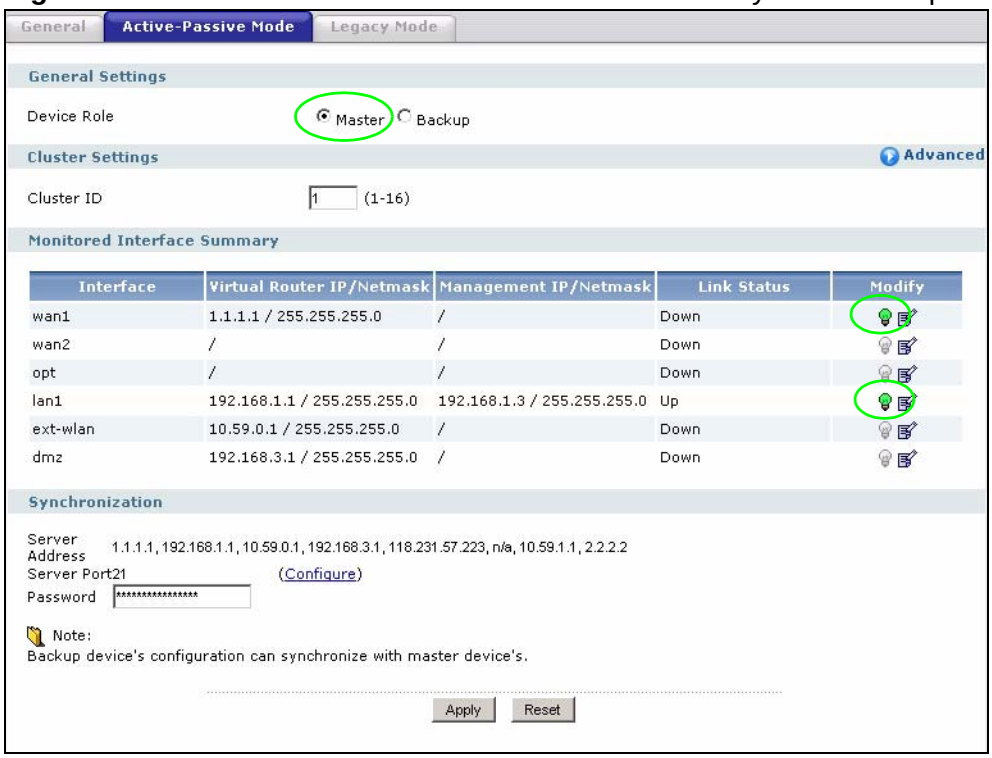
2 Configure 192.168.1.3 as the **Management IP** and 255.255.255.0 as the **Subnet Mask**. Click **OK**.

**Figure 107** Device HA > Active-Passive Mode > Edit: Master ZyWALL Example



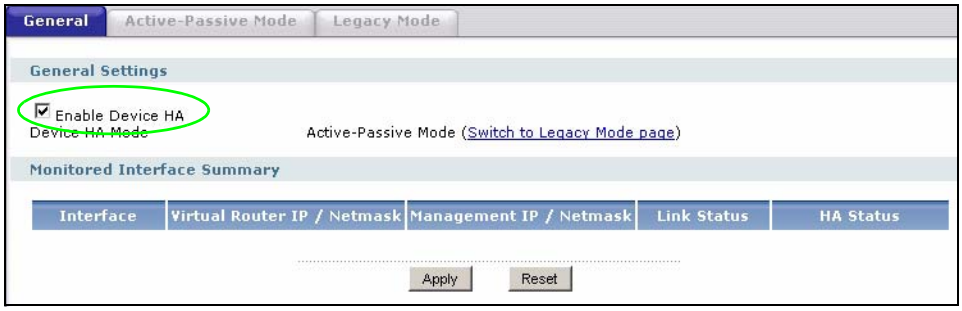

3 Set the **Device Role** to **Master**. This example focuses on the connection from the LAN (**lan1**) to the Internet through the **wan1** interface, so turn on monitoring for the **lan1** and **wan1** interfaces. Enter a **Synchronization Password** ("mySyncPassword" in this example) and click **Apply**.

**Figure 108** Device HA > Active-Passive Mode: Master ZyWALL Example



4 Click the **General** tab. Turn on device HA and click **Apply**.

**Figure 109** Device HA > General: Master ZyWALL Example



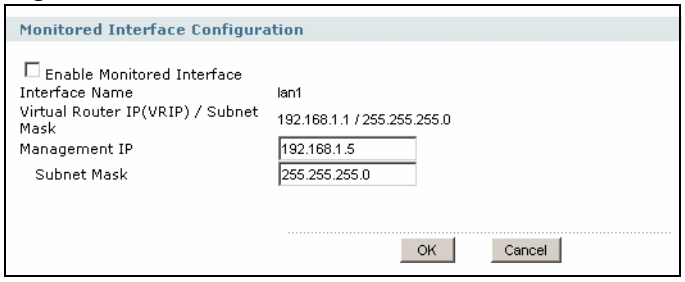

## 6.9.3 Configure the Backup ZyWALL

1 Connect a computer to ZyWALL **B**'s **lan1** interface and log into its Web Configurator. Connect ZyWALL **B** to the Internet and subscribe it to the same subscription services (like content filtering and anti-virus) to which ZyWALL **A** is subscribed. See Chapter 8 on page 165 for more on the subscription services.

2 In ZyWALL **B** click **Device HA > Active-Passive Mode**. Click **lan1**'s **Edit** icon.

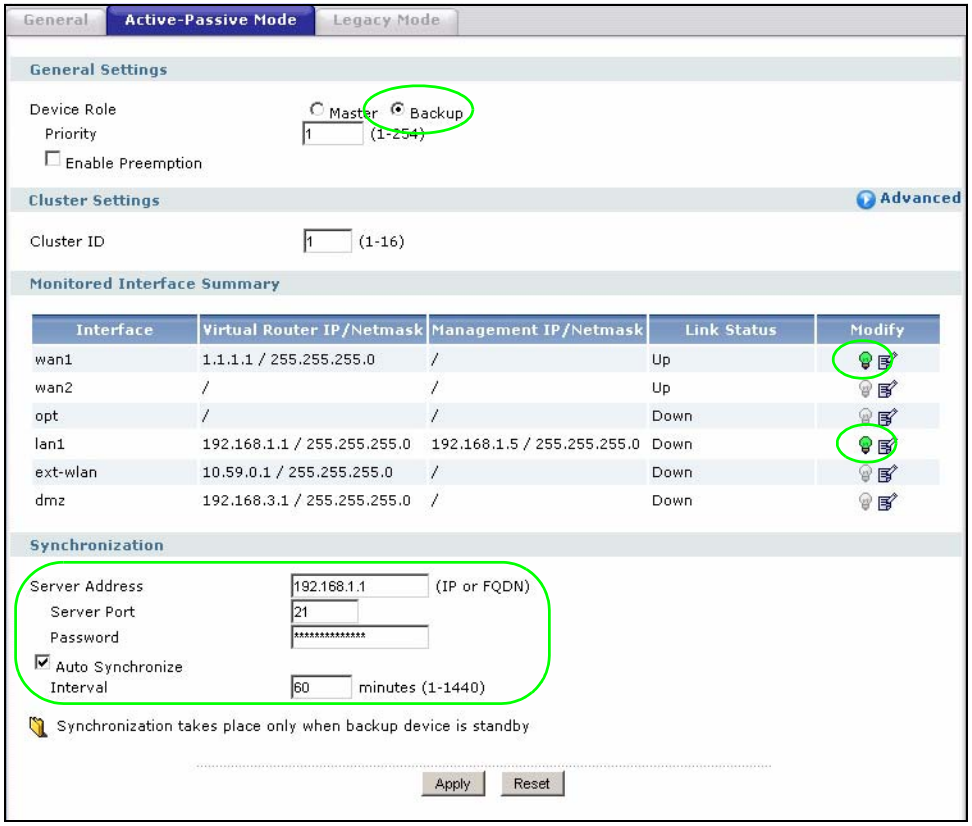
3 Configure 192.168.1.5 as the **Management IP** and 255.255.255.0 as the **Subnet Mask**. Click **OK**.

**Figure 110** Device HA > Active-Passive Mode > Edit: Backup ZyWALL Example



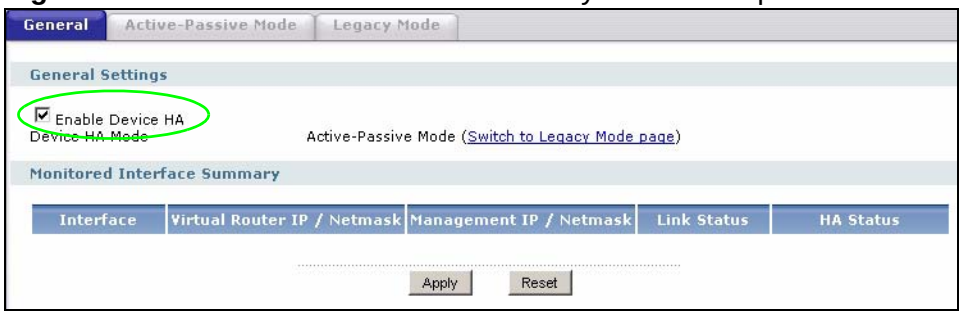
4 Set the **Device Role** to **Backup**. Turn on monitoring for the **lan1** and **wan1** interfaces. Set the **Synchronization Server Address** to 192.168.1.1, the **Port** to 21, and the **Password** to "mySyncPassword". Select **Auto Synchronize** and set the **Interval** to 60. Click **Apply**.

**Figure 111** Device HA > Active-Passive Mode: Backup ZyWALL Example




5 Click the **General** tab. Turn on device HA and click **Apply**.

**Figure 112** Device HA > General: Master ZyWALL Example




## 6.9.4 Deploy the Backup ZyWALL

Connect ZyWALL **B**'s **lan1** interface to the LAN network. Connect ZyWALL **B**'s **wan1** interface to the same router that ZyWALL **A**'s **wan1** interface uses for Internet access. ZyWALL **B** copies **A**'s configuration (and re-synchronizes with **A**

every hour). If ZyWALL **A** fails or loses its **lan1** or **wan1** connection, ZyWALL **B** functions as the master.

### 6.9.5 Check Your Device HA Setup

1. To make sure ZyWALL **B** copied ZyWALL **A**'s settings, you can log into ZyWALL **B**'s management IP address (192.168.1.5) and check the configuration. You can use the **Maintenance > File Manager > Configuration File** screen to save copies of the ZyWALLs' configuration files that you can compare.

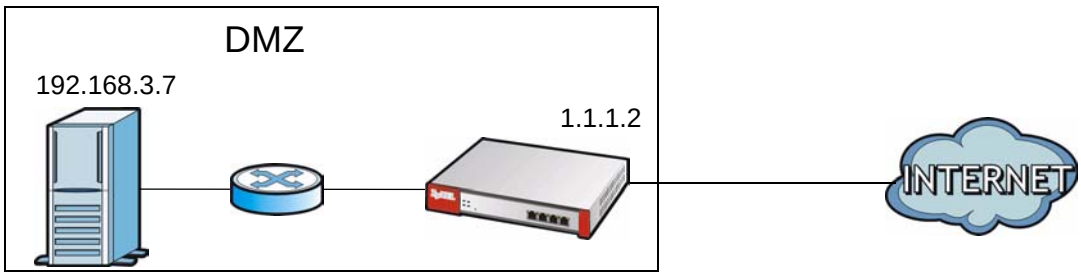
2. To test your device HA configuration, disconnect ZyWALL **A**'s **lan1** or **wan1** interface. Computers on LAN1 should still be able to access the Internet. If they cannot, check your connections and device HA configuration.

   Congratulations! Now that you have configured device HA for LAN1, you can use the same process for any of the ZyWALL's other local networks. For example, enable device HA monitoring on the DMZ interfaces and use an Ethernet switch to connect both ZyWALLs' DMZ interfaces to your publicly available servers.

## 6.10 How to Allow Public Access to a Server

This is an example of making an HTTP (web) server in the DMZ zone accessible from the Internet (the WAN zone). You will use a public IP address of 1.1.1.2 on the **wan2** interface and map it to the HTTP server's private IP address of 192.168.3.7.

**Figure 113** Public Server Example Network Topology

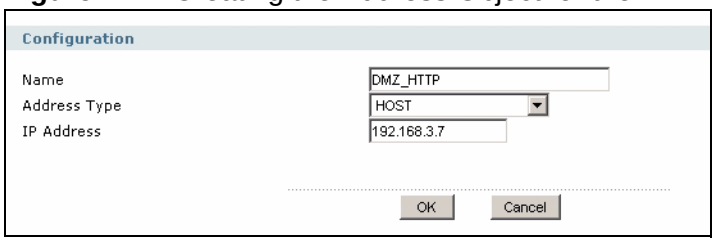



### 6.10.1 Create the Address Objects

Use **Object > Address > Add** to create the address objects.

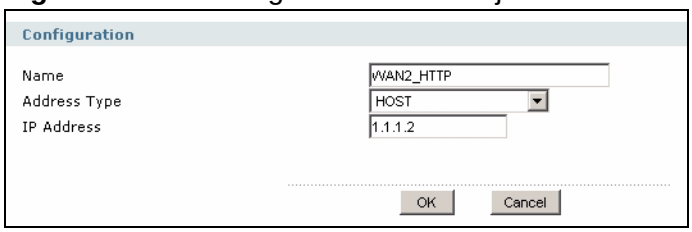
1 Create an address object named DMZ_HTTP for the HTTP server's private IP address of 192.168.3.7.

**Figure 114** Creating the Address Object for the HTTP Server's Private IP Address




2 Create an address object named ge3_HTTP for the **wan2** public IP address of 1.1.1.2.

**Figure 115** Creating the Address Object for the wan2 Public IP Address



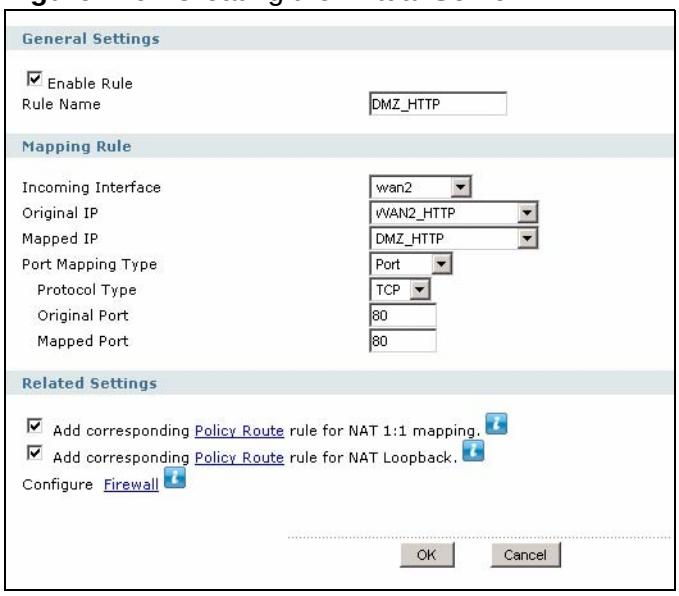

## 6.10.2 Configure a Virtual Server

You need a virtual server to send HTTP traffic coming to IP address 1.1.1.2 on **wan2** to the HTTP server's private IP address of 192.168.3.7. In the **Network > Virtual Server** screen, click the + symbol and create a new virtual server entry as shown next.

- This virtual server is for traffic coming in on **wan2** to IP address 1.1.1.2 (defined in the **wan2_HTTP** object).
- The virtual server sends this traffic to the HTTP server's private IP address of 192.168.3.7 (defined in the **DMZ_HTTP** object).
- HTTP traffic and the HTTP server in this example both use TCP port 80. So you set the **Port Mapping Type** to **Port**, the **Protocol Type** to **TCP**, and the original and mapped ports to 80.
- In this example 1.1.1.2 is not the default IP address for sessions going out through **wan2**. Select **Add corresponding Policy Route rule for NAT 1:1 mapping** to send the HTTP server's outgoing sessions through **wan2** and use 1.1.1.2 as the source IP address (to match the IP address for accessing it). See NAT 1:1 Example on page 314 for details.

- Select **Add corresponding Policy Route rule for NAT Loopback** to allow local users to use a domain name to access the HTTP server. See NAT Loopback Example on page 318 for details.

**Figure 116** Creating the Virtual Server




The firewall allows traffic from the WAN zone to the DMZ zone by default so your configuration is done. Now the public can go to IP address 1.1.1.2 to access the HTTP server. If a domain name is registered for IP address 1.1.1.2, users can just go to the domain name to access the web server.

# 7 Status

## 7.1 Overview

Use the **Status** screens to check status information about the ZyWALL.

### 7.1.1 What You Can Do in the Status Screens

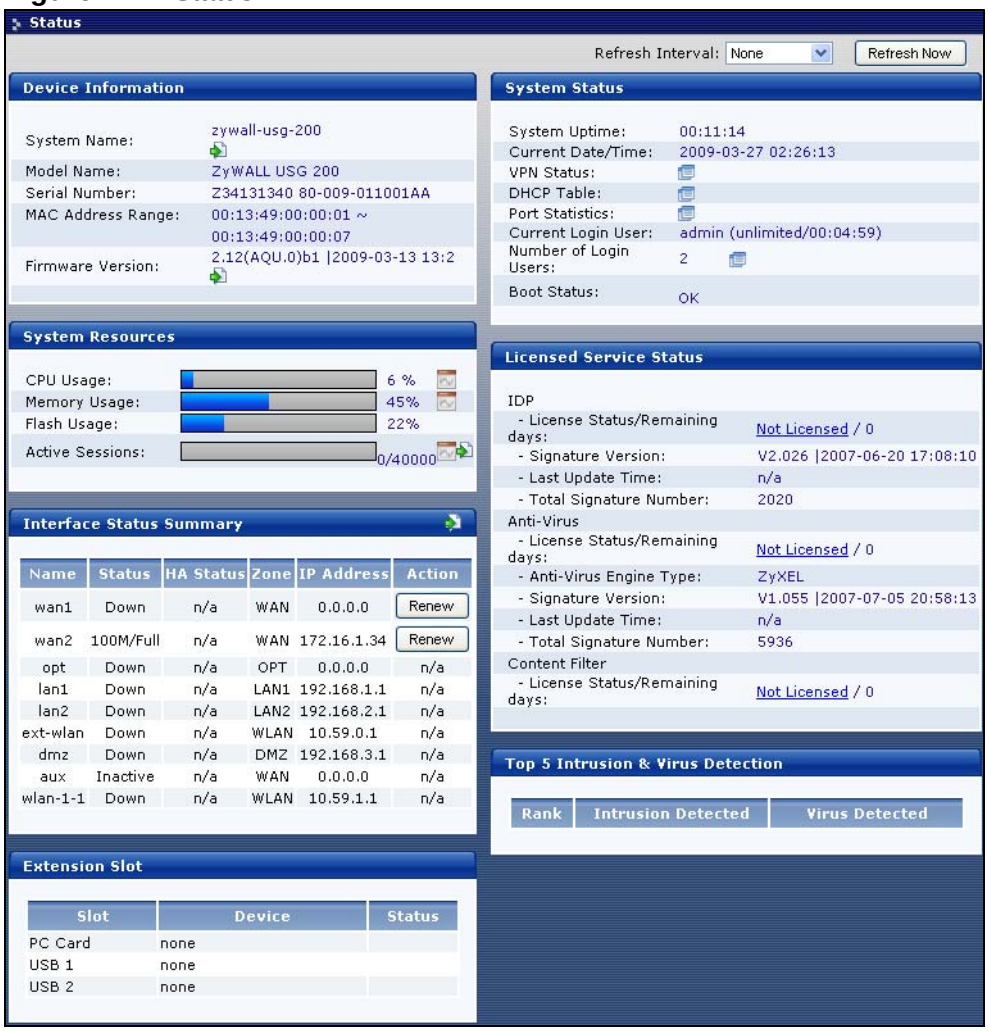
Use the **Status** screens for the following.

- Use the main **Status** screen (see Section 7.2 on page 150) to see the ZyWALL's general device information, system status, system resource usage, licensed service status, and interface status. You can also go to the other status screens for more information.
- Use the **VPN** status screen (see Section 7.2.1 on page 155) to look at the VPN tunnels that are currently established.
- Use the **DHCP Table** screen (see Section 7.2.5 on page 159) to look at the IP addresses currently assigned to DHCP clients and the IP addresses reserved for specific MAC addresses.
- Use the **Port Statistics** screen (see Section 7.2.7 on page 161) to look at packet statistics for each physical port. To access this screen, click **Port Statistics** in the **Status** screen.
- Use the **Port Statistics Graph** screen (see Section 7.2.7 on page 161) to look at a line graph of packet statistics for each physical port.
- Use the **Current Users** screen (see Section 7.2.8 on page 162) to look at a list of the users currently logged into the ZyWALL.

# 7.2 The Status Screen

The **Status** screen displays when you log into the ZyWALL or click **Status**. Use this screen to look at the ZyWALL's general device information, system status, system resource usage, licensed service status, and interface status.

**Figure 117** Status




The following table describes the labels in this screen.

**Table 30** Status

| LABEL | DESCRIPTION |
|---|---|
| Refresh Interval | Select how often you want the screen to automatically refresh. |
| Refresh Now | Click this to update the screen immediately. |
| Device Information | |

**Table 30** Status (continued)

| LABEL | DESCRIPTION |
|---|---|
| System Name | This field displays the name used to identify the ZyWALL on any network. Click the icon to open the screen where you can change it. See Section 45.2 on page 732. |
| Model Name | This field displays the model name of this ZyWALL. |
| Serial Number | This field displays the serial number of this ZyWALL. |
| MAC Address Range | This field displays the MAC addresses used by the ZyWALL. Each physical port has one MAC address. The first MAC address is assigned to physical port 1, the second MAC address is assigned to physical port 2, and so on. |
| Firmware Version | This field displays the version number and date of the firmware the ZyWALL is currently running. Click the icon to open the screen where you can upload firmware. See Section 46.3 on page 788. |
| System Resources | |
| CPU Usage | This field displays what percentage of the ZyWALL's processing capability is currently being used. Click the icon to display a chart of the ZyWALL's recent CPU usage. |
| Memory Usage | This field displays what percentage of the ZyWALL's RAM is currently being used. Click the icon to display a chart of the ZyWALL's recent memory usage. |
| Flash Usage | This field displays what percentage of the ZyWALL's onboard flash memory is currently being used. Click the icon to display a chart of the ZyWALL's recent flash usage. |
| Active Sessions | This field displays how many traffic sessions are currently open on the ZyWALL. These are the sessions that are traversing the ZyWALL. Click the icon to display a chart of ZyWALL's recent session usage. |
| Interface Status Summary | If an Ethernet interface does not have any physical ports associated with it, its entry is displayed in light gray text. Click the **Detail** icon to go to a (more detailed) summary screen of interface statistics. |
| Name | This field displays the name of each interface. |

**Table 30** Status (continued)

| LABEL | DESCRIPTION |
|---|---|
| Status | This field displays the current status of each interface. The possible values depend on what type of interface it is.<br><br>For Ethernet interfaces:<br><br>**Inactive** - The Ethernet interface is disabled.<br><br>**Down** - The Ethernet interface does not have any physical ports associated with it or the Ethernet interface is enabled but not connected.<br><br>**Speed / Duplex** - The Ethernet interface is enabled and connected. This field displays the port speed and duplex setting (**Full** or **Half**).<br><br>For cellular (3G) interfaces, see Section 10.9 on page 219 for the status that can appear.<br><br>For the auxiliary interface:<br><br>**Inactive** - The auxiliary interface is disabled.<br><br>**Connected** - The auxiliary interface is enabled and connected.<br><br>**Disconnected** - The auxiliary interface is not connected. |
| HA Status | This field displays the status of the interface in the virtual router.<br><br>**Active** - This interface is the master interface in the virtual router.<br><br>**Stand-By** - This interface is a backup interface in the virtual router.<br><br>**Fault** - This VRRP group is not functioning in the virtual router right now. For example, this might happen if the interface is down.<br><br>**n/a** - Device HA is not active on the interface. |
| Zone | This field displays the zone to which the interface is currently assigned. |
| IP Address | This field displays the current IP address assigned to the interface. If the IP address is 0.0.0.0, the interface is disabled or did not receive an IP address and subnet mask via DHCP.<br><br>If this interface is a member of an active virtual router, this field displays the IP address it is currently using. This is either the static IP address of the interface (if it is the master) or the management IP address (if it is a backup). |
| Action | Use this field to get or to update the IP address for the interface.<br><br>Click **Renew** to send a new DHCP request to a DHCP server.<br><br>Click the **Connect** icon to have the ZyWALL try to connect a PPPoE/PPTP interface or the auxiliary interface. If the interface cannot use one of these ways to get or to update its IP address, this field displays **n/a**.<br><br>Click the **Disconnect** icon to stop a PPPoE/PPTP or auxiliary interface's connection. |
| Extension Slot | This section of the screen displays the status of the extension card slot and the USB ports. |
| Slot | This field displays the name of each extension slot. |
| Device | This field displays the name of the device connected to the extension slot (or **none** if no device is detected). |

**Table 30** Status (continued)

| LABEL | DESCRIPTION |
|---|---|
| Status | For installed cellular (3G) cards, this field displays the card's current status. See Table 62 on page 220. |
| System Status | |
| System Uptime | This field displays how long the ZyWALL has been running since it last restarted or was turned on. |
| Current Date/ Time | This field displays the current date and time in the ZyWALL. The format is yyyy-mm-dd hh:mm:ss. |
| VPN Status | Click this to look at the VPN tunnels that are currently established. See Section 7.2.1 on page 155. |
| DHCP Table | Click this to look at the IP addresses currently assigned to the ZyWALL's DHCP clients and the IP addresses reserved for specific MAC addresses. See Section 7.2.5 on page 159. |
| Port Statistics | Click this to look at packet statistics for each Gigabit Ethernet port. See Section 7.2.7 on page 161. |
| Current Login User | This field displays the user name used to log in to the current session, the amount of reauthentication time remaining, and the amount of lease time remaining. See Chapter 37 on page 649. |
| Number of Login Users | This field displays the number of users currently logged in to the ZyWALL. Click the icon to pop-open a list of the users who are currently logged in to the ZyWALL. See Section 7.2.8 on page 162. |
| Boot Status | This field displays details about the ZyWALL's startup state.<br>**OK** - The ZyWALL started up successfully.<br>**Firmware update OK** - A firmware update was successful.<br>**Problematic configuration after firmware update** - The application of the configuration failed after a firmware upgrade.<br>**System default configuration** - The ZyWALL successfully applied the system default configuration. This occurs when the ZyWALL starts for the first time or you intentionally reset the ZyWALL to the system default settings.<br>**Fallback to lastgood configuration** - The ZyWALL was unable to apply the startup-config.conf configuration file and fell back to the lastgood.conf configuration file.<br>**Fallback to system default configuration** - The ZyWALL was unable to apply the lastgood.conf configuration file and fell back to the system default configuration file (system-default.conf ).<br>**Booting in progress** - The ZyWALL is still applying the system configuration. |
| Licensed Service Status | |
| IDP | |
| License Status / Remaining days | This field displays the current status of the license and how many days longer it is still valid. If it displays 0 days, the license has expired. If the status is not **Licensed**, click this to open the screen where you can activate or extend the license. See Section 8.2 on page 167. |

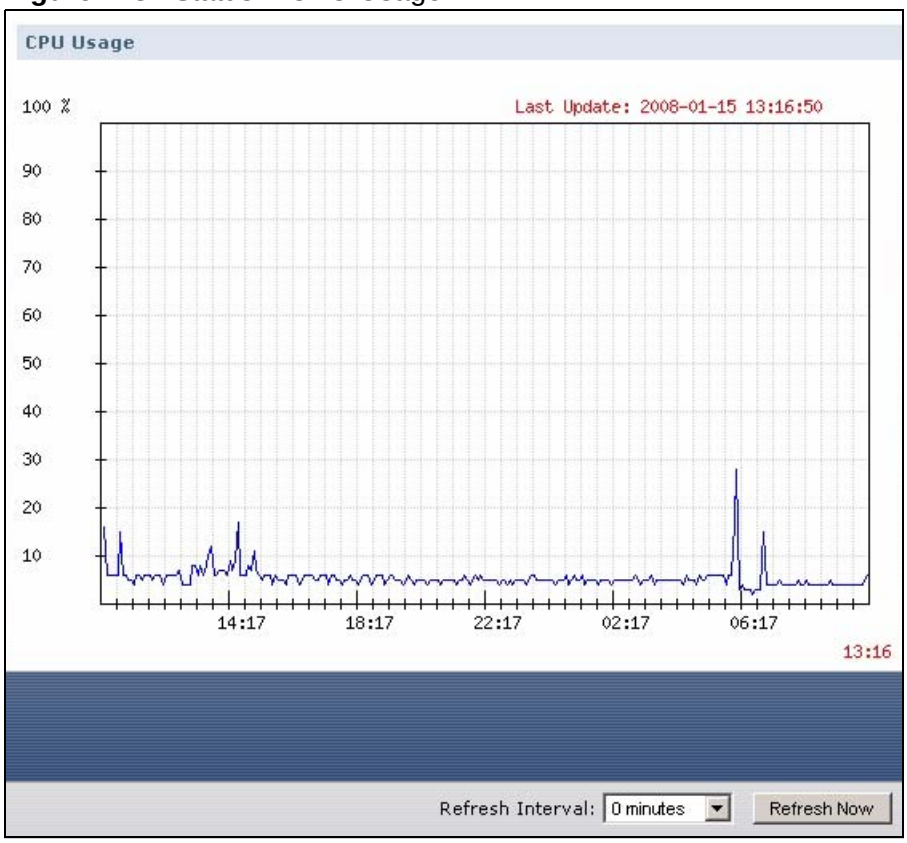
**Table 30** Status (continued)

| LABEL | DESCRIPTION |
|---|---|
| Signature Version | This field displays the version number, date, and time of the current set of signatures the ZyWALL is using. |
| Last Update Time | This field displays the last time the ZyWALL received updated signatures. |
| Total Signature Number | This field displays the total number of signatures in the current signature version. |
| Anti-Virus | |
| License Status / Remaining days | This field displays the current status of the license and how many days longer it is still valid. If it displays 0 days, the license has expired. If the status is not **Licensed**, click this to open the screen where you can activate or extend the license. See Section 8.2 on page 167. |
| Anti-Virus Engine Type | This field displays whether the ZyWALL is set to use ZyXEL's anti-virus engine or the one powered by Kaspersky.<br>Upgrading the ZyWALL to firmware version 2.11 and updating the anti-virus signatures automatically upgrades the ZyXEL anti-virus engine to v2.0. v2.0 has more virus signatures and offers improved non-executable file scan throughput. |
| Signature Version | This field displays the version number, date, and time of the current set of signatures the ZyWALL is using. |
| Last Update Time | This field displays the last time the ZyWALL received updated signatures. |
| Total Signature Number | This field displays the total number of signatures in the current signature version. |
| Content Filter | |
| License Status / Remaining Days | This field displays the current status of the license and how many days longer it is still valid. If it displays 0 days, the license has expired. If the status is not **Licensed**, click this to open the screen where you can activate or extend the license. See Section 8.2 on page 167. |
| Top 5 Intrusion & Virus Detection | The following is a list of the five intrusions or viruses that the ZyWALL has most frequently detected since it last started up. |
| Rank | This is the ranking number of an intrusion or virus. This is an intrusion's or virus's place in the list of most common intrusions or viruses. |
| Intrusion Detected | This is the name of a signature for which the ZyWALL has detected matching packets. The number in brackets indicates how many times the signature has been matched.<br>Click the hyperlink for more detailed information on the intrusion. |
| Virus Detected | This is the name of the virus that the ZyWALL has detected. |

## 7.2.1 The CPU Usage Screen

Use this screen to look at a chart of the ZyWALL's recent CPU usage. To access this screen, click **CPU Usage** in the **Status** screen.

**Figure 118** Status > CPU Usage




The following table describes the labels in this screen.

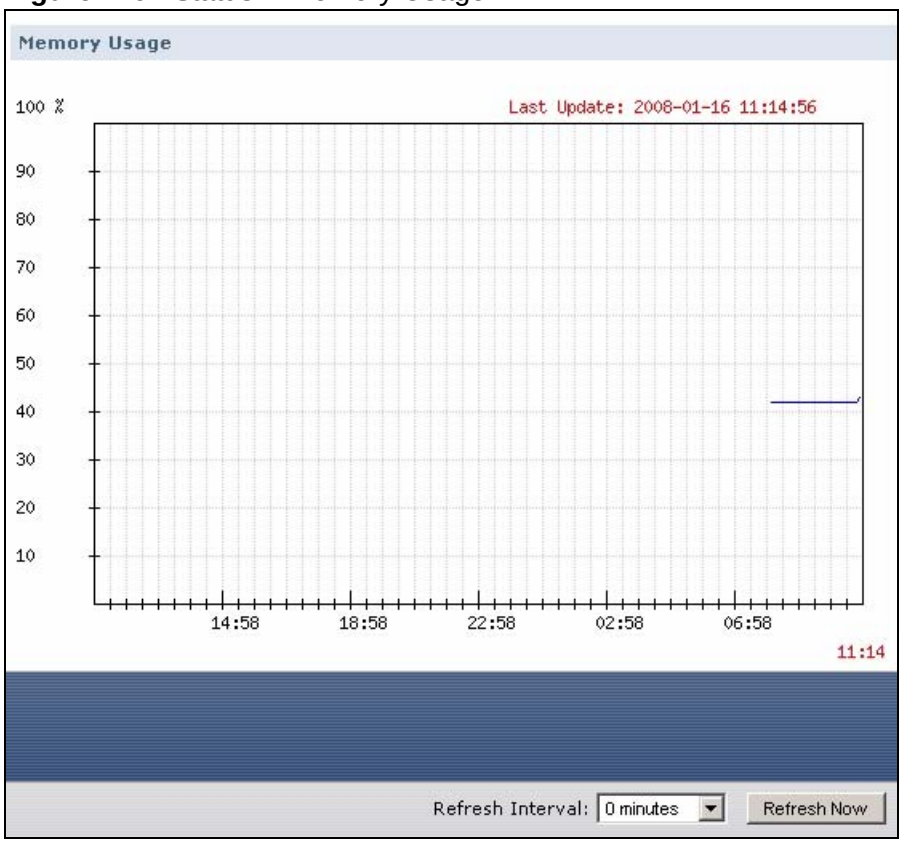
**Table 31** Status > CPU Usage

| LABEL | DESCRIPTION |
|---|---|
| 100 % | The y-axis represents the percentage of CPU usage. |
| time | The x-axis shows the time period over which the CPU usage occurred |
| Refresh Interval | Enter how often you want this window to be automatically updated. |
| Refresh Now | Click this to update the information in the window right away. |

## 7.2.2 The Memory Usage Screen

Use this screen to look at a chart of the ZyWALL's recent memory (RAM) usage. To access this screen, click **Memory Usage** in the **Status** screen.

**Figure 119** Status > Memory Usage




The following table describes the labels in this screen.

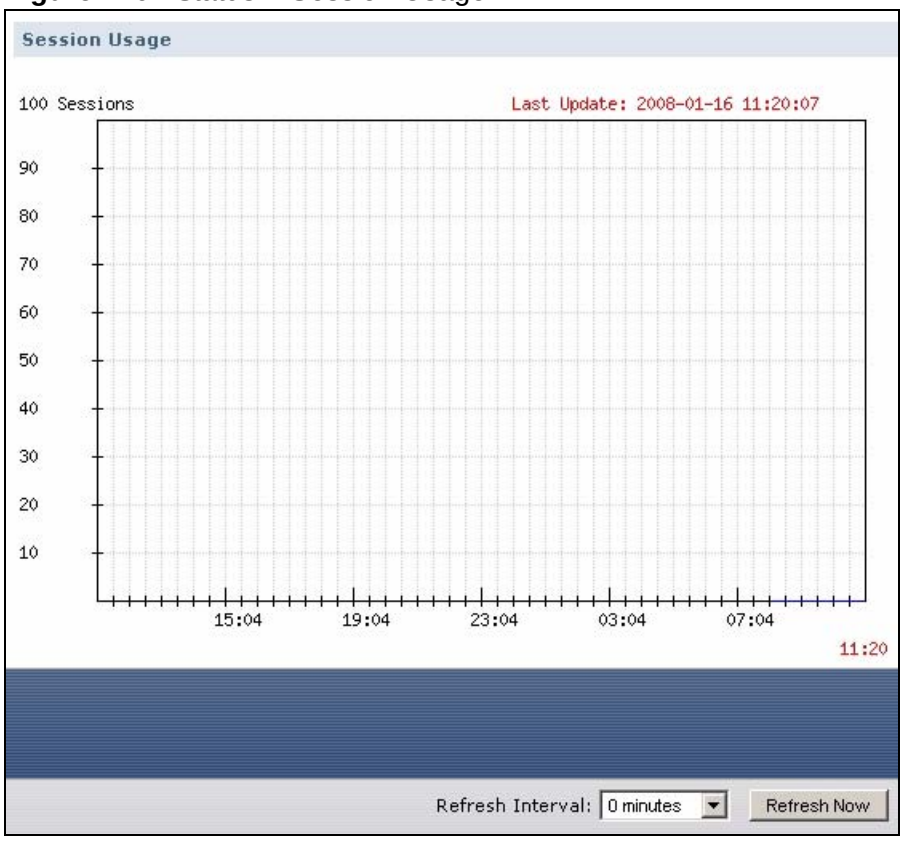
**Table 32** Status > Memory Usage

| LABEL | DESCRIPTION |
|---|---|
| 100 % | The y-axis represents the percentage of RAM usage. |
| time | The x-axis shows the time period over which the RAM usage occurred |
| Refresh Interval | Enter how often you want this window to be automatically updated. |
| Refresh Now | Click this to update the information in the window right away. |

## 7.2.3 The Session Usage Screen

Use this screen to look at a chart of the ZyWALL's recent traffic session usage. To access this screen, click **Session Usage** in the **Status** screen.

**Figure 120** Status > Session Usage




The following table describes the labels in this screen.

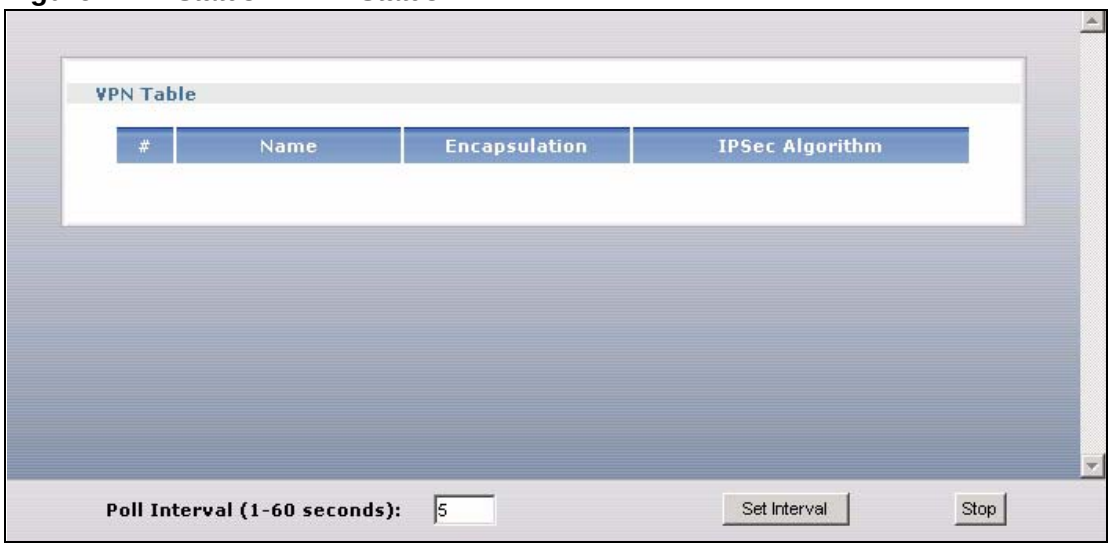
**Table 33** Status > Session Usage

| LABEL | DESCRIPTION |
|---|---|
| Sessions | The y-axis represents the number of session. |
| time | The x-axis shows the time period over which the session usage occurred |
| Refresh Interval | Enter how often you want this window to be automatically updated. |
| Refresh Now | Click this to update the information in the window right away. |

## 7.2.4 The VPN Status Screen

Use this screen to look at the VPN tunnels that are currently established. To access this screen, click **VPN Status** in the **Status** screen.

**Figure 121** Status > VPN Status




The following table describes the labels in this screen.

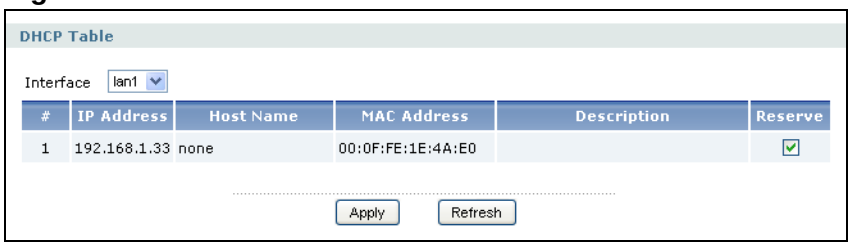
**Table 34** Status > VPN Status

| LABEL | DESCRIPTION |
|---|---|
| # | This field is a sequential value, and it is not associated with a specific SA. |
| Name | This field displays the name of the IPSec SA. |
| Encapsulation | This field displays how the IPSec SA is encapsulated. |
| IPSec Algorithm | This field displays the encryption and authentication algorithms used in the SA. |
| Poll Interval | Enter how often you want this window to be updated automatically, and click **Set Interval**. |
| Set Interval | Click this to set the **Poll Interval** the screen uses. |
| Stop | Click this to stop the window from updating automatically. You can start it again by setting the **Poll Interval** and clicking **Set Interval**. |

## 7.2.5 The DHCP Table Screen

Use this screen to look at the IP addresses currently assigned to DHCP clients and the IP addresses reserved for specific MAC addresses. To access this screen, click the icon beside **DHCP Table** in the **Status** screen.

**Figure 122** Status > DHCP Table




The following table describes the labels in this screen.

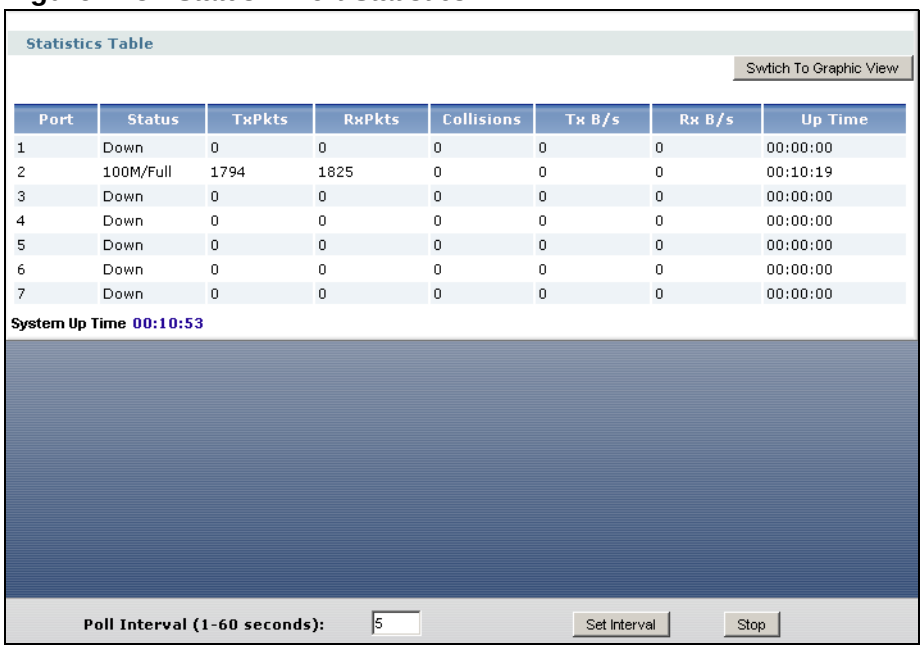
**Table 35** Status > DHCP Table

| LABEL | DESCRIPTION |
|---|---|
| Interface | Select for which interface you want to look at the IP addresses currently assigned to DHCP clients and the IP addresses reserved for specific MAC addresses. |
| # | This field is a sequential value, and it is not associated with a specific entry. |
| IP Address | This field displays the IP address currently assigned to a DHCP client or reserved for a specific MAC address. Click the column's heading cell to sort the table entries by IP address. Click the heading cell again to reverse the sort order. |
| Host Name | This field displays the name used to identify this device on the network (the computer name). The ZyWALL learns these from the DHCP client requests. "None" shows here for a static DHCP entry. |
| MAC Address | This field displays the MAC address to which the IP address is currently assigned or for which the IP address is reserved. Click the column's heading cell to sort the table entries by MAC address. Click the heading cell again to reverse the sort order. |
| Description | For a static DHCP entry, the host name or the description you configured shows here. This field is blank for dynamic DHCP entries. |
| Reserve | If this field is selected, this entry is a static DHCP entry. The IP address is reserved for the MAC address.<br><br>If this field is clear, this entry is a dynamic DHCP entry. The IP address is assigned to a DHCP client.<br><br>To create a static DHCP entry using an existing dynamic DHCP entry, select this field, and then click **Apply**.<br><br>To remove a static DHCP entry, clear this field, and then click **Apply**. |
| Apply | Click this to save your settings to the ZyWALL. |
| Refresh | Click this to update the screen immediately. |

## 7.2.6 The Port Statistics Screen

Use this screen to look at packet statistics for each Gigabit Ethernet port. To access this screen, click **Port Statistics** in the **Status** screen.

**Figure 123** Status > Port Statistics




The following table describes the labels in this screen.

**Table 36** Status > Port Statistics

| LABEL | DESCRIPTION |
|---|---|
| Switch to Graphic View | Click this to display the port statistics as a line graph. |
| Port | This field displays the physical port number. |
| Status | This field displays the current status of the physical port.<br>**Down** - The physical port is not connected.<br>**Speed / Duplex** - The physical port is connected. This field displays the port speed and duplex setting (**Full** or **Half**). |
| TxPkts | This field displays the number of packets transmitted from the ZyWALL on the physical port since it was last connected. |
| RxPkts | This field displays the number of packets received by the ZyWALL on the physical port since it was last connected. |
| Collisions | This field displays the number of collisions on the physical port since it was last connected. |
| Tx B/s | This field displays the transmission speed, in bytes per second, on the physical port in the one-second interval before the screen updated. |
| Rx B/s | This field displays the reception speed, in bytes per second, on the physical port in the one-second interval before the screen updated. |
| Up Time | This field displays how long the physical port has been connected. |

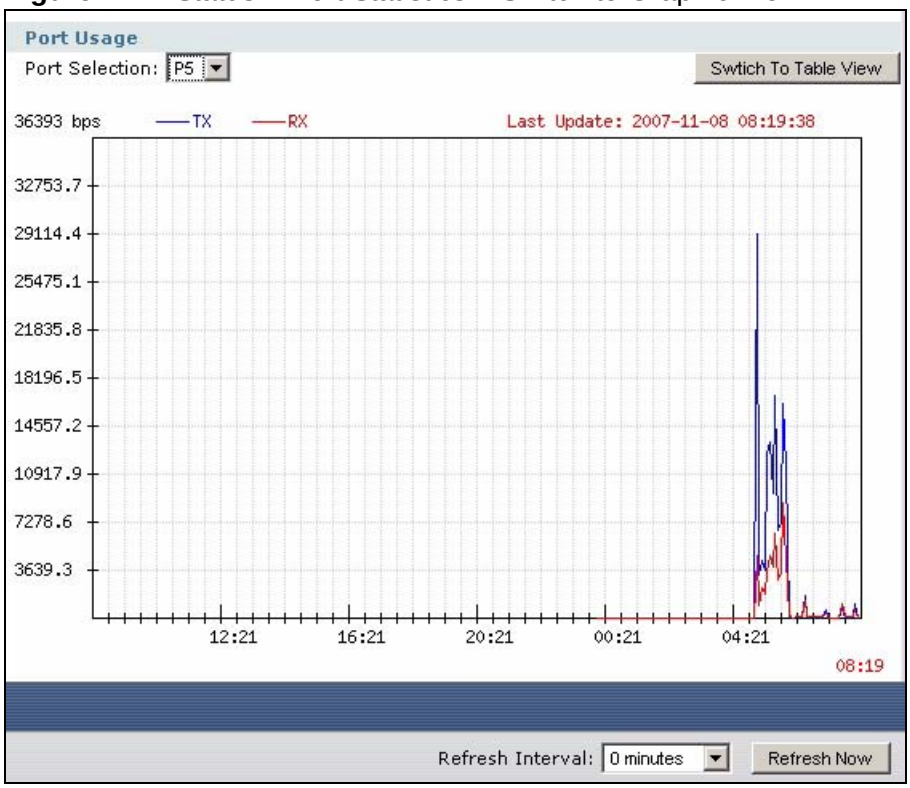
**Table 36** Status > Port Statistics (continued)

| LABEL | DESCRIPTION |
|---|---|
| System Up Time | This field displays how long the ZyWALL has been running since it last restarted or was turned on. |
| Poll Interval | Enter how often you want this window to be updated automatically, and click **Set Interval**. |
| Set Interval | Click this to set the **Poll Interval** the screen uses. |
| Stop | Click this to stop the window from updating automatically. You can start it again by setting the **Poll Interval** and clicking **Set Interval**. |

## 7.2.7 The Port Statistics Graph Screen

Use this screen to look at a line graph of packet statistics for each physical port. To access this screen, click **Port Statistics** in the **Status** screen and then the **Switch to Graphic View Button**.

**Figure 124** Status > Port Statistics > Switch to Graphic View



The following table describes the labels in this screen.

**Table 37** Status > Port Statistics > Switch to Graphic View

| LABEL | DESCRIPTION |
|---|---|
| Port | Select the number of the physical port for which you want to display graphics. |
| Switch to Table View | Click this to display the port statistics as a table. |
| bps | The y-axis represents the speed of transmission or reception. |
| time | The x-axis shows the time period over which the transmission or reception occurred |
| Tx | This line represents traffic transmitted from the ZyWALL on the physical port since it was last connected. |
| Rx | This line represents the traffic received by the ZyWALL on the physical port since it was last connected. |
| Last Update | This field displays the date and time the information in the window was last updated. |
| System Up Time | This field displays how long the ZyWALL has been running since it last restarted or was turned on. |
| Refresh Interval | Enter how often you want this window to be automatically updated. |
| Refresh Now | Click this to update the information in the window right away. |

## 7.2.8 The Current Users Screen

Use this screen to look at a list of the users currently logged into the ZyWALL. To access this screen, click the **Number of Login Users Detail** icon in the **Status** screen.

**Figure 125** Status > Current Users


The following table describes the labels in this screen.

**Table 38** Status > Current Users

| LABEL | DESCRIPTION |
|---|---|
| # | This field is a sequential value and is not associated with any entry. |
| User ID | This field displays the user name of each user who is currently logged in to the ZyWALL. |
| Reauth Lease T. | This field displays the amount of reauthentication time remaining and the amount of lease time remaining for each user. See Chapter 37 on page 649. |
| Type | This field displays the way the user logged in to the ZyWALL. |

**Table 38** Status > Current Users (continued)

| LABEL | DESCRIPTION |
|---|---|
| IP address | This field displays the IP address of the computer used to log in to the ZyWALL. |
| Force Logout | Click this icon to end a user's session. |

# 8

# Registration

## 8.1 Overview

Use the **Licensing > Registration** screens to register your ZyWALL and manage its service subscriptions.

### 8.1.1 What You Can Do in the Registration Screens

- Use the **Registration** screen (see Section 8.2 on page 167) to register your ZyWALL with myZyXEL.com and activate a service, such as content filtering.
- Use the **Service** screen (see Section 8.3 on page 169) to display the status of your service registrations and upgrade licenses.

### 8.1.2 What you Need to Know About Service Registration

This section introduces the topics covered in this chapter.

#### myZyXEL.com

myZyXEL.com is ZyXEL's online services center where you can register your ZyWALL and manage subscription services available for the ZyWALL. To update signature files or use a subscription service, you have to register the ZyWALL and activate the corresponding service at myZyXEL.com (through the ZyWALL).

Note: You need to create a myZyXEL.com account before you can register your device and activate the services at myZyXEL.com.

You can directly create a myZyXEL.com account, register your ZyWALL and activate a service using the **Registration** screen. Alternatively, go to http://www.myZyXEL.com with the ZyWALL's serial number and LAN MAC address to register it. Refer to the web site's on-line help for details.

Note: To activate a service on a ZyWALL, you need to access myZyXEL.com via that ZyWALL.

## Subscription Services Available on the ZyWALL

You can have the ZyWALL use anti-virus, IDP/AppPatrol (Intrusion Detection and Prevention and application patrol), and content filtering subscription services. You can also purchase and enter a license key to have the ZyWALL use more SSL VPN tunnels. See the respective User's Guide chapters for more information about these features.

## Anti-Virus Engines

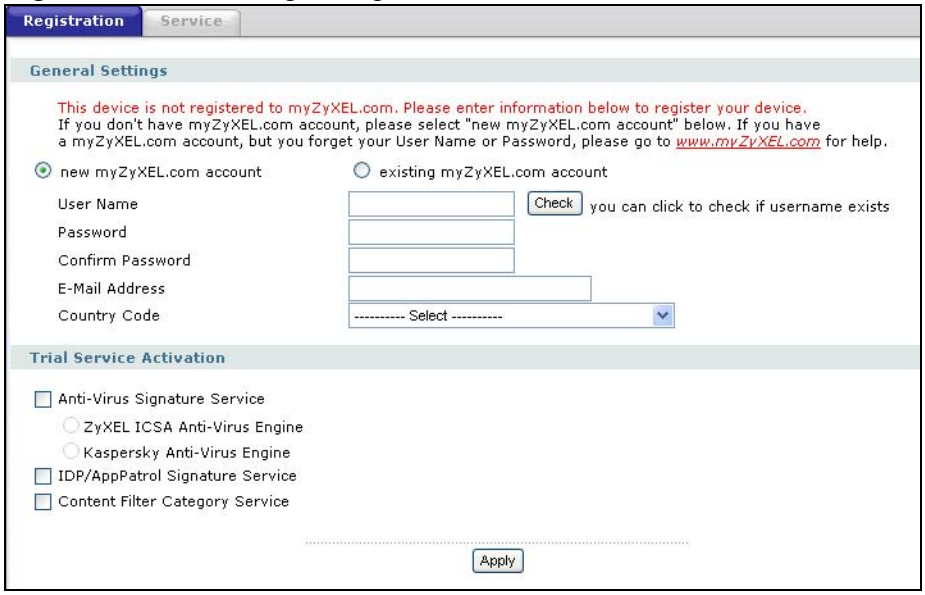
Subscribe to signature files for ZyXEL's anti-virus engine or one powered by Kaspersky.

- When using the trial, you can switch from one engine to the other in the **Registration** screen. There is no limit on the number of times you can change the anti-virus engine selection during the trial, but you only get a total of one anti-virus trial period (not a separate trial period for each anti-virus engine).
- After the trial expires, you need to purchase an iCard for the anti-virus engine you want to use and enter the PIN number (license key) in the **Registration > Service** screen. You must use the ZyXEL anti-virus iCard for the ZyXEL anti-virus engine and the Kaspersky anti-virus iCard for the Kaspersky anti-virus engine. If you were already using an iCard anti-virus subscription, any remaining time on your earlier subscription is automatically added to the new subscription. Even if the earlier iCard anti-virus subscription was for a different anti-virus engine. For example, suppose you purchase a one-year Kaspersky engine anti-virus service subscription and use it for six months. Then you purchase a one-year ZyXEL engine anti-virus service subscription and enter the iCard's PIN number (license key) in the **Registration > Service** screen. The one-year ZyXEL engine anti-virus service subscription is automatically extended to 18 months.

# 8.2 The Registration Screen

Use this screen to register your ZyWALL with myZyXEL.com and activate a service, such as content filtering. Click **Licensing > Registration** in the navigation panel to open the screen as shown next.

**Figure 126** Licensing > Registration




The following table describes the labels in this screen.

**Table 39** Licensing > Registration

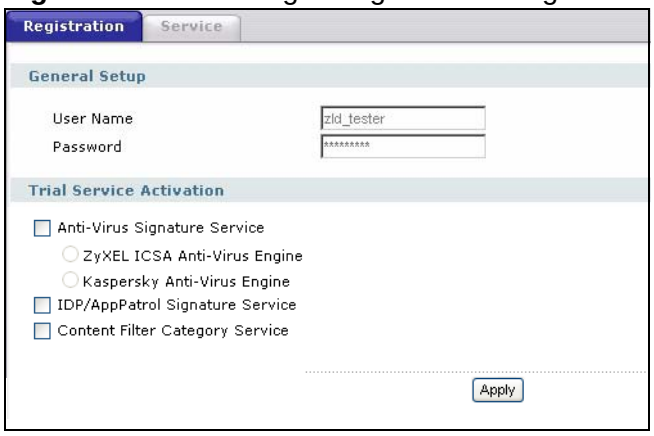
| LABEL | DESCRIPTION |
|---|---|
| General Setup | If you select **existing myZyXEL.com account**, only the **User Name** and **Password** fields are available. |
| new myZyXEL.com account | If you haven't created an account at myZyXEL.com, select this option and configure the following fields to create an account and register your ZyWALL. |
| existing myZyXEL.com account | If you already have an account at myZyXEL.com, select this option and enter your user name and password in the fields below to register your ZyWALL. |
| UserName | Enter a user name for your myZyXEL.com account. The name should be from six to 20 alphanumeric characters (and the underscore). Spaces are not allowed. |
| Check | Click this button to check with the myZyXEL.com database to verify the user name you entered has not been used. |
| Password | Enter a password of between six and 20 alphanumeric characters (and the underscore). Spaces are not allowed. |
| Confirm Password | Enter the password again for confirmation. |
| E-Mail Address | Enter your e-mail address. You can use up to 80 alphanumeric characters (periods and the underscore are also allowed) without spaces. |

**Table 39** Licensing > Registration (continued)

| LABEL | DESCRIPTION |
|---|---|
| Country Code | Select your country from the drop-down box list. |
| Trial Service Activation | Select the check box to activate a trial service subscription. The trial period starts the day you activate the trial. After the trial expires, you can buy an iCard and enter the license key in the **Registration Service** screen to extend the service. |
| Anti-Virus Signature Service | The ZyWALL's anti-virus packet scanner uses the signature files on the ZyWALL to detect virus files.<br><br>Select ZyXEL's anti-virus engine or the Kaspersky anti-virus engine. During the trial you can use these fields to change from one anti-virus engine to the other.<br><br>After the service is activated, the ZyWALL can download the up-to-date signature files for the selected anti-virus engine from the update server (http://myupdate.zywall.zyxel.com). |
| IDP/AppPatrol Signature Service | The IDP and application patrol features use the IDP/AppPatrol signature files on the ZyWALL. IDP detects malicious or suspicious packets and responds immediately. Application patrol conveniently manages the use of various applications on the network. After the service is activated, the ZyWALL can download the up-to-date signature files from the update server (http://myupdate.zywall.zyxel.com).<br><br>You will get automatic e-mail notification of new signature releases from mySecurityZone after you activate the IDP/AppPatrol service. You can also check for new signatures at http://mysecurity.zyxel.com. |
| Content Filter Category Service | The content filter allows or blocks access to web sites. Subscribe to category-based content filtering to block access to categories of web sites based on content. Your ZyWALL accesses an external database that has millions of web sites categorized based on content. You can have the ZyWALL block, block and/or log access to web sites based on these categories. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |

Note: If the ZyWALL is registered already, this screen is read-only and indicates whether trial services are activated (if any). You can still select the unchecked trial service(s) to activate it after registration. Use the **Service** screen to update your service subscription status.

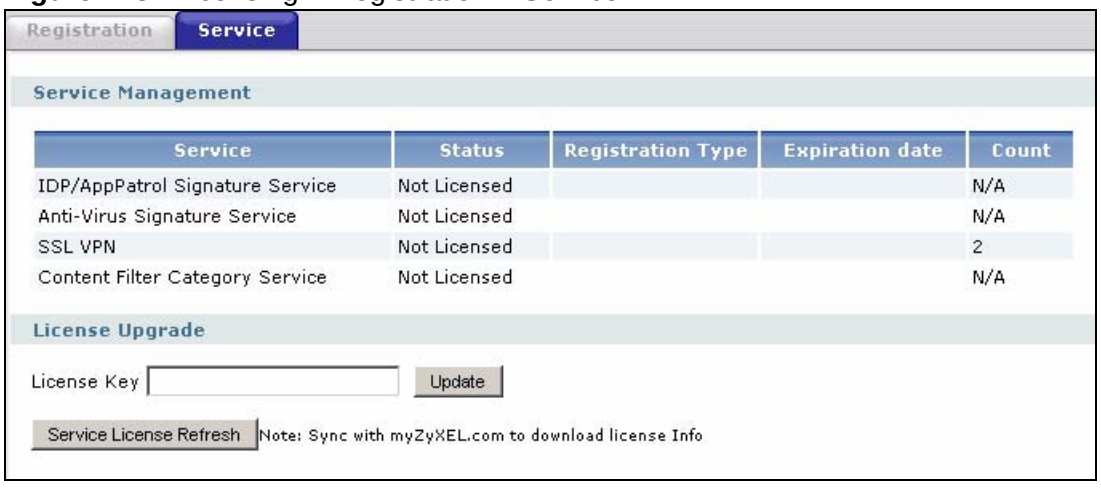
**Figure 127** Licensing > Registration: Registered Device




# 8.3 The Service Screen

Use this screen to display the status of your service registrations and upgrade licenses. To activate or extend a standard service subscription, purchase an iCard and enter the iCard's PIN number (license key) in this screen. Click **Licensing > Registration** > **Service** to open the screen as shown next.

**Figure 128** Licensing > Registration > Service



The following table describes the labels in this screen.

**Table 40** Licensing > Registration > Service

| LABEL | DESCRIPTION |
|---|---|
| Service Management | |
| Service | This lists the services that available on the ZyWALL. |
| Status | This field displays whether a service is activated (**Licensed**) or not (**Not Licensed**) or expired (**Expired**). |
| Registration Type | This field displays whether you applied for a trial application (**Trial**) or registered a service with your iCard's PIN number (**Standard**). This field is blank when a service is not activated. For an anti-virus service subscription this field also displays the type of anti-virus engine. |
| Expiration date | This field displays the date your service expires.<br>You can continue to use IDP/AppPatrol or Anti-Virus after the registration expires, you just won't receive updated signatures. |
| Count | This field displays how many VPN tunnels you can use with your current license. This field does not apply to the other services. |
| License Upgrade | |
| License Key | Enter your iCard's PIN number and click **Update** to activate or extend a standard service subscription. If a standard service subscription runs out, you need to buy a new iCard (specific to your ZyWALL) and enter the new PIN number to extend the service. |
| Service License Refresh | Click this button to renew service license information (such as the registration status and expiration day). |

# 9

# Signature Update

## 9.1 Overview

This chapter shows you how to update the ZyWALL's signature packages.

### 9.1.1 What You Can Do in the Update Screens

- Use the **Licensing > Update > Anti-virus** screen (Section 9.2 on page 172) to update the anti-virus signatures. See Chapter 30 on page 505 for details on anti-virus.
- Use the **Licensing > Update > IDP/AppPatrol** screen (Section 9.3 on page 173) to update the signatures used for IDP and application patrol. See Chapter 31 on page 521 for details on IDP. See Chapter 29 on page 477 for details on application patrol.
- Use the **Licensing > Update > System Protect** screen (Section 9.4 on page 175) to update the system-protection signatures.

### 9.1.2 What you Need to Know About Signature Updates

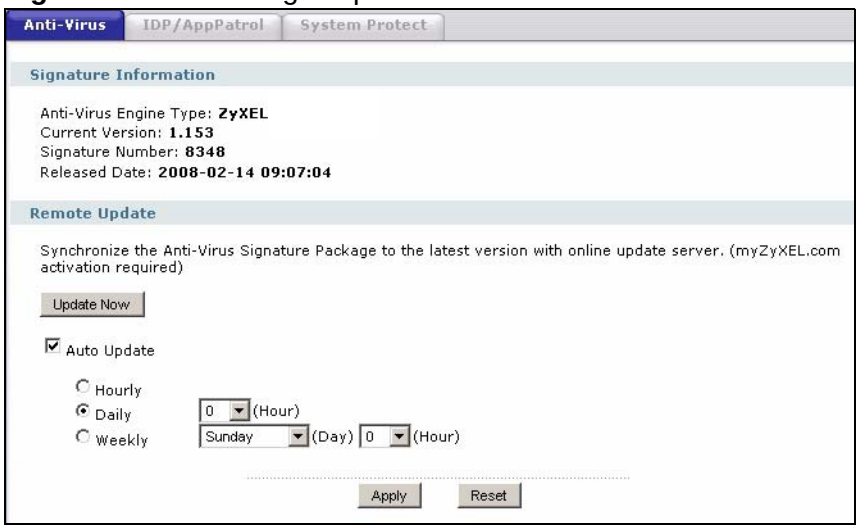
- You need a valid service registration to update the anti-virus signatures and the IDP/AppPatrol signatures.
- You do not need a service registration to update the system-protection signatures.
- Schedule signature updates for a day and time when your network is least busy to minimize disruption to your network.
- Your custom signature configurations are not over-written when you download new signatures.

Note: The ZyWALL does not have to reboot when you upload new signatures.

# 9.2 The Antivirus Update Screen

Click **Licensing > Update > Anti-Virus** to display the following screen.

**Figure 129** Licensing > Update >Anti-Virus




The following table describes the labels in this screen.

| LABEL | DESCRIPTION |
|---|---|
| Signature Information | The following fields display information on the current signature set that the ZyWALL is using. |
| Anti-Virus Engine Type | This field displays whether the ZyWALL is set to use ZyXEL's anti-virus engine or the one powered by Kaspersky.<br><br>Upgrading the ZyWALL to firmware version 2.11 and updating the anti-virus signatures automatically upgrades the ZyXEL anti-virus engine to v2.0. v2.0 has more virus signatures and offers improved non-executable file scan throughput. |
| Current Version | This field displays the anti-virus signatures version number currently used by the ZyWALL. This number is defined by the ZyXEL Security Response Team (ZSRT) who maintain and update them.<br><br>This number gets larger as new signatures are added, so you should refer to this number regularly. Go to https://mysecurity.zyxel.com/mysecurity/ to see what the latest version number is. You can also subscribe to signature update e-mail notifications. |
| Signature Number | This field displays the number of signatures in this set. |
| Released Date | This field displays the date and time the set was released. |
| Remote Update | Use these fields to have the ZyWALL check for new signatures at myZyXEL.com. If new signatures are found, they are then downloaded to the ZyWALL. |
| Update Now | Click this button to have the ZyWALL check for new signatures immediately. If there are new ones, the ZyWALL will then download them. |

| LABEL | DESCRIPTION |
|---|---|
| Auto Update | Select this check box to have the ZyWALL automatically check for new signatures regularly at the time and day specified.<br>You should select a time when your network is not busy for minimal interruption. |
| Hourly | Select this option to have the ZyWALL check for new signatures every hour. |
| Daily | Select this option to have the ZyWALL check for new signatures every day at the specified time. The time format is the 24 hour clock, so '23' means 11PM for example. |
| Weekly | Select this option to have the ZyWALL check for new signatures once a week on the day and at the time specified. |
| Apply | Click this button to save your changes to the ZyWALL. |
| Reset | Click this button to return the screen to its last-saved settings. |

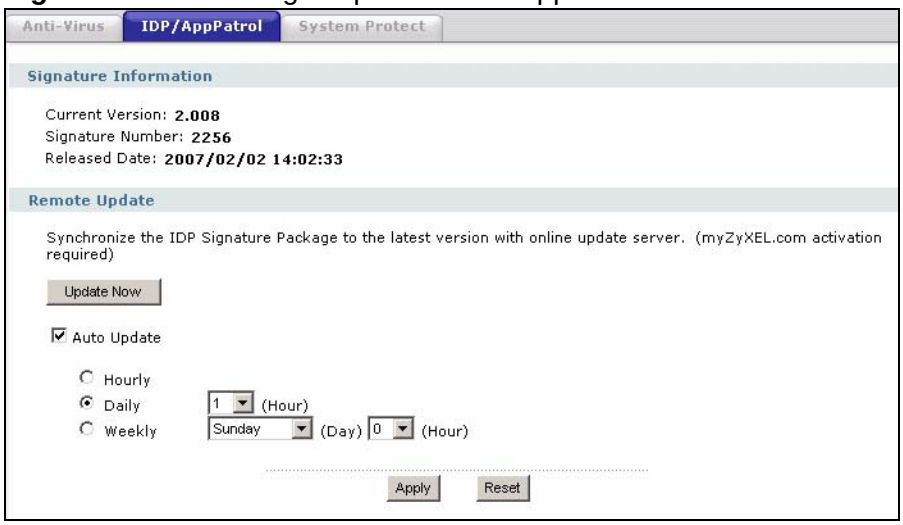
# 9.3 The IDP/AppPatrol Update Screen

Click **Licensing > Update > IDP/AppPatrol** to display the following screen.

The ZyWALL comes with signatures for the IDP and application patrol features. These signatures are continually updated as new attack types evolve. New signatures can be downloaded to the ZyWALL periodically if you have subscribed for the IDP/AppPatrol signatures service.

You need to create an account at myZyXEL.com, register your ZyWALL and then subscribe for IDP service in order to be able to download new packet inspection signatures from myZyXEL.com (see the **Registration** screens). Use the **Update IDP /AppPatrol** screen to schedule or immediately download IDP signatures.

**Figure 130** Licensing > Update > IDP/AppPatrol



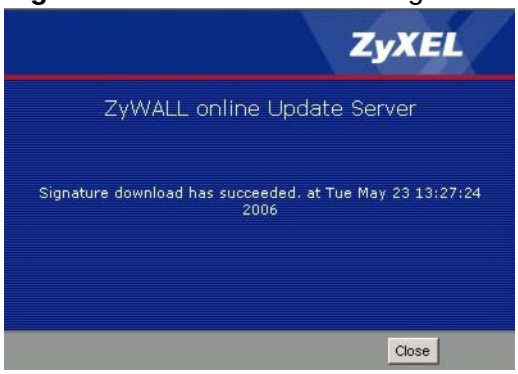
The following table describes the fields in this screen.

**Table 41** Licensing > Update > IDP/AppPatrol

| LABEL | DESCRIPTION |
|---|---|
| Signature Information | The following fields display information on the current signature set that the ZyWALL is using. |
| Current Version | This field displays the IDP signature and anomaly rule set version number. This number gets larger as the set is enhanced. |
| Signature Number | This field displays the number of IDP signatures in this set. This number usually gets larger as the set is enhanced. Older signatures and rules may be removed if they are no longer applicable or have been supplanted by newer ones. |
| Released Date | This field displays the date and time the set was released. |
| Remote Update | Use these fields to have the ZyWALL check for new IDP signatures at myZyXEL.com. If new signatures are found, they are then downloaded to the ZyWALL. |
| Update Now | Click this button to have the ZyWALL check for new IDP signatures immediately. If there are new ones, the ZyWALL will then download them. |
| Auto Update | Select this check box to have the ZyWALL automatically check for new IDP signatures regularly at the time and day specified.<br>You should select a time when your network is not busy for minimal interruption. |
| Hourly | Select this option to have the ZyWALL check for new IDP signatures every hour. |
| Daily | Select this option to have the ZyWALL check for new IDP signatures everyday at the specified time. The time format is the 24 hour clock, so '23' means 11PM for example. |
| Weekly | Select this option to have the ZyWALL check for new IDP signatures once a week on the day and at the time specified. |
| Apply | Click this button to save your changes to the ZyWALL. |
| Reset | Click this button to return the screen to its last-saved settings. |

**Figure 131** Downloading IDP Signatures

**Figure 132** Successful IDP Signature Download

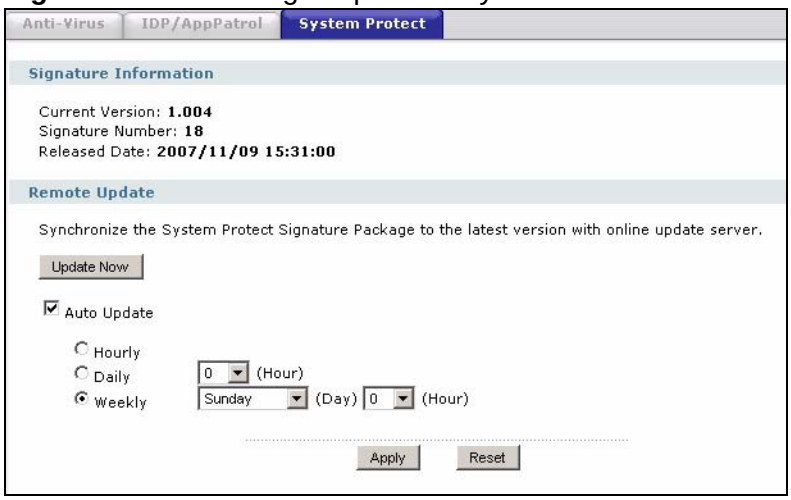



# 9.4 The System Protect Update Screen

Click **Licensing > Update > System Protect** to display the following screen.

Use this screen to schedule or immediately download system-protection signatures. The ZyWALL comes with signatures that it uses to protect itself from intrusions. These signatures are continually updated as new attack types evolve. These system protection signature updates are free and can be downloaded to the ZyWALL periodically. The system-protection function is part of the IDP feature. The system-protection feature is enabled by default and can only be disabled via the commands. You do not need an IDP subscription to use the system-protection feature or to download updated system-protection signatures.

**Figure 133** Licensing > Update > System Protect



The following table describes the fields in this screen.

**Table 42** Licensing > Update > System Protect

| LABEL | DESCRIPTION |
|---|---|
| Signature Information | The following fields display information on the current signature set that the ZyWALL is using. |
| Current Version | This field displays the system protect signature and anomaly rule set version number. This number gets larger as the set is enhanced. |
| Signature Number | This field displays the number of signatures in this set. This number usually gets larger as the set is enhanced. Older signatures and rules may be removed if they are no longer applicable or have been supplanted by newer ones. |
| Released Date | This field displays the date and time the set was released. |
| Remote Update | Use these fields to have the ZyWALL check for new signatures at myZyXEL.com. If new signatures are found, they are then downloaded to the ZyWALL. |
| Update Now | Click this button to have the ZyWALL check for new signatures immediately. If there are new ones, the ZyWALL will then download them. |
| Auto Update | Select this check box to have the ZyWALL automatically check for new signatures regularly at the time and day specified.<br>You should select a time when your network is not busy for minimal interruption. |
| Hourly | Select this option to have the ZyWALL check for new signatures every hour. |
| Daily | Select this option to have the ZyWALL check for new signatures every day at the specified time. The time format is the 24 hour clock, so '23' means 11PM for example. |
| Weekly | Select this option to have the ZyWALL check for new signatures once a week on the day and at the time specified. |
| Apply | Click this button to save your changes to the ZyWALL. |
| Reset | Click this button to return the screen to its last-saved settings. |

**Figure 134** Downloading System Protect Signatures

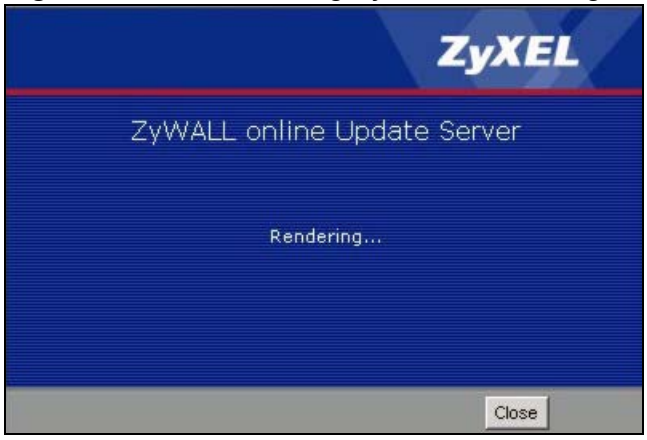
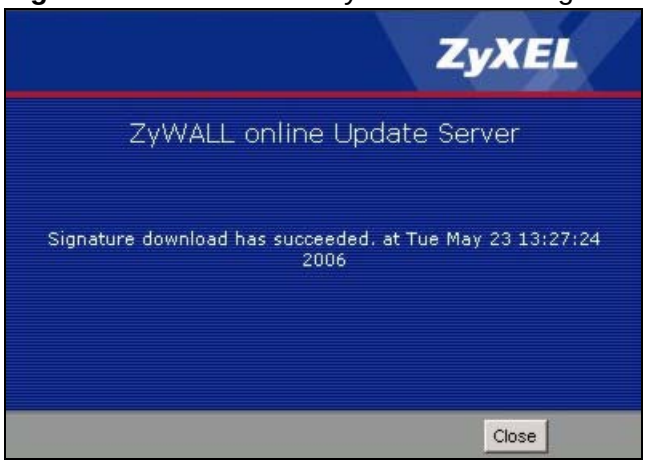


**Figure 135** Successful System Protect Signature Download



# PART II
# Network

# 10

# Interfaces

## 10.1 Interface Overview

Use the **Interface** screens to configure the ZyWALL's interfaces. You can also create interfaces on top of other interfaces.

- **Ports** are the physical ports to which you connect cables.
- **Interfaces** are used within the system operationally. You use them in configuring various features. An interface also describes a network that is directly connected to the ZyWALL. For example, You connect the LAN1 network to the LAN1 interface.
- **Zones** are groups of interfaces used to ease security policy configuration.

### 10.1.1 What You Can Do in the Interface Screens

- Use the **Status** screen (Section 10.2 on page 185) to see all of the ZyWALL's interfaces and their packet statistics.
- Use the **Port Grouping** screens (Section 10.3 on page 188) to create port groups and to assign physical ports and port groups to Ethernet interfaces.
- Use the **Ethernet** screens (Section 10.4 on page 189) to configure the Ethernet interfaces. Ethernet interfaces are the foundation for defining other interfaces and network policies. RIP and OSPF are also configured in these interfaces.
- Use the **PPP** screens (Section 10.7 on page 207) for PPPoE or PPTP Internet connections.
- Use the **Cellular** screens (Section 10.8 on page 212) to configure settings for interfaces for Internet connections through an installed 3G card.
- Use the **WLAN** screens (Section 10.10 on page 221) to configure settings for interfaces on a wireless LAN card.
- Use the **VLAN** screens (Section 10.13 on page 237) to divide the physical network into multiple logical networks. VLAN interfaces receive and send tagged frames. The ZyWALL automatically adds or removes the tags as needed. Each VLAN can only be associated with one Ethernet interface.
- Use the **Bridge** screens (Section 10.14 on page 245) to combine two or more network segments into a single network.
- Use the **Auxiliary** screens (Section 10.15 on page 253) to configure the ZyWALL's auxiliary interface to use an external modem.

- Use the **Virtual Interface** screen (Section 10.16 on page 256) to create virtual interfaces on top of Ethernet interfaces to tell the ZyWALL where to route packets. You can create virtual Ethernet interfaces, virtual VLAN interfaces, and virtual bridge interfaces.
- Use the **Trunks** screens (Chapter 11 on page 263) to configure load balancing.

## 10.1.2 What You Need to Know About Interfaces

### Interface Characteristics

Interfaces generally have the following characteristics (although not all characteristics apply to each type of interface).

- An interface is a logical entity through which (layer-3) packets pass.
- An interface is bound to a physical port or another interface.
- Many interfaces can share the same physical port.
- An interface belongs to at most one zone.
- Many interfaces can belong to the same zone.
- Layer-3 virtualization (IP alias, for example) is a kind of interface.

### Types of Interfaces

You can create several types of interfaces in the ZyWALL.

- Setting interfaces to the same port role forms a port group. Port groups create a hardware connection between physical ports at the layer-2 (data link, MAC address) level.
- **Ethernet interfaces** are the foundation for defining other interfaces and network policies. RIP and OSPF are also configured in these interfaces.
- **VLAN interfaces** receive and send tagged frames. The ZyWALL automatically adds or removes the tags as needed. Each VLAN can only be associated with one Ethernet interface.
- **Bridge interfaces** create a software connection between Ethernet or VLAN interfaces at the layer-2 (data link, MAC address) level. Unlike port groups, bridge interfaces can take advantage of some security features in the ZyWALL. You can also assign an IP address and subnet mask to the bridge.
- **PPP interfaces** support Point-to-Point Protocols (PPP). ISP accounts are required for PPPoE/PPTP interfaces.
- **Cellular interfaces** are for 3G WAN connections via a connected 3G device.
- **WLAN interfaces** are for wireless LAN (IEEE 802.11b/g) connections via an installed wireless LAN card.
- **Virtual interfaces** provide additional routing information in the ZyWALL. There are three types: **virtual Ethernet interfaces**, **virtual VLAN interfaces**, and **virtual bridge interfaces**.

- The **auxiliary interface**, along with an external modem, provides an interface the ZyWALL can use to dial out. This interface can be used as a backup WAN interface, for example. The auxiliary interface controls the **AUX** port.
- **Trunks** manage load balancing between interfaces.

Port groups, trunks, and the auxiliary interface have a lot of characteristics that are specific to each type of interface. See Section 10.3 on page 188, Chapter 11 on page 263, and Section 10.15 on page 253 for details. The other types of interfaces--Ethernet, PPP, cellular, VLAN, bridge, and virtual--have a lot of similar characteristics. These characteristics are listed in the following table and discussed in more detail below.

**Table 43** Ethernet, PPP, Cellular, VLAN, Bridge, and Virtual Interface Characteristics

| CHARACTERISTICS | ETHERNET | ETHERNET | ETHERNET | PPP | CELLULAR | VLAN | BRIDGE | VIRTUAL |
|---|---|---|---|---|---|---|---|---|
| Name* | opt | wan1, wan2 | lan1, lan2, ext-wlan, dmz | ppp *x* | cellular*x* | vlan*x* | br*x* | ** |
| Configurable Zone | Yes | No | No | No | No | Yes | Yes | No |
| IP Address Assignment | | | | | | | | |
| Static IP address | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| DHCP client | Yes | Yes | No | Yes | Yes | Yes | Yes | No |
| Routing metric | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Interface Parameters | | | | | | | | |
| Bandwidth restrictions | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Packet size (MTU) | Yes | Yes | Yes | Yes | Yes | Yes | Yes | No |
| DHCP | | | | | | | | |
| DHCP server | Yes | No | Yes | No | No | Yes | Yes | No |
| DHCP relay | Yes | No | Yes | No | No | Yes | Yes | No |
| Connectivity Check | Yes | Yes | No | Yes | No | Yes | Yes | No |

- Each name consists of 2-4 letters (interface type), followed by a number (*x*). For most interfaces, x is limited by the maximum number of the type of interface. For VLAN interfaces, x is defined by the number you enter in the VLAN name field. For example, Ethernet interface names are wan1, wan2, opt, lan1, lan2, ext-wlan, dmz; VLAN interfaces are vlan0, vlan1, vlan2, ...; and so on.

** - The names of virtual interfaces are derived from the interfaces on which they are created. For example, virtual interfaces created on Ethernet interface wan1 are called wan1:1, wan1:2, and so on. Virtual interfaces created on VLAN interface vlan2 are called vlan2:1, vlan2:2, and so on. You cannot specify the number after the colon(:) in the web configurator; it is a sequential number. You can specify the number after the colon if you use the CLI to set up a virtual interface.

## Relationships Between Interfaces

In the ZyWALL, interfaces are usually created on top of other interfaces. Only Ethernet interfaces are created directly on top of the physical ports or port groups. The relationships between interfaces are explained in the following table.

**Table 44** Relationships Between Different Types of Interfaces

| INTERFACE | REQUIRED PORT / INTERFACE |
|---|---|
| auxiliary interface | auxiliary port |
| port group | physical port |
| Ethernet interface | physical port<br>port group |
| VLAN interface | Ethernet interface |
| bridge interface | Ethernet interface*<br>WLAN interface*<br>VLAN interface* |
| PPP interface | WAN1, WAN2, OPT* |
| virtual interface<br>(virtual Ethernet interface)<br>(virtual VLAN interface)<br>(virtual bridge interface) | Ethernet interface*<br>VLAN interface*<br>bridge interface |
| trunk | Ethernet interface<br>Cellular interface<br>VLAN interface<br>bridge interface<br>PPP interface<br>auxiliary interface |

* - You cannot set up a PPP interface, virtual Ethernet interface or virtual VLAN interface if the underlying interface is a member of a bridge. You also cannot add an Ethernet interface or VLAN interface to a bridge if the member interface has a virtual interface or PPP interface on top of it.

## Finding Out More

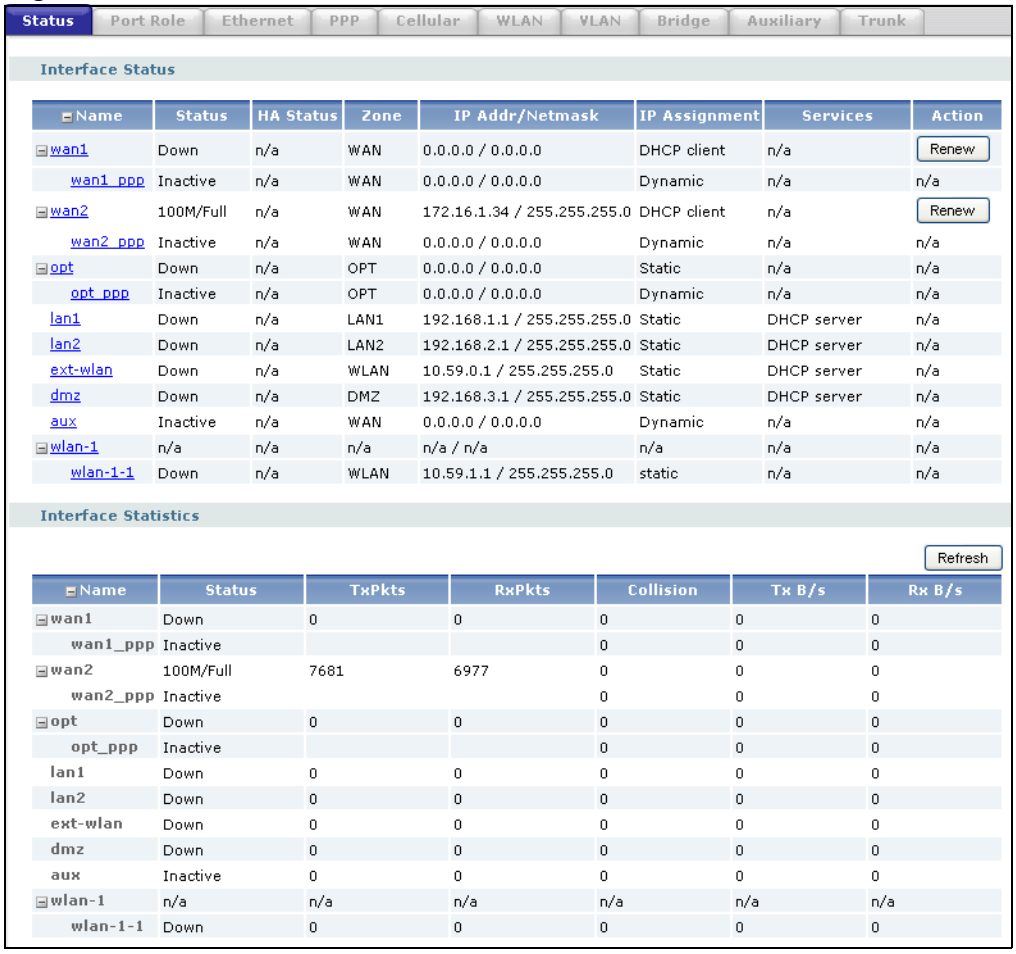
- See Section 5.2 on page 82 details on the differences between physical ports, interfaces, and zones in the ZyWALL.
- See Section 5.4.2 on page 87 for related information about the **Interface** screens.
- See Section 10.17 on page 257 for background information on interfaces.

- See Section 6.1 on page 101 for an example of configuring Ethernet interfaces and port groups.
- See Section 6.2 on page 106 for an example of configuring a cellular (3G) interface.
- See Section 6.4 on page 110 for an example of configuring a WLAN interface.
- See Chapter 11 on page 263 to configure load balancing using trunks.

# 10.2 Interface Status Screen

This screen lists all of the ZyWALL's interfaces and gives packet statistics for them. Click **Network** > **Interface** to access this screen.

**Figure 136** Network > Interface > Status



Each field is described in the following table.

**Table 45** Network > Interface > Status

| LABEL | DESCRIPTION |
|---|---|
| Interface Status | If an Ethernet interface does not have any physical ports associated with it, its entry is displayed in light gray text. |
| Expand/Close | Click this button to show or hide statistics for all the virtual interfaces on top of the Ethernet interfaces. |
| Name | This field displays the name of each interface. If there is a **Expand** icon (plus-sign) next to the name, click this to look at the status of virtual interfaces on top of this interface. |
| Status | This field displays the current status of each interface. The possible values depend on what type of interface it is.<br><br>For Ethernet interfaces:<br><br>**Inactive** - The Ethernet interface is disabled.<br><br>**Down** - The Ethernet interface does not have any physical ports associated with it or the Ethernet interface is enabled but not connected.<br><br>**Speed / Duplex** - The Ethernet interface is enabled and connected. This field displays the port speed and duplex setting (**Full** or **Half**).<br><br>For cellular (3G) interfaces, see Section 10.9 on page 219 for the status that can appear.<br><br>For the auxiliary interface:<br><br>**Inactive** - The auxiliary interface is disabled.<br><br>**Connected** - The auxiliary interface is enabled and connected.<br><br>**Disconnected** - The auxiliary interface is not connected.<br><br>For virtual interfaces, this field always displays **Up**. If the virtual interface is disabled, it does not appear in the list.<br><br>For VLAN and bridge interfaces, this field always displays **Up**. If the VLAN or bridge interface is disabled, it does not appear in the list.<br><br>For PPP interfaces:<br><br>**Connected** - The PPP interface is connected.<br><br>**Disconnected** - The PPP interface is not connected.<br><br>If the PPPP interface is disabled, it does not appear in the list.<br><br>For WLAN interfaces:<br><br>**Up** - The WLAN interface is enabled.<br><br>**Down** - The WLAN interface is disabled. |

**Table 45** Network > Interface > Status (continued)

| LABEL | DESCRIPTION |
|---|---|
| HA Status | This field displays the status of the interface in the virtual router.<br>**Active** - This interface is the master interface in the virtual router.<br>**Stand-By** - This interface is a backup interface in the virtual router.<br>**Fault** - This VRRP group is not functioning in the virtual router right now. For example, this might happen if the interface is down.<br>**n/a** - Device HA is not active on the interface. |
| Zone | This field displays the zone to which the interface is assigned. |
| IP Addr/ Netmask | This field displays the current IP address and subnet mask assigned to the interface. If the IP address and subnet mask are 0.0.0.0, the interface is disabled or did not receive an IP address and subnet mask via DHCP.<br>If this interface is a member of an active virtual router, this field displays the IP address it is currently using. This is either the static IP address of the interface (if it is the master) or the management IP address (if it is a backup). |
| IP Assignment | This field displays how the interface gets its IP address.<br>**Static** - This interface has a static IP address.<br>**DHCP Client** - This interface gets its IP address from a DHCP server.<br>**Dynamic** - This is the auxiliary interface. |
| Services | This field lists which services the interface provides to the network. Examples include **DHCP relay**, **DHCP server**, **DDNS**, **RIP**, and **OSPF**. This field displays **n/a** if the interface does not provide any services to the network. |
| Action | Use this field to get or to update the IP address for the interface. Click **Renew** to send a new DHCP request to a DHCP server. Click **Connect** to try to connect the auxiliary interface or a PPPoE/PPTP interface. If the interface cannot use one of these ways to get or to update its IP address, this field displays **n/a**. |
| Interface Statistics | This table provides packet statistics for each interface. |
| Refresh | Click this button to update the information in the screen. |
| Expand/Close | Click this button to show or hide statistics for all the virtual interfaces on top of the Ethernet interfaces. |
| Name | This field displays the name of each interface. If there is a **Expand** icon (plus-sign) next to the name, click this to look at the statistics for virtual interfaces on top of this interface. |
| Status | This field displays the current status of the interface.<br>**Down** - The interface is not connected.<br>**Speed / Duplex** - The interface is connected. This field displays the port speed and duplex setting (**Full** or **Half**). |
| TxPkts | This field displays the number of packets transmitted from the ZyWALL on the interface since it was last connected. |

**Table 45** Network > Interface > Status (continued)

| LABEL | DESCRIPTION |
|---|---|
| RxPkts | This field displays the number of packets received by the ZyWALL on the interface since it was last connected. |
| Collision | This field displays the number of collisions on the interface since it was last connected. |
| Tx B/s | This field displays the transmission speed, in bytes per second, on the interface in the one-second interval before the screen updated. |
| Rx B/s | This field displays the reception speed, in bytes per second, on the interface in the one-second interval before the screen updated. |

# 10.3 Port Roles

**Figure 137** Network > Interface > Port Grouping

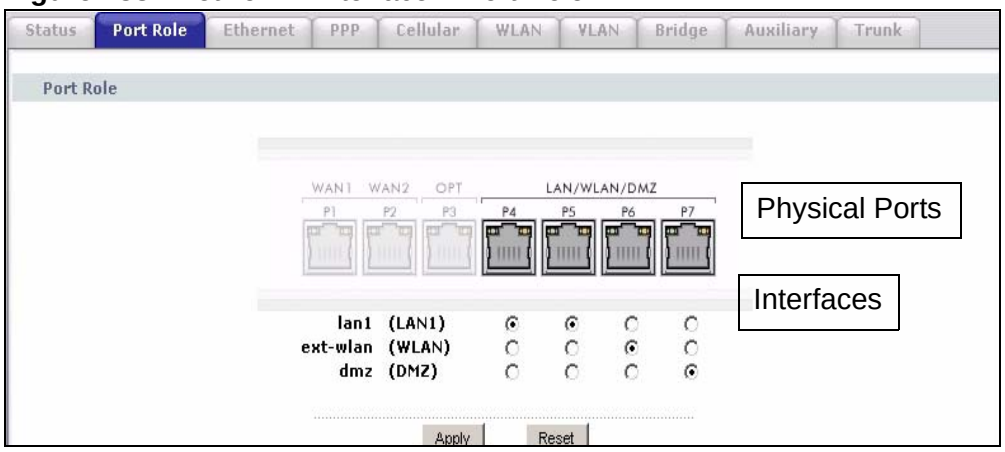
To access this screen, click **Network** > **Interface** > **Port Role**. Use the **Port Role** screen to set the ZyWALL's flexible ports as part of the **lan1**, **lan2**, **ext-wlan** or **dmz** interfaces. This creates a hardware connection between the physical ports at the layer-2 (data link, MAC address) level. This provides wire-speed throughput but no security.

Not the following if you are configuring from a computer connected to a **lan1**, **lan2**, **ext-wlan** or **dmz** port and change the port's role:

1 A port's IP address varies as its role changes, make sure your computer's IP address is in the same subnet as the ZyWALL's **lan1**, **lan2**, **ext-wlan** or **dmz** IP address.

2 Use the appropriate **lan1**, **lan2**, **ext-wlan** or **dmz** IP address to access the ZyWALL.

**Figure 138** Network > Interface > Port Role



Each section in this screen is described below.

**Table 46** Network > Interface > Port Role

| LABEL | DESCRIPTION |
|---|---|
| LAN1/WLAN/DMZ PX~P7 | These are physical Ethernet ports. |
| lan1 (LAN1)<br>lan2 (LAN2)<br>ext-wlan (WLAN)<br>dmz (DMZ) | These are Ethernet interfaces and the zone to which each belongs. Use the radio buttons to select for which interface (network) you want to use each physical port. For example, select a port's **LAN1** radio button to use the port as part of the lan1 interface. The port will use the ZyWALL's lan1 IP address and MAC address.<br>When you assign more than one physical port to a network, you create a **port group**. Port groups have the following characteristics:<br>• There is a layer-2 Ethernet switch between physical ports in the port group. This provides wire-speed throughput but no security.<br>• It can increase the bandwidth between the port group and other interfaces.<br>• The port group uses a single MAC address. |
| Apply | Click this button to save your changes and apply them to the ZyWALL. |
| Reset | Click this button to change the port groups to their current configuration (last-saved values). |

# 10.4 Ethernet Summary Screen

This screen lists every Ethernet interface and virtual interface created on top of Ethernet interfaces. To access this screen, click **Network** > **Interface**.

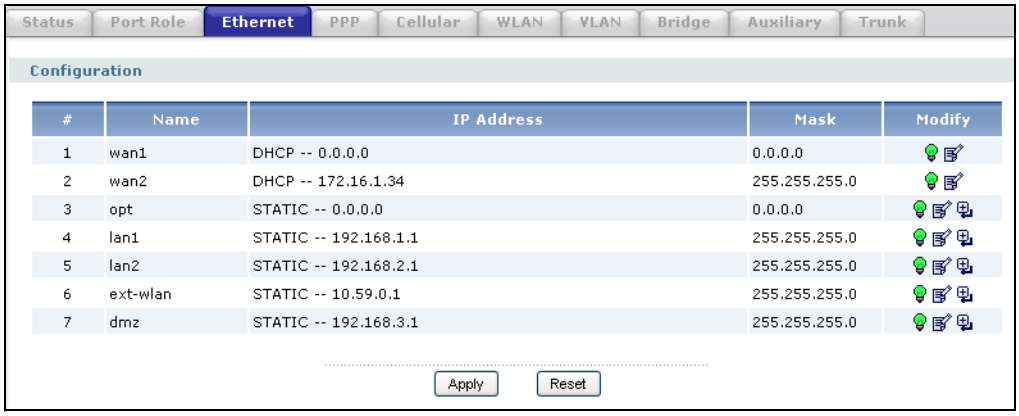
Unlike other types of interfaces, you cannot create new Ethernet interfaces nor can you delete any of them. If an Ethernet interface does not have any physical ports assigned to it (see Section 10.3 on page 188), the Ethernet interface is effectively removed from the ZyWALL, but you can still configure it.

Ethernet interfaces are similar to other types of interfaces in many ways. They have an IP address, subnet mask, and gateway used to make routing decisions. They restrict the amount of bandwidth and packet size. They can provide DHCP services, and they can verify the gateway is available.

Use Ethernet interfaces to control which physical ports exchange routing information with other routers and how much information is exchanged through each one. The more routing information is exchanged, the more efficient the routers should be. However, the routers also generate more network traffic, and some routing protocols require a significant amount of configuration and management. The ZyWALL supports two routing protocols, RIP and OSPF. See

Chapter 13 on page 285 for background information about these routing protocols.

**Figure 139** Network > Interface > Ethernet




Each field is described in the following table.

**Table 47** Network > Interface > Ethernet

| LABEL | DESCRIPTION |
|---|---|
| # | This field is a sequential value, and it is not associated with any interface. |
| Name | This field displays the name of the interface. |
| IP Address | This field displays the current IP address of the interface. If the IP address is 0.0.0.0, the interface does not have an IP address yet.<br><br>This screen also shows whether the IP address is a static IP address (**STATIC**) or dynamically assigned (**DHCP**). IP addresses are always static in virtual interfaces. |
| Mask | This field displays the interface's subnet mask in dot decimal notation. |
| Modify | This column lets you create, edit, remove, activate, and deactivate interfaces. You cannot add or remove Ethernet interfaces, however.<br><br>To create a virtual Ethernet interface, click the **Add** icon next to the corresponding Ethernet interface. The **Virtual Interface Add/Edit** screen appears. See Section 10.16 on page 256.<br><br>To edit an interface, click the **Edit** icon next to it. The **Ethernet Edit** screen or **Virtual Interface Add/Edit** screen appears accordingly.<br><br>To remove a virtual interface, click the **Remove** icon next to it. The ZyWALL confirms you want to remove it before doing so.<br><br>To activate or deactivate an interface, click the **Active** icon next to it. Make sure you click **Apply** to save and apply the change. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 10.4.1 Ethernet Edit

The **Ethernet Edit** screen lets you configure IP address assignment, interface parameters, RIP settings, OSPF settings, DHCP settings, connectivity check, and MAC address settings. To access this screen, click an **Edit** icon in the **Ethernet Summary** screen. (See Section 10.4 on page 189.)

For the WAN and OPT interfaces you can click the **Wizard** tab to configure just the key settings. See Section 10.5 on page 198 for details.

The OPT interface's **Edit > Configuration** screen is shown here as an example. The screens for other interfaces are similar and contain a subset to the OPT interface screen's fields.

Note: If you create IP address objects based on an interface's IP address, subnet, or gateway, the ZyWALL automatically updates every rule or setting that uses the object whenever the interface's IP address settings change. For example, if you change LAN1's IP address, the ZyWALL automatically updates the corresponding interface-based, LAN1 subnet address object.

With RIP, you can use Ethernet interfaces to do the following things.

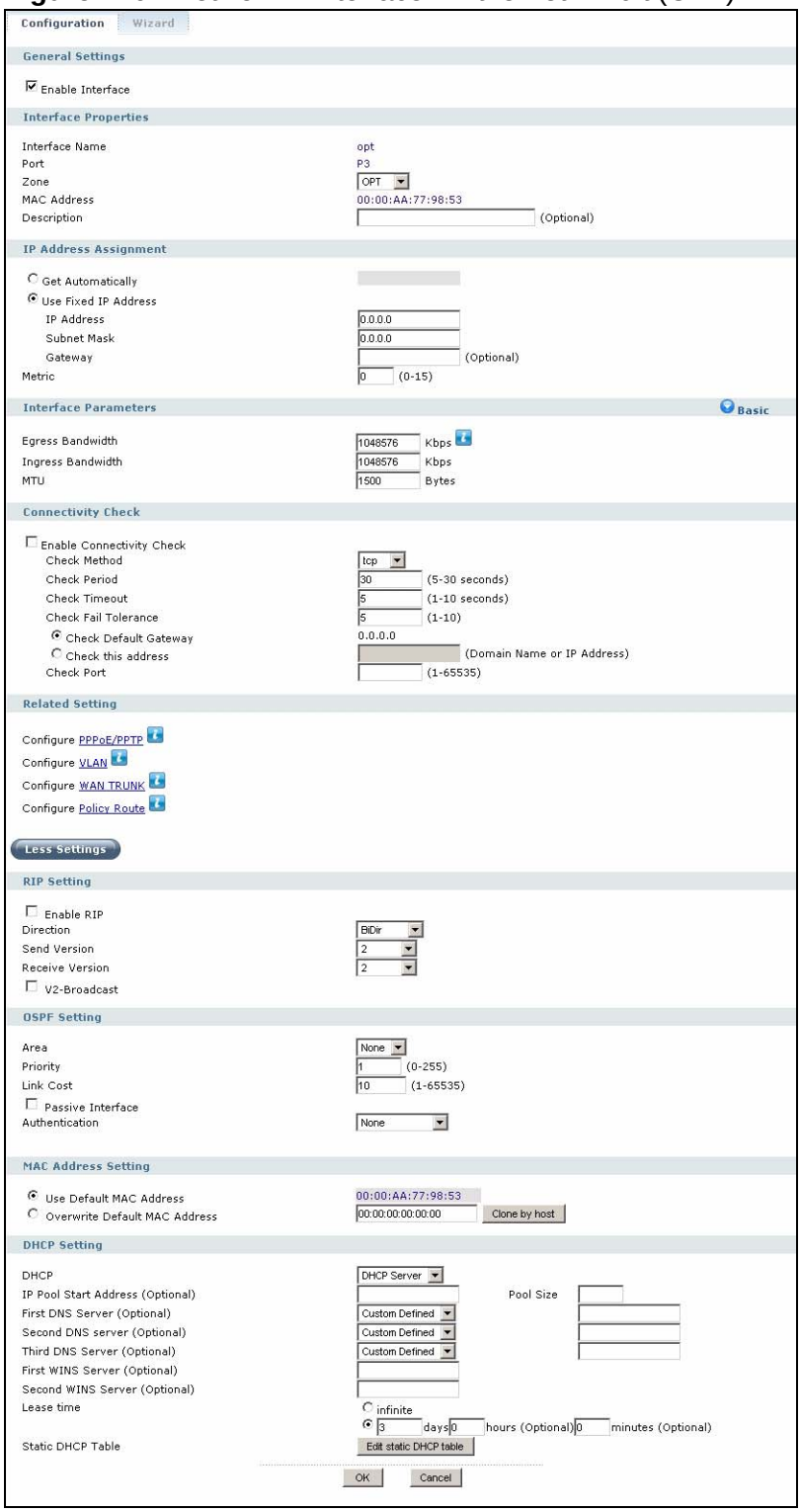
- Enable and disable RIP in the underlying physical port or port group.
- Select which direction(s) routing information is exchanged - The ZyWALL can receive routing information, send routing information, or do both.
- Select which version of RIP to support in each direction - The ZyWALL supports RIP-1, RIP-2, and both versions.
- Select the broadcasting method used by RIP-2 packets - The ZyWALL can use subnet broadcasting or multicasting.

With OSPF, you can use Ethernet interfaces to do the following things.

- Enable and disable OSPF in the underlying physical port or port group.
- Select the area to which the interface belongs.
- Override the default link cost and authentication method for the selected area.
- Select in which direction(s) routing information is exchanged - The ZyWALL can receive routing information, send routing information, or do both.

- Set the priority used to identify the DR or BDR if one does not exist.

**Figure 140** Network > Interface > Ethernet > Edit (OPT)



Each field is described in the table below.

**Table 48** Network > Interface > Ethernet > Edit

| LABEL | DESCRIPTION |
|---|---|
| General Settings | |
| Enable Interface | Select this to enable this interface. Clear this to disable this interface. |
| Interface Properties | |
| Interface Name | This field is read-only. This is the name of the Ethernet interface. |
| MAC Address | This field is read-only. This is the MAC address that the Ethernet interface uses. |
| Description | Enter a description of this interface. It is not used elsewhere. You can use alphanumeric and ( )+/:=?!*#@$_%- characters, and it can be up to 60 characters long. |
| IP Address Assignment | These IP address fields configure an IP address on the interface itself. If you change this IP address on the interface, you may also need to change a related address object for the network connected to the interface. For example, if you use this screen to change the IP address of your LAN interface, you should also change the corresponding LAN subnet address object. |
| Get Automatically | Select this to make the interface a DHCP client and automatically get the IP address, subnet mask, and gateway address from a DHCP server.<br><br>You should not select this if the interface is assigned to a VRRP group. See Chapter 36 on page 629. |
| Use Fixed IP Address | Select this if you want to specify the IP address, subnet mask, and gateway manually. |
| IP Address | This field is enabled if you select **Use Fixed IP Address**.<br><br>Enter the IP address for this interface. |
| Subnet Mask | This field is enabled if you select **Use Fixed IP Address**.<br><br>Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network. |
| Gateway | This field is enabled if you select **Use Fixed IP Address**.<br><br>Enter the IP address of the gateway. The ZyWALL sends packets to the gateway when it does not know how to route the packet to its destination. The gateway should be on the same network as the interface. |
| Metric | Enter the priority of the gateway (if any) on this interface. The ZyWALL decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the ZyWALL uses the one that was configured first. |
| Interface Parameters | |

**Table 48** Network > Interface > Ethernet > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Egress Bandwidth | Enter the maximum amount of traffic, in kilobits per second, the ZyWALL can send through the interface to the network. Allowed values are 0 - 1048576. |
| Ingress Bandwidth | This is reserved for future use.<br>Enter the maximum amount of traffic, in kilobits per second, the ZyWALL can receive from the network through the interface. Allowed values are 0 - 1048576. |
| MTU | Maximum Transmission Unit. Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the ZyWALL divides it into smaller fragments. Allowed values are 576 - 1500. Usually, this value is 1500. |
| Connectivity Check | The interface can regularly check the connection to the gateway you specified to make sure it is still available. You specify how often the interface checks the connection, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the ZyWALL stops routing to the gateway. The ZyWALL resumes routing to the gateway the first time the gateway passes the connectivity check. |
| Enable Connectivity Check | Select this to turn on the connection check. |
| Check Method | Select the method that the gateway allows.<br>Select **icmp** to have the ZyWALL regularly ping the gateway you specify to make sure it is still available.<br>Select **tcp** to have the ZyWALL regularly perform a TCP handshake with the gateway you specify to make sure it is still available. |
| Check Period | Enter the number of seconds between connection check attempts. |
| Check Timeout | Enter the number of seconds to wait for a response before the attempt is a failure. |
| Check Fail Tolerance | Enter the number of consecutive failures before the ZyWALL stops routing through the gateway. |
| Check Default Gateway | Select this to use the default gateway for the connectivity check. |
| Check this address | Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it. |
| Check Port | This field only displays when you set the **Check Method** to **tcp**. Specify the port number to use for a TCP connectivity check. |
| DHCP Setting | |

**Table 48** Network > Interface > Ethernet > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| DHCP | Select what type of DHCP service the ZyWALL provides to the network. Choices are:<br><br>**None** - the ZyWALL does not provide any DHCP services. There is already a DHCP server on the network.<br><br>**DHCP Relay** - the ZyWALL routes DHCP requests to one or more DHCP servers you specify. The DHCP server(s) may be on another network.<br><br>**DHCP Server** - the ZyWALL assigns IP addresses and provides subnet mask, gateway, and DNS server information to the network. The ZyWALL is the DHCP server for the network. |
| | These fields appear if the ZyWALL is a **DHCP Relay**. |
| Relay Server 1 | Enter the IP address of a DHCP server for the network. |
| Relay Server 2 | This field is optional. Enter the IP address of another DHCP server for the network. |
| | These fields appear if the ZyWALL is a **DHCP Server**. |
| IP Pool Start Address | Enter the IP address from which the ZyWALL begins allocating IP addresses. If you want to assign a static IP address to a specific computer, click **Edit static DHCP table**.<br><br>If this field is blank, the **Pool Size** must also be blank. In this case, the ZyWALL can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address. |
| Pool Size | Enter the number of IP addresses to allocate. This number must be at least one and is limited by the interface's **Subnet Mask**. For example, if the **Subnet Mask** is 255.255.255.0 and **IP Pool Start Address** is 10.10.10.10, the ZyWALL can allocate 10.10.10.10 to 10.10.10.254, or 245 IP addresses.<br><br>If this field is blank, the **IP Pool Start Address** must also be blank. In this case, the ZyWALL can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address. |
| First DNS Server, Second DNS Server, Third DNS Server | Specify the IP addresses up to three DNS servers for the DHCP clients to use. Use one of the following ways to specify these IP addresses.<br><br>**Custom Defined** - enter a static IP address.<br><br>**From ISP** - select the DNS server that another interface received from its DHCP server.<br><br>**ZyWALL** - the DHCP clients use the IP address of this interface and the ZyWALL works as a DNS relay. |
| First WINS Server, Second WINS Server | Type the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the DHCP clients. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using. |

**Table 48** Network > Interface > Ethernet > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Lease time | Specify how long each computer can use the information (especially the IP address) before it has to request the information again. Choices are:<br><br>**infinite** - select this if IP addresses never expire.<br><br>**days, hours, and minutes** - select this to enter how long IP addresses are valid. |
| Enable IP/MAC Binding | Select this option to have this interface enforce links between specific IP addresses and specific MAC addresses. This stops anyone else from manually using a bound IP address on another device connected to this interface. Use this to make use only the intended users get to use specific IP addresses. |
| Enable Logs for IP/MAC Binding Violation | Select this option to have the ZyWALL generate a log if a device connected to this interface attempts to use an IP address that is bound to another device's MAC address. |
| Edit static DHCP table | Click this to configure static IP addresses for the ZyWALL to assign to computers connected to this interface. See Section 10.6 on page 206. |
| Related Setting | |
| Configure PPPoE/PPTP | Click **PPPoE/PPTP** if this interface's Internet connection uses PPPoE or PPTP. |
| Configure VLAN | Click **VLAN** if you want to configure a VLAN interface for this Ethernet interface. |
| Configure WAN TRUNK | Click **WAN TRUNK** to go to a screen where you can set this interface to be part of a WAN trunk for load balancing. |
| Configure Policy Route | Click **Policy Route** to go to the screen where you can manually configure a policy route to associate traffic with this interface. |
| More Settings/ Less Settings | Click this button to display a greater or lesser number of configuration fields. |
| RIP Setting | See Section 13.2 on page 286 for more information about RIP. |
| Enable RIP | Select this to enable RIP in this interface. |
| Direction | This field is effective when RIP is enabled. Select the RIP direction from the drop-down list box.<br><br>**BiDir** - This interface sends and receives routing information.<br><br>**In-Only** - This interface receives routing information.<br><br>**Out-Only** - This interface sends routing information. |
| Send Version | This field is effective when RIP is enabled. Select the RIP version(s) used for sending RIP packets. Choices are **1**, **2**, and **1 and 2**. |
| Receive Version | This field is effective when RIP is enabled. Select the RIP version(s) used for receiving RIP packets. Choices are **1**, **2**, and **1 and 2**. |
| V2-Broadcast | This field is effective when RIP is enabled. Select this to send RIP-2 packets using subnet broadcasting; otherwise, the ZyWALL uses multicasting. |
| OSPF Setting | See Section 13.3 on page 287 for more information about OSPF. |

**Table 48** Network > Interface > Ethernet > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Area | Select the area in which this interface belongs. Select **None** to disable OSPF in this interface. |
| Priority | Enter the priority (between 0 and 255) of this interface when the area is looking for a Designated Router (DR) or Backup Designated Router (BDR). The highest-priority interface identifies the DR, and the second-highest-priority interface identifies the BDR. Set the priority to zero if the interface can not be the DR or BDR. |
| Link Cost | Enter the cost (between 1 and 65,535) to route packets through this interface. |
| Passive Interface | Select this to stop forwarding OSPF routing information from the selected interface. As a result, this interface only receives routing information. |
| Authentication | Select an authentication method, or disable authentication. To exchange OSPF routing information with peer border routers, you must use the same authentication method that they use. Choices are:<br>**Same-as-Area** - use the default authentication method in the area<br>**None** - disable authentication<br>**Text** - authenticate OSPF routing information using a plain-text password<br>**MD5** - authenticate OSPF routing information using MD5 encryption |
| Text Authentication Key | This field is available if the **Authentication** is **Text**. Type the password for text authentication. The key can consist of alphanumeric characters and the underscore, and it can be up to eight characters long. |
| MD5 Authentication ID | This field is available if the **Authentication** is **MD5**. Type the ID for MD5 authentication. The ID can be between 1 and 255. |
| MD5 Authentication Key | This field is available if the **Authentication** is **MD5**. Type the password for MD5 authentication. The password can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long. |
| MAC Address Setting | Have the interface use either the factory assigned default MAC address, a manually specified MAC address, or clone the MAC address of another device or computer. |
| Use Default MAC Address | Select this option to have the interface use the factory assigned default MAC address. By default, the ZyWALL uses the factory assigned MAC address to identify itself. |
| Overwrite Default MAC Address | Select this option to have the interface use a different MAC address. Either enter the MAC address in the fields or click **Clone by host** and enter the IP address of the device or computer whose MAC you are cloning. Once it is successfully configured, the address will be copied to the configuration file. It will not change unless you change the setting or upload a different configuration file. |
| OK | Click **OK** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# 10.5 Interface Wizards

You can use the interface wizard (instead of the regular **Ethernet Edit** screen) to configure a WAN, OPT, or PPP (WAN) interface. To access the interface wizard screens:

- Click **Network > Interface > Ethernet** and then a WAN or OPT interface's **Edit** icon and the **Wizard** tab.
- Or click **Network > Interface > PPP** and then a WAN or OPT interface's **Edit** icon and the **Wizard** tab.

The wizard screens vary by interface and encapsulation type.

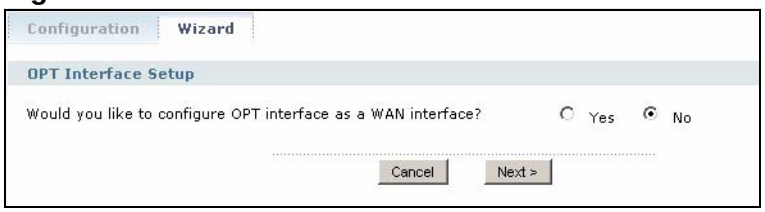
- For the OPT interface, go to Section 10.5.1 on page 198.
- For a WAN interface, go to Section 10.5.2 on page 199.

For a WAN interface, enter the Internet access information exactly as your ISP gave it to you. Leave a field blank if you don't have that information.

## 10.5.1 Interface Wizard: OPT Interface First Screen

This screen displays first when you use the interface wizard for the OPT interface.

**Figure 141** Interface Wizard: OPT Interface First Screen




The following table describes the labels in this screen.

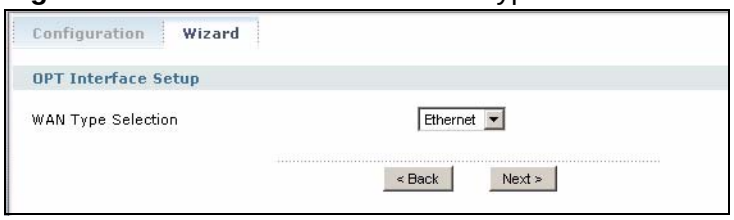
**Table 49** Interface Wizard: OPT Interface First Screen

| LABEL | DESCRIPTION |
|---|---|
| Would you like to configure OPT interface as a WAN interface? | Select **Yes** to use the OPT interface as a WAN interface (for an Internet connection).<br><br>select **No** to use the OPT interface for a local network (similar to a lan1, ext-wlan, or dmz interface). |
| Cancel | Click **Cancel** to exit the wizard without saving your changes. |
| Next | Click **Next** to continue. If you selected **Yes**, go to Section 10.5.2 on page 199.<br><br>If you selected **No**, go to Section 10.5.3 on page 199. |

## 10.5.2 Interface Wizard: WAN Type

This screen appears if you are configuring one of the WAN interfaces or you use the OPT interface for a WAN connection. Select the type of encapsulation this interface uses for its Internet connection.

**Figure 142** Interface Wizard: WAN Type




The following table describes the labels in this screen.

**Table 50** Interface Wizard: WAN Type

| LABEL | DESCRIPTION |
|---|---|
| WAN Type Selection | Choose the **Ethernet** option to use the WAN port as a regular Ethernet.<br>Otherwise, choose **PPPoE** or **PPTP** for a dial-up connection according to the information from your ISP. |
| Back | Click **Back** to return to the previous screen. |
| Next | Click **Next** to continue. Go to Section 10.5.4 on page 201. |

## 10.5.3 Interface Wizard: Non-WAN OPT Interface Setup

This screen displays if you choose to not use the OPT interface for an Internet connection. Configure the OPT interface as an interface for a local network (similar to a LAN or DMZ interface).

**Figure 143** Interface Wizard: Non-WAN OPT Interface Setup

The following table describes the labels in this screen.

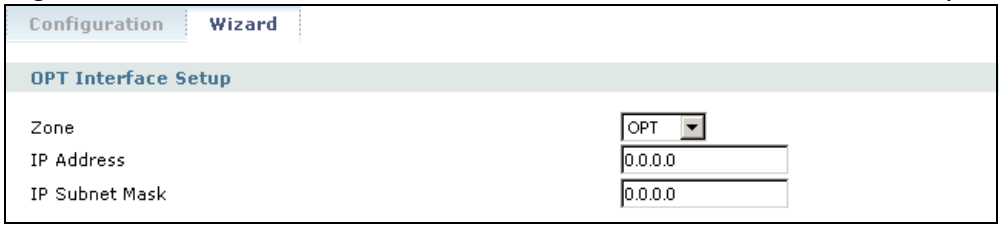
**Table 51** Interface Wizard: Non-WAN OPT Interface Setup

| LABEL | DESCRIPTION |
|---|---|
| Zone | Select the security zone to which you want this interface to belong. |
| IP Address | Enter the IP address for this interface. |
| IP Subnet Mask | Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network. |
| Enable DHCP Server | Select this to have the assign IP addresses and provide subnet mask, gateway, and DNS server information to the network. The ZyWALL is the DHCP server for the network. |
| IP Pool Start Address | Enter the IP address from which the ZyWALL begins allocating IP addresses.<br><br>If this field is blank, the **Pool Size** must also be blank. In this case, the ZyWALL can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address. |
| Pool Size | Enter the number of IP addresses to allocate. This number must be at least one and is limited by the interface's **Subnet Mask**. For example, if the **Subnet Mask** is 255.255.255.0 and **IP Pool Start Address** is 10.10.10.10, the ZyWALL can allocate 10.10.10.10 to 10.10.10.254, or 245 IP addresses.<br><br>If this field is blank, the **IP Pool Start Address** must also be blank. In this case, the ZyWALL can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address. |
| Add default policy routes for WAN access | Select this option to have the ZyWALL automatically configure default policy routes to allow users connected to this interface to access the WAN. Only clear this check box if you want to manually configure policy routes for traffic from the users connected to this interface. |
| Back | Click **Back** to return to the previous screen. |
| Next | Click **Next** to continue to Section 10.5.6 on page 204. |

## 10.5.4 Interface Wizard: WAN Zone and IP Address Assignment

Use this screen to select to which zone the interface belongs and whether is should use a fixed or dynamic IP address.

**Figure 144** Interface Wizard: WAN Interface Zone and IP Address Setup




The following table describes the labels in this screen.

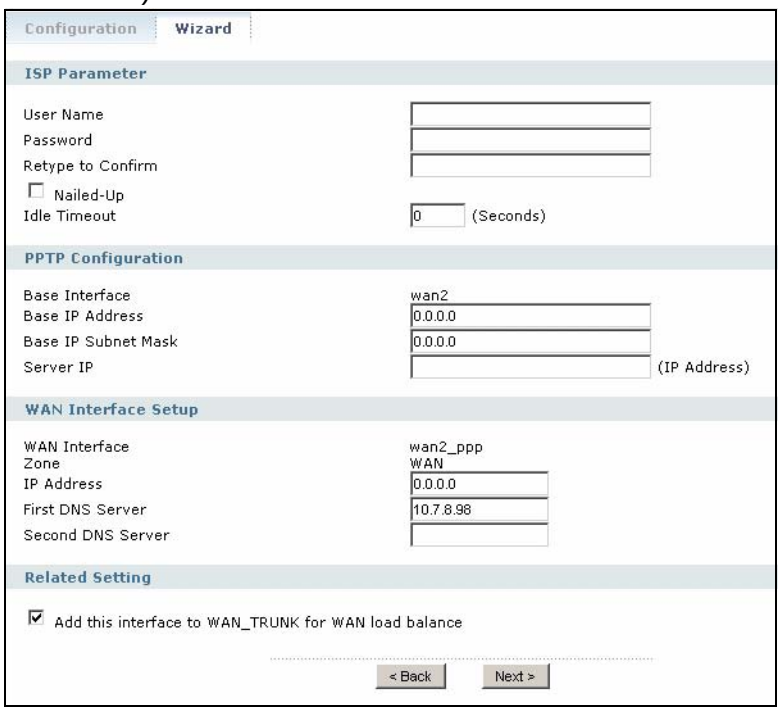
**Table 52** Interface Wizard: WAN Interface Zone and IP Address Setup

| LABEL | DESCRIPTION |
|---|---|
| Zone | Select to which zone this interface and Internet connection will belong to. You configure security policies by zone. |
| IP Address Assignment | Fill in the IP address assigned by your ISP. |
| Subnet Mask | Fill in the subnet mask assigned by your ISP. |
| Back | Click **Back** to return to the previous screen. |
| Next | Click **Next** to continue to Section 10.5.5 on page 202. |

## 10.5.5 Interface Wizard: WAN ISP Connection Settings

Use this screen to configure the ISP and WAN interface settings.

**Figure 145** Interface Wizard: WAN ISP Connection Settings (PPTP, Static IP Shown)




The following table describes the labels in this screen.

**Table 53** Interface Wizard: WAN ISP Connection Settings

| LABEL | DESCRIPTION |
|---|---|
| ISP Parameter | This section appears if the interface uses a PPPoE or PPTP Internet connection. |
| User Name | Type the user name given to you by your ISP. You can use alphanumeric and -_@$./ characters, and it can be up to 31 characters long. |
| Password | Type the password associated with the user name above. Use up to 64 ASCII characters except the [] and ?. This field can be blank. |
| Retype to Confirm | Type your password again for confirmation. |
| Nailed-Up | Select **Nailed-Up** if you do not want the connection to time out. |
| Idle Timeout | Type the time in seconds that elapses before the router automatically disconnects from the PPPoE server. 0 means no timeout. |
| PPTP Configuration | This section only appears if the interface uses a PPPoE or PPTP Internet connection. |
| Base Interface | This displays the identity of the Ethernet interface you configure to connect with a modem or router. |
| Base IP Address | Type the (static) IP address assigned to you by your ISP. |

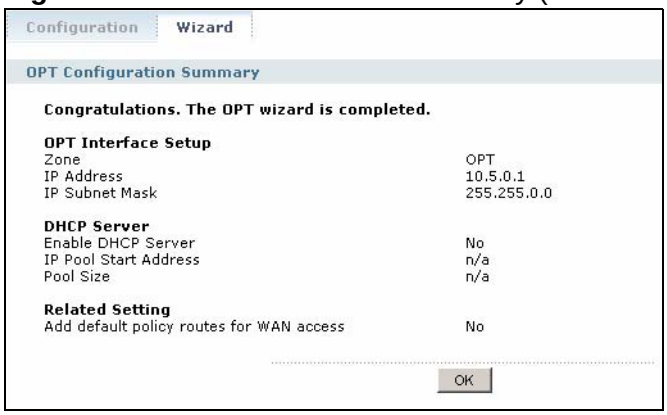
**Table 53** Interface Wizard: WAN ISP Connection Settings

| LABEL | DESCRIPTION |
|---|---|
| IP Subnet Mask | Type the subnet mask assigned to you by your ISP (if given). |
| Server IP | Type the IP address of the PPTP server. |
| WAN Interface Setup | |
| WAN Interface | This displays the identity of the interface you configure to connect with your ISP. |
| Zone | This field displays to which security zone this interface and Internet connection will belong. |
| IP Address | This field is read-only when the WAN interface uses a dynamic IP address. If your WAN interface uses a dynamic IP address, enter it in this field. |
| First DNS Server Second DNS Server | These fields only display for an interface with a static IP address. Enter the DNS server IP address(es) in the field(s) to the right.<br><br>Leave the field as **0.0.0.0** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it.<br><br>DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The ZyWALL uses a system DNS server (in the order you specify here) to resolve domain names for VPN, DDNS and the time server. |
| Related Setting | |
| Add this interface to WAN_TRUNK for WAN load balance. | Select this option to use the interface as part of the default WAN trunk (named “WAN_TRUNK”) for load balancing. This has the ZyWALL send traffic destined for the Internet out through this interface. If you want to only allow certain traffic through this interface, clear this check box and configure policy routes to send traffic through the interface. |
| Back | Click **Back** to return to the previous screen. |
| Next | Click **Next** to continue to Section 10.5.7 on page 205. |

## 10.5.6 Interface Wizard: Summary (Non-WAN)

Use this screen to review the local interface's settings.

**Figure 146** Interface Wizard: Summary (Non-WAN)




The following table describes the labels in this screen.

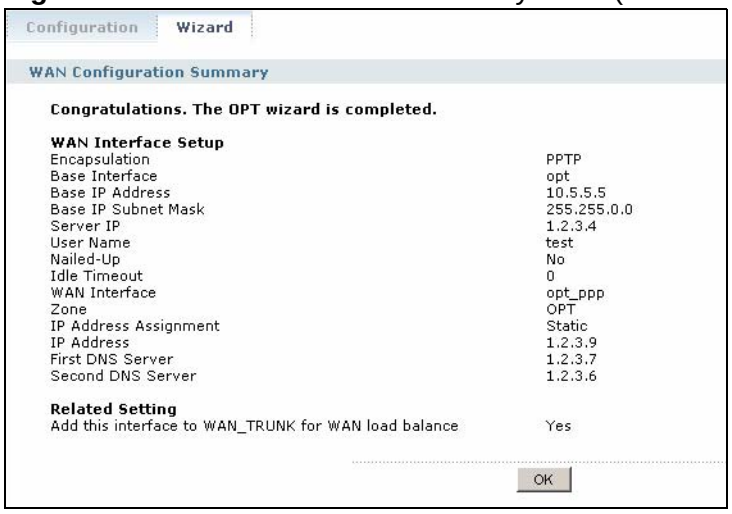
**Table 54** Interface Wizard: Summary (Non-WAN)

| LABEL | DESCRIPTION |
|---|---|
| Zone | This is the security zone to which you want this interface belongs. |
| IP Address | This is the interface's IP address. |
| IP Subnet Mask | This is the interface's subnet mask in dot decimal notation. |
| Enable DHCP Server | This shows whether or not the ZyWALL is the DHCP server for the network connected to this interface. |
| IP Pool Start Address | If the ZyWALL is the DHCP server for the network connected to this interface, this field displays the IP address from which the ZyWALL begins allocating IP addresses. |
| Pool Size | If the ZyWALL is the DHCP server for the network connected to this interface, this field displays how many IP addresses the ZyWALL can allocate. |
| Add default policy routes for WAN access | This shows whether or not the ZyWALL automatically configured default policy routes to allow users connected to this interface to access the WAN. |
| OK | Click **OK** to close the screen. |

## 10.5.7 Interface Wizard: Summary (WAN)

This screen displays the WAN interface's settings.

**Figure 147** Interface Wizard: Summary WAN (PPTP Shown)




The following table describes the labels in this screen.

**Table 55** Interface Wizard: Summary WAN

| LABEL | DESCRIPTION |
|---|---|
| Encapsulation | This displays what encapsulation this interface uses to connect to the Internet. |
| Base Interface | This field only appears for a PPTP interface. It displays the identity of the Ethernet interface for connecting with a modem or router. |
| Base IP Address | This field only appears for a PPTP interface. It displays the (static) IP address assigned to you by your ISP. |
| IP Subnet Mask | This field only appears for a PPTP interface. It displays the subnet mask assigned to you by your ISP (if you entered one). |
| Server IP | This field only appears for a PPTP interface. It displays the IP address of the PPTP server. |
| User Name | Type the user name given to you by your ISP. You can use alphanumeric and -_@$./ characters, and it can be up to 31 characters long. |
| Nailed-Up | Select **Nailed-Up** if you do not want the connection to time out. |
| Idle Timeout | Type the time in seconds that elapses before the router automatically disconnects from the PPPoE server. 0 means no timeout. |
| WAN Interface | This displays the identity of the interface you configure to connect with your ISP. |
| Zone | This field displays to which security zone this interface and Internet connection will belong. |
| IP Address Assignment | This field displays whether the WAN IP address is static or dynamic (**Auto**). |

**Table 55** Interface Wizard: Summary WAN

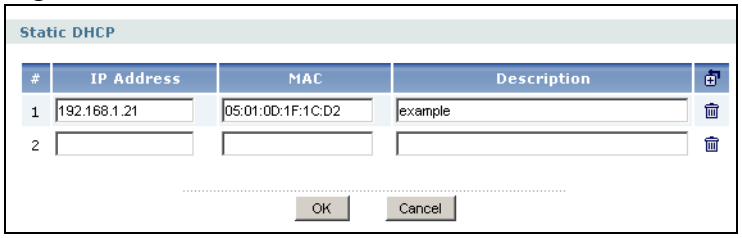
| LABEL | DESCRIPTION |
|---|---|
| First DNS Server<br><br>Second DNS Server | If the **IP Address Assignment** is **Static**, these fields display the DNS server IP address(es). |
| Add this interface to WAN_TRUNK for WAN load balance. | This shows whether or not the interface is part of the default WAN trunk for load balancing. |
| OK | Click **OK** to close the screen. |

# 10.6 The Static DHCP Screen

In an interface add or edit screen, click **Edit static DHCP table** to open the **Static DHCP** screen. Use this screen to configure the list of static IP addresses the ZyWALL assigns to computers connected to the interface. If a computer's MAC address is in the interface's static DHCP table, the ZyWALL assigns the corresponding IP address. Otherwise, the ZyWALL assigns an IP address dynamically using the interface's **IP Pool Start Address** and **Pool Size**.

You must click **OK** in the **Static DHCP** screen and then click **OK** in the interface add or edit screen to save your changes.

**Figure 148** Static DHCP




The following table describes this screen.

**Table 56** Static DHCP

| LABEL | DESCRIPTION |
|---|---|
| # | This field is a sequential value, and it is not associated with a specific entry. |
| IP Address | Enter the IP address to assign to a device with this entry's MAC address. |
| MAC Address | Enter the MAC address to which to assign this entry's IP address. |
| Description | Enter a description to help identify this static DHCP entry. You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 60 characters long. |

**Table 56** Static DHCP

| LABEL | DESCRIPTION |
|---|---|
| Add icon | This column lets you create and remove static DHCP entries.<br>To add an entry, click the **Add** icon.<br>To remove an entry, click it's **Remove** icon. |
| OK | Click **OK** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# 10.7 PPP Interfaces

Use PPPoE/PPTP interfaces to connect to your ISP. This way, you do not have to install or manage PPPoE/PPTP software on each computer in the network.

**Figure 149** Example: PPPoE/PPTP Interfaces


PPPoE/PPTP interfaces are similar to other interfaces in some ways. They have an IP address, subnet mask, and gateway used to make routing decisions; they restrict bandwidth and packet size; and they can verify the gateway is available. There are two main differences between PPPoE/PPTP interfaces and other interfaces.

- You must have an ISP account before you create a PPPoE/PPTP interface.
- You do not set up the subnet mask or gateway.

  PPPoE/PPTP interfaces are interfaces between the ZyWALL and only one computer. Therefore, the subnet mask is always 255.255.255.255. In addition, the ZyWALL always treats the ISP as a gateway.

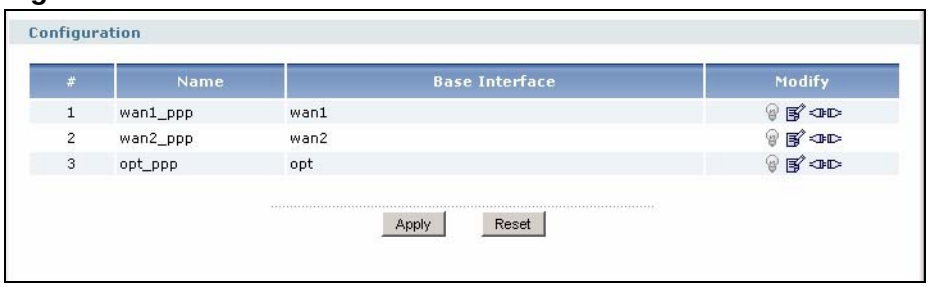
At the time of writing, it is possible to set up the IP address of the gateway (ISP) using CLI commands but not in the web configurator.

## 10.7.1 PPP Interface Summary

Note: You must have an ISP account before you create a PPPoE/PPTP interface.

This screen lists every PPPoE/PPTP interface. To access this screen, click **Network** > **Interface** > **PPP**.

**Figure 150** Network > Interface > PPP




Each field is described in the table below.

**Table 57** Network > Interface > PPP

| LABEL | DESCRIPTION |
|---|---|
| # | This field is a sequential value, and it is not associated with any interface. |
| Name | This field displays the name of the interface. |
| Base Interface | This field displays the interface on the top of which the PPPoE/PPTP interface is. |
| Add icon | This column lets you create, edit, remove, activate, deactivate, connect and disconnect interfaces.<br><br>To edit an interface, click the **Edit** icon next to it. The **PPPoE/PPTP Interface Edit** screen appears.<br><br>To activate or deactivate an interface, click the **Active** icon next to it. Make sure you click **Apply** to save and apply the change.<br><br>To connect or disconnect an interface, click the **Connect** icon next to it. You might use this icon to test the interface or to manually establish the connection for a **Dial-on-Demand** PPPoE/PPTP interface. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

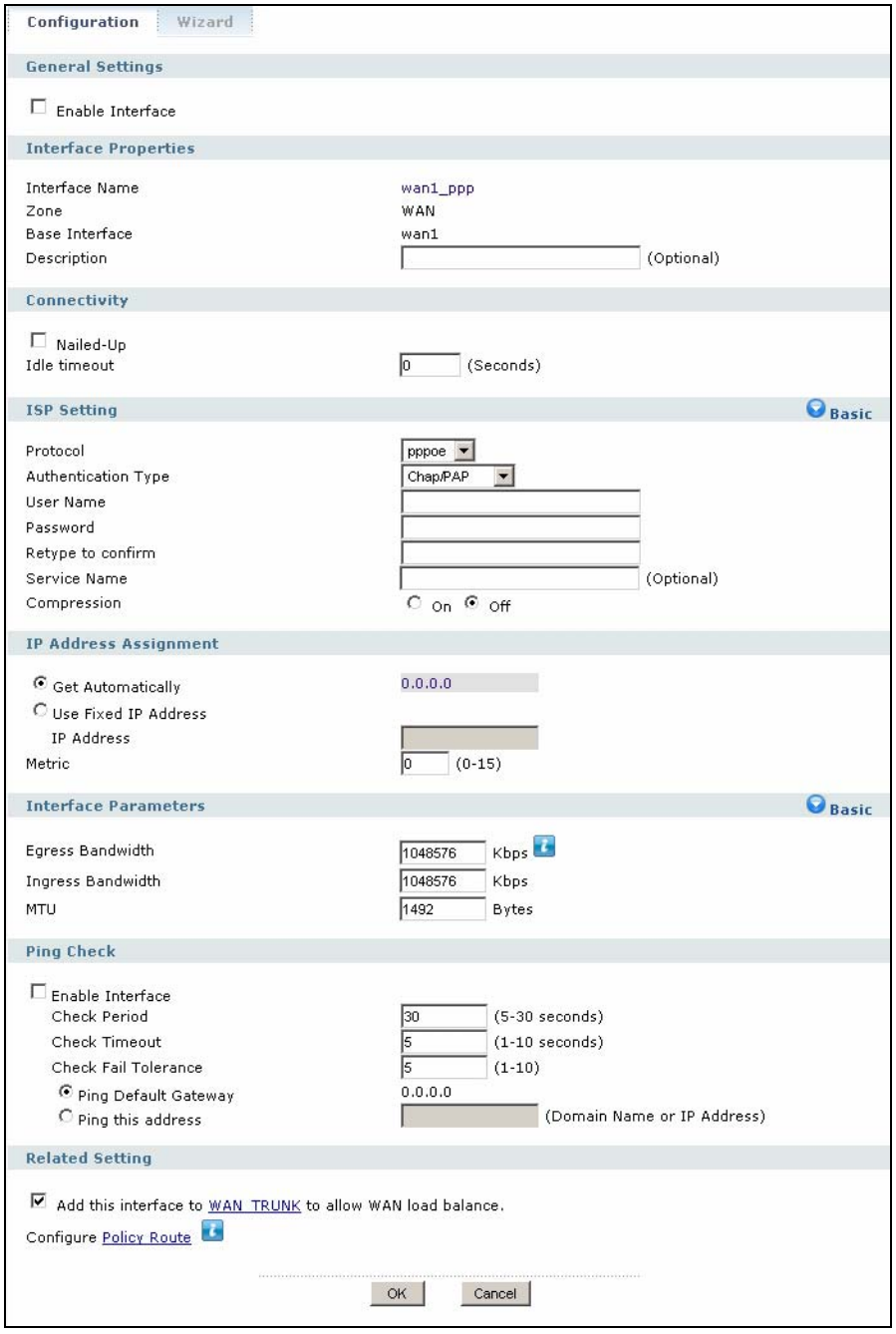
## 10.7.2 PPP Interface Edit

Note: You have to set up an ISP account before you create a PPPoE/PPTP interface.

This screen lets you configure a PPPoE or PPTP interface. To access this screen, click an **Edit** icon in the PPP Interface screen. The PPP interface **Edit > Configuration** screen is shown here as an example. You can click the Wizard tab

instead to configure just the key settings. See Section 10.5 on page 198 for details.

**Figure 151** Network > Interface > PPP > Edit



Each field is explained in the following table.

**Table 58** Network > Interface > PPP > Edit > Configuration

| LABEL | DESCRIPTION |
|---|---|
| General Settings | |
| Enable Interface | Select this to enable this interface. Clear this to disable this interface. |
| Interface Properties | |
| Interface Name | This field is read-only and displays the name of the PPP interface. The format is the name of the physical port followed by “ppp”. For example, “wan1_pppoe”. |
| Base Interface | This field is read-only and displays the name of the interface upon which this PPP interface is built. |
| Description | Enter a description of this interface. It is not used elsewhere. You can use alphanumeric and ( )+/:=?!*#@$_%- characters, and it can be up to 60 characters long. |
| Connectivity | |
| Nailed-Up | Select this if the PPPoE/PPTP connection should always be up. Clear this to have the ZyWALL establish the PPPoE/PPTP connection only when there is traffic. You might use this option if a lot of traffic needs to go through the interface or it does not cost extra to keep the connection up all the time. |
| Dial-on-Demand | Select this to have the ZyWALL establish the PPPoE/PPTP connection only when there is traffic. You might use this option if there is little traffic through the interface or if it costs money to keep the connection available. |
| ISP Setting | |
| Protocol | Select the protocol that your ISP uses for the account. Options are:<br>**pppoe** - This ISP account uses the PPPoE protocol.<br>**pptp** - This ISP account uses the PPTP protocol. |
| Authentication Type | Use the drop-down list box to select an authentication protocol for outgoing calls. Options are:<br>**CHAP/PAP** - Your ZyWALL accepts either CHAP or PAP when requested by this remote node.<br>**CHAP** - Your ZyWALL accepts CHAP only.<br>**PAP** - Your ZyWALL accepts PAP only.<br>**MSCHAP** - Your ZyWALL accepts MSCHAP only.<br>**MSCHAP-V2** - Your ZyWALL accepts MSCHAP-V2 only. |
| User Name | This field is read-only. It displays the user name for the ISP account. |
| Password ,/ Retype to Confirm | Type your password. Then re- to make sure that you have entered is correctly. |
| Service Name | This field is optional. It displays the PPPoE service name specified in the ISP account. This field is blank if the ISP account uses PPTP. |

**Table 58** Network > Interface > PPP > Edit > Configuration (continued)

| LABEL | DESCRIPTION |
|---|---|
| Compression | Select **On** button to turn on stac compression, and select **Off** to turn off stac compression. Stac compression is a data compression technique capable of compressing data by a factor of about four. |
| IP Address Assignment | Click **Advanced** to display more settings. Click **Basic** to display fewer settings. |
| Get Automatically | Select this if this interface is a DHCP client. In this case, the DHCP server configures the IP address automatically. The subnet mask and gateway are always defined automatically in PPPoE/PPTP interfaces. |
| Use Fixed IP Address | Select this if you want to specify the IP address manually. |
| IP Address | This field is enabled if you select **Use Fixed IP Address**.<br><br>Enter the IP address for this interface. |
| Metric | Enter the priority of the gateway (the ISP) on this interface. The ZyWALL decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the ZyWALL uses the one that was configured first. |
| Interface Parameters | |
| Egress Bandwidth | Enter the maximum amount of traffic, in kilobits per second, the ZyWALL can send through the interface to the network. Allowed values are 0 - 1048576. |
| Ingress Bandwidth | This is reserved for future use.<br><br>Enter the maximum amount of traffic, in kilobits per second, the ZyWALL can receive from the network through the interface. Allowed values are 0 - 1048576. |
| MTU | Maximum Transmission Unit. Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the ZyWALL divides it into smaller fragments. Allowed values are 576 - 1492. Usually, this value is 1492. |
| Connectivity Check | The interface can regularly check the connection to the gateway you specified to make sure it is still available. You specify how often the interface checks the connection, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the ZyWALL stops routing to the gateway. The ZyWALL resumes routing to the gateway the first time the gateway passes the connectivity check. |
| Enable Connectivity Check | Select this to turn on the connection check. |
| Check Method | Select the method that the gateway allows.<br><br>Select **icmp** to have the ZyWALL regularly ping the gateway you specify to make sure it is still available.<br><br>Select **tcp** to have the ZyWALL regularly perform a TCP handshake with the gateway you specify to make sure it is still available. |
| Check Period | Enter the number of seconds between connection check attempts. |

**Table 58** Network > Interface > PPP > Edit > Configuration (continued)

| LABEL | DESCRIPTION |
|---|---|
| Check Timeout | Enter the number of seconds to wait for a response before the attempt is a failure. |
| Check Fail Tolerance | Enter the number of consecutive failures before the ZyWALL stops routing through the gateway. |
| Check Default Gateway | Select this to use the default gateway for the connectivity check. |
| Check this address | Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it. |
| Check Port | This field only displays when you set the **Check Method** to **tcp**. Specify the port number to use for a TCP connectivity check. |
| Related Setting | |
| Add this interface to WAN_TRUNK to allow WAN load balance. | Select this option to use the interface as part of a WAN trunk for load balancing. |
| Policy Route | Click **Policy Route** to go to the screen where you can manually configure a policy route to associate traffic with this interface. |
| OK | Click **OK** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# 10.8 Cellular Configuration Screen (3G)

3G (Third Generation) is a digital, packet-switched wireless technology. Bandwidth usage is optimized as multiple users share the same channel and bandwidth is only allocated to users when they send data. It allows fast transfer of voice and non-voice data and provides broadband Internet access to mobile devices.

Note: The actual data rate you obtain varies depending on the 3G card you use, the signal strength to the service provider's base station, and so on.

If the signal strength of a 3G network is too low, the 3G card may switch to an available 2.5G or 2.75G network. See the following table for a comparison between 2G, 2.5G, 2.75G and 3G of wireless technologies.

**Table 59** 2G, 2.5G, 2.75G, 3G and 3.5G Wireless Technologies

| NAME | TYPE | MOBILE PHONE AND DATA STANDARDS | | DATA SPEED |
|---|---|---|---|---|
| | | GSM-BASED | CDMA-BASED | |
| 2G | Circuit-switched | GSM (Global System for Mobile Communications), Personal Handy-phone System (PHS), etc. | Interim Standard 95 (IS-95), the first CDMA-based digital cellular standard pioneered by Qualcomm. The brand name for IS-95 is cdmaOne. IS-95 is also known as TIA-EIA-95. | Slow |
| 2.5G | Packet-switched | GPRS (General Packet Radio Services), High-Speed Circuit-Switched Data (HSCSD), etc. | CDMA2000 is a hybrid 2.5G / 3G protocol of mobile telecommunications standards that use CDMA, a multiple access scheme for digital radio.<br><br>CDMA2000 1xRTT (1 times Radio Transmission Technology) is the core CDMA2000 wireless air interface standard. It is also known as 1x, 1xRTT, or IS-2000 and considered to be a 2.5G or 2.75G technology. | |
| 2.75G | Packet-switched | Enhanced Data rates for GSM Evolution (EDGE), Enhanced GPRS (EGPRS), etc. | | |
| 3G | Packet-switched | UMTS (Universal Mobile Telecommunications System), a third-generation (3G) wireless standard defined in ITU[A] specification, is sometimes marketed as 3GSM. The UMTS uses GSM infrastructures and W-CDMA (Wideband Code Division Multiple Access) as the air interface. | CDMA2000 EV-DO (Evolution-Data Optimized, originally 1x Evolution-Data Only), also referred to as EV-DO, EVDO, or just EV, is an evolution of CDMA2000 1xRTT and enables high-speed wireless connectivity. It is also denoted as IS-856 or High Data Rate (HDR). | |
| 3.5G | Packet-switched | HSDPA (High-Speed Downlink Packet Access) is a mobile telephony protocol, used for UMTS-based 3G networks and allows for higher data transfer speeds. | | Fast |

A. The International Telecommunication Union (ITU) is an international organization within which governments and the private sector coordinate global telecom networks and services.

To change your 3G WAN settings, click **Network** > **Interface** > **Cellular**.

Note: Install (or connect) a compatible 3G card to use a cellular connection. See Chapter 52 on page 835 for details.

Note: The WAN IP addresses of a ZyWALL with multiple WAN interfaces must be on different subnets.

**Figure 152** Network > Interface > Cellular


The following table describes the labels in this screen.

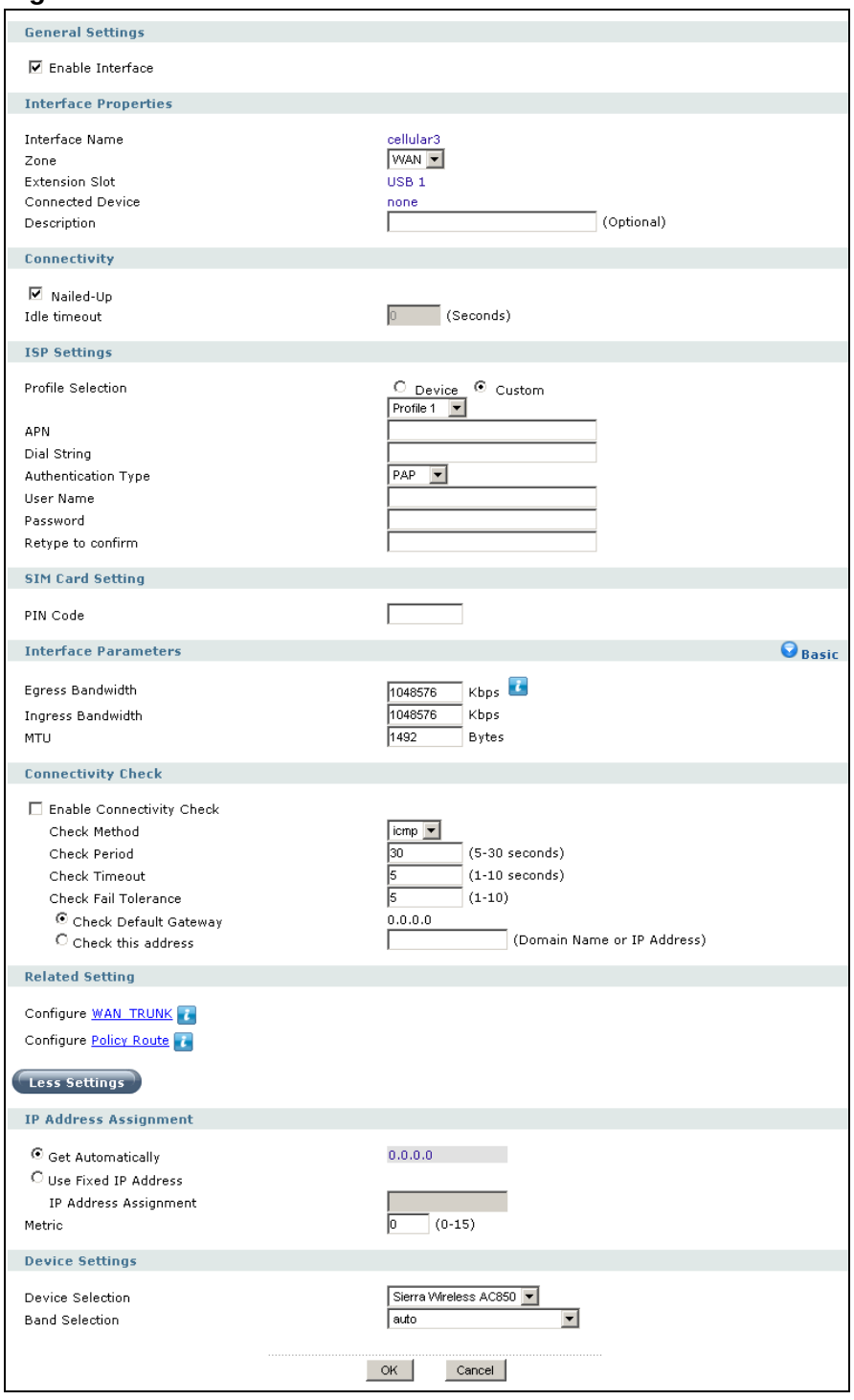
**Table 60** Network > Interface > Cellular

| LABEL | DESCRIPTION |
|---|---|
| # | This field is a sequential value, and it is not associated with any interface. |
| Name | This field displays the name of the interface. |
| Extension Slot | This field displays where the entry's cellular card is located. |
| Connected Device | This field displays the name of the cellular card. |
| ISP Settings | This field displays the profile of ISP settings that this cellular interface is set to use. |
| Add icon | This column lets you create, edit, remove, activate, and deactivate cellular interfaces.<br><br>To create an interface, click the **Add** icon at the top of the column. In the pop-up window that displays, select the slot that you want to configure.<br><br>To activate or deactivate an interface, click the **Active** icon next to it. Make sure you click **Apply** to save and apply the change.<br><br>To edit an interface, click the **Edit** icon next to it. The edit screen appears.<br><br>To remove an interface, click the **Remove** icon next to it. The ZyWALL confirms you want to remove it before doing so.<br><br>To connect or disconnect an interface, click the **Connect** icon next to it. You might use this icon to test the interface or to manually establish the connection. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 10.8.1 Cellular Add/Edit Screen

To change your 3G settings, click **Network** > **Interface** > **Cellular > Add** (or **Edit**). In the pop-up window that displays, select the slot that you want to configure. The following screen displays.

**Figure 153** Interface > Cellular > Add



The following table describes the labels in this screen.

**Table 61** Interface > Cellular > Add

| LABEL | DESCRIPTION |
|---|---|
| General Settings | |
| Enable Interface | Select this option to turn on this interface. |
| Interface Properties | |
| Interface Name | This field is read-only. This is the name of the cellular interface. |
| Zone | Select the zone to which you want the cellular interface to belong. The zone determines the security settings the ZyWALL uses for the interface. |
| Extension Slot | This is the PCMCIA or USB slot that you are configuring for use with a 3G card. |
| Connected Device | This displays the manufacturer and model name of your 3G card if you inserted one in the ZyWALL. Otherwise, it displays **none**. |
| Description | Enter a description of this interface. It is not used elsewhere. You can use alphanumeric and ( )+/:=?!*#@$_%- characters, and it can be up to 60 characters long. |
| Connectivity | |
| Nailed-Up | Select this if the connection should always be up. Clear this to have the ZyWALL to establish the connection only when there is traffic. You might not nail up the connection if there is little traffic through the interface or if it costs money to keep the connection available. |
| Idle timeout | This value specifies the time in seconds (0~360) that elapses before the ZyWALL automatically disconnects from the ISP's server. Zero disables the idle timeout. |
| ISP Settings | |
| Profile Selection | Select **Device** to use one of the 3G device's profiles of device settings. Then select the profile (use **Profile 1** unless your ISP instructed you to do otherwise).<br><br>Select **Custom** to configure your device settings yourself. |
| APN | This field is read-only if you selected **Device** in the profile selection. Select **Custom** in the profile selection to be able to manually input the APN (Access Point Name) provided by your service provider. This field applies with a GSM or HSDPA 3G card. Enter the APN from your service provider. Connections with different APNs may provide different services (such as Internet access or MMS (Multi-Media Messaging Service)) and charge method.<br><br>You can enter up to 63 ASCII printable characters. Spaces are allowed. |
| Dial String | Enter the dial string if your ISP provides a string, which would include the APN, to initialize the 3G card.<br><br>You can enter up to 63 ASCII printable characters. Spaces are allowed.<br><br>This field is available only when you insert a GSM 3G card. |

**Table 61** Interface > Cellular > Add (continued)

| LABEL | DESCRIPTION |
|---|---|
| Authentication Type | The ZyWALL supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). CHAP is more secure than PAP; however, PAP is readily available on more platforms.<br><br>Use the drop-down list box to select an authentication protocol for outgoing calls. Options are:<br><br>**None:** No authentication for outgoing calls.<br><br>**CHAP** - Your ZyWALL accepts CHAP requests only.<br><br>**PAP** - Your ZyWALL accepts PAP requests only. |
| User Name | This field displays when you select an authentication type other than **None**. This field is read-only if you selected **Device** in the profile selection. If this field is configurable, enter the user name for this 3G card exactly as the service provider gave it to you.<br><br>You can use 1 ~ 64 alphanumeric and `#:%-_@$./` characters. The first character must be alphanumeric or `-_@$./`. Spaces are not allowed. |
| Password | This field displays when you select an authentication type other than **None**. This field is read-only if you selected **Device** in the profile selection and the password is included in the 3G card's profile. If this field is configurable, enter the password for this SIM card exactly as the service provider gave it to you.<br><br>You can use 0 ~ 63 alphanumeric and `` `~!@#$%^&*()_-+={}\|;:'<,>./ `` characters. Spaces are not allowed. |
| Retype to Confirm | This field displays when you select an authentication type other than **None**. This field is read-only if you selected **Device** in the profile selection and the password is included in the 3G card's profile. If this field is configurable, re-enter the password for this SIM card exactly as the service provider gave it to you. |
| SIM Card Setting | |
| PIN Code | This field displays with a GSM or HSDPA 3G card. A PIN (Personal Identification Number) code is a key to a 3G card. Without the PIN code, you cannot use the 3G card.<br><br>Enter the 4-digit PIN code (0000 for example) provided by your ISP. If you enter the PIN code incorrectly, the 3G card may be blocked by your ISP and you cannot use the account to access the Internet.<br><br>If your ISP disabled PIN code authentication, enter an arbitrary number. |
| Interface Parameters | Click **Advanced** to display more settings. Click **Basic** to display fewer settings. |
| Egress Bandwidth | Enter the maximum amount of traffic, in kilobits per second, the ZyWALL can send through the interface to the network. Allowed values are 0 - 1048576. This setting is used in WAN load balancing and bandwidth management. |
| Ingress Bandwidth | This is reserved for future use.<br><br>Enter the maximum amount of traffic, in kilobits per second, the ZyWALL can receive from the network through the interface. Allowed values are 0 - 1048576. |

**Table 61** Interface > Cellular > Add (continued)

| LABEL | DESCRIPTION |
|---|---|
| MTU | Maximum Transmission Unit. Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the ZyWALL divides it into smaller fragments. Allowed values are 576 - 1492. Usually, this value is 1492. |
| Connectivity Check | The interface can regularly check the connection to the gateway you specified to make sure it is still available. You specify how often the interface checks the connection, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the ZyWALL stops routing to the gateway. The ZyWALL resumes routing to the gateway the first time the gateway passes the connectivity check. |
| Enable Connectivity Check | Select this to turn on the connection check. |
| Check Method | Select the method that the gateway allows.<br>Select **icmp** to have the ZyWALL regularly ping the gateway you specify to make sure it is still available.<br>Select **tcp** to have the ZyWALL regularly perform a TCP handshake with the gateway you specify to make sure it is still available. |
| Check Period | Enter the number of seconds between connection check attempts. |
| Check Timeout | Enter the number of seconds to wait for a response before the attempt is a failure. |
| Check Fail Tolerance | Enter the number of consecutive failures before the ZyWALL stops routing through the gateway. |
| Check Default Gateway | Select this to use the default gateway for the connectivity check. |
| Check this address | Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it. |
| Check Port | This field only displays when you set the **Check Method** to **tcp**. Specify the port number to use for a TCP connectivity check. |
| Related Setting | |
| Configure WAN TRUNK | Click **WAN TRUNK** to go to a screen where you can configure the interface as part of a WAN trunk for load balancing. |
| Configure Policy Route | Click **Policy Route** to go to the screen where you can configure a policy route to associate traffic with this interface. |
| More Settings/ Less Settings | Click this button to display a greater or lesser number of configuration fields. |
| IP Address Assignment | |
| Get Automatically | Select this option If your ISP did not assign you a fixed IP address. This is the default selection. |
| Use Fixed IP Address | Select this option If the ISP assigned a fixed IP address. |
| IP Address | Enter the cellular interface's WAN IP address in this field if you selected **Use Fixed IP Address**. |

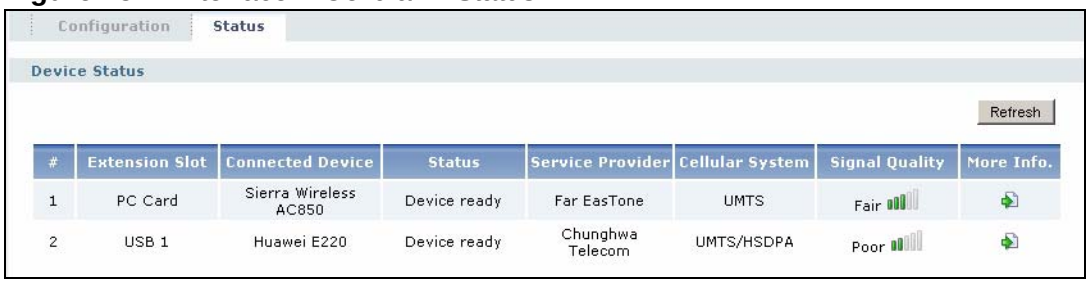
**Table 61** Interface > Cellular > Add (continued)

| LABEL | DESCRIPTION |
|---|---|
| Metric | Enter the priority of the gateway (if any) on this interface. The ZyWALL decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the ZyWALL uses the one that was configured first. |
| Device Settings | |
| Device Selection | Select the 3G card to use with this entry or select **auto** to have the ZyWALL automatically detect the type of card. |
| Band Selection | This field appears if you selected a 3G device that allows you to select the type of network to use. Select the type of 3G service for your 3G connection. If you are unsure what to select, check with your 3G service provider to find the 3G service available to you in your region.<br><br>Select **auto** to have the card connect to an available network. Choose this option if you do not know what networks are available.<br><br>You may want to manually specify the type of network to use if you are charged differently for different types of network or you only have one type of network available to you.<br><br>Select **GPRS / EDGE (GSM) only** to have this interface only use a 2.5G or 2.75G network (respectively). If you only have a GSM network available to you, you may want to select this so the ZyWALL does not spend time looking for a WCDMA network.<br><br>Select **UMTS / HSDPA (WCDMA) only** to have this interface only use a 3G or 3.5G network (respectively). You may want to do this if you want to make sure the interface does not use the GSM network. |
| OK | Click **OK** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# 10.9 Cellular Status Screen

To check your 3G connection status, click **Network** > **Interface** > **Cellular** > **Status**. The following screen displays.

**Figure 154** Interface > Cellular > Status



The following table describes the labels in this screen.

**Table 62** Interface > Cellular > Status

| LABEL | DESCRIPTION |
|---|---|
| Refresh | Click this button to update the information in the screen. |
| # | This field is a sequential value, and it is not associated with any interface. |
| Extension Slot | This field displays where the entry's cellular card is located. |
| Connected Device | This field displays the model name of the cellular card. |
| Status | **No device** - no 3G device is connected to the ZyWALL.<br>**Device detected** - displays when you connect a 3G device.<br>**Device error** - a 3G device is connected but there is an error.<br>**Probe device fail** - the ZyWALL's test of the 3G device failed.<br>**Probe device ok** - the ZyWALL's test of the 3G device failed.<br>**Init device fail** - the ZyWALL was not able to initialize the 3G device.<br>**Init device ok** - the ZyWALL initialized the 3G card.<br>**Check lock fail** - the ZyWALL's check of whether or not the 3G device is locked failed.<br>**Device locked** - the 3G device is locked.<br>**SIM error** - there is a SIM card error on the 3G device.<br>**SIM locked-PUK** - the PUK is locked on the 3G device's SIM card.<br>**SIM locked-PIN** - the PIN is locked on the 3G device's SIM card.<br>**Unlock PUK fail** - Your attempt to unlock a WCDMA 3G device's PUK failed because you entered an incorrect PUK.<br>**Unlock PIN fail** - Your attempt to unlock a WCDMA 3G device's PIN failed because you entered an incorrect PIN.<br>**Unlock device fail** - Your attempt to unlock a CDMA2000 3G device failed because you entered an incorrect device code.<br>**Device unlocked** - You entered the correct device code and unlocked a CDMA2000 3G device.<br>**Get dev-info fail** - The ZyWALL cannot get cellular device information.<br>**Get dev-info ok** - The ZyWALL succeeded in retrieving 3G device information.<br>**Searching network** - The 3G device is searching for a network.<br>**Get signal fail** - The 3G device cannot get a signal from a network.<br>**Network found** - The 3G device found a network.<br>**Apply config** - The ZyWALL is applying your configuration to the 3G device.<br>**Inactive** - The 3G interface is disabled.<br>**Active** - The 3G interface is enabled.<br>**Incorrect device** - The connected 3G device is not compatible with the ZyWALL.<br>**Correct device** - The ZyWALL detected a compatible 3G device.<br>**Set band fail** - Applying your band selection was not successful.<br>**Set band ok** - The ZyWALL successfully applied your band selection.<br>**Set profile fail** - Applying your ISP settings was not successful.<br>**Set profile ok** - The ZyWALL successfully applied your ISP settings.<br>**PPP fail** - The ZyWALL failed to create a PPP connection for the cellular interface.<br>**Need auth-password** - You need to enter the password for the 3G card in the cellular edit screen.<br>**Device ready** - The ZyWALL successfully applied all of your configuration and you can use the 3G connection. |

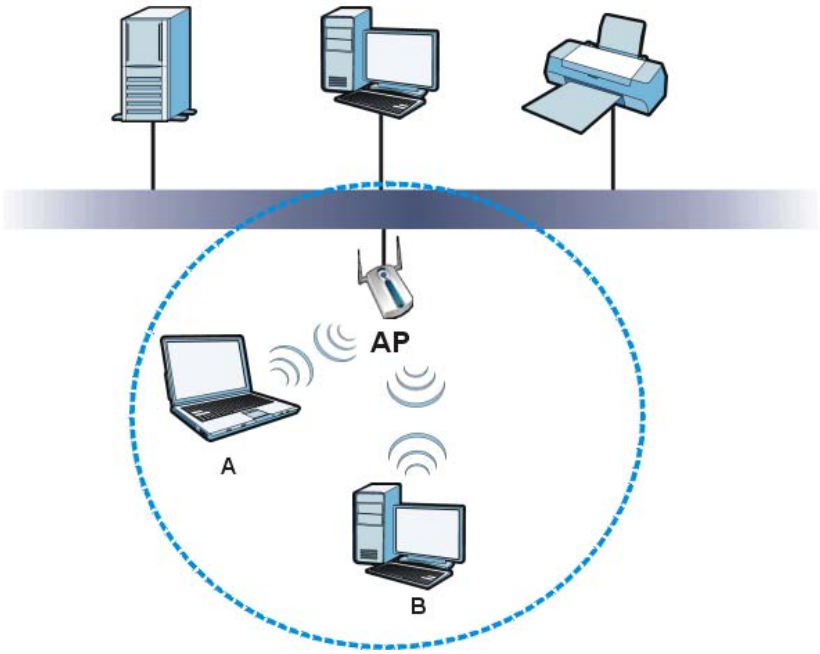
**Table 62** Interface > Cellular > Status (continued)

| LABEL | DESCRIPTION |
|---|---|
| Service Provider | This displays the name of your network service provider or **Limited Service** when the signal strength is too low. |
| Cellular System | This field displays what type of cellular network the 3G connection is using. The network type varies depending on the 3G card you inserted and could be **UMTS**, **UMTS/HSDPA**, **GPRS** or **EDGE** when you insert a GSM 3G card, or **1xRTT**, **EVDO Rev.0** or **EVDO Rev.A** when you insert a CDMA 3G card. |
| Signal Quality | This displays the strength of the signal. The signal strength mainly depends on the antenna output power and the distance between your ZyWALL and the service provider's base station. |
| More Info. | This field displays other details about the 3G connection. |

# 10.10 WLAN Interface General Screen

The following figure provides an example of a wireless network. The wireless network is in the blue circle. Wireless clients (A and B) connect to an access point (AP) to access other devices (such as the printer) or the Internet. Your ZyWALL works as an AP when you install a compatible WLAN card.

**Figure 155** Example of a Wireless Network




- Every device in a wireless network must use the same SSID.

  The SSID is the name of the wireless network. It stands for Service Set IDentity.

- Different wireless networks in the same area should use different channels.

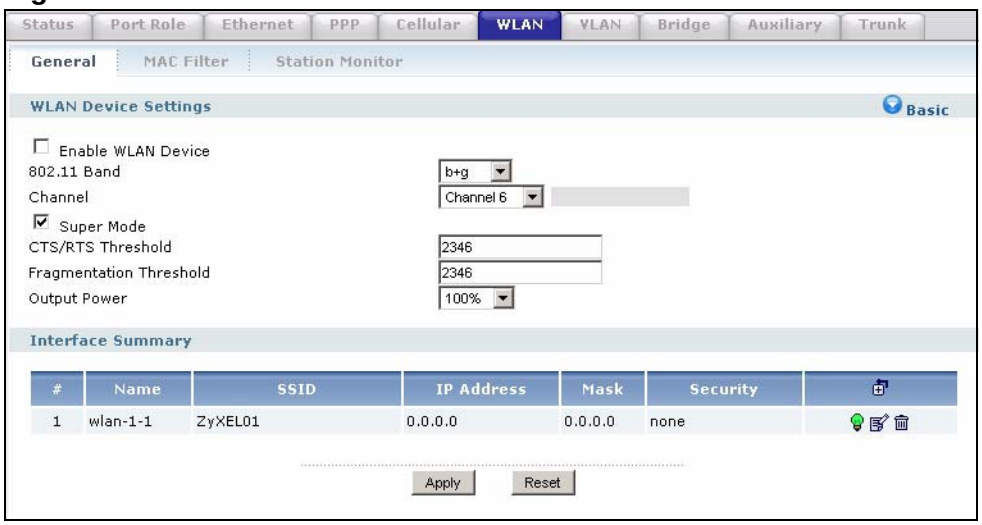
  Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.

- Every wireless client in a wireless network must use security compatible with the AP.

  Security stops unauthorized devices from using the wireless network and can protect the information that is sent in the wireless network.

Click **Network > Interface > WLAN** to open the following screen. See Appendix F on page 987 for more details on wireless LANs.

**Figure 156** Network > Interface > WLAN




The following table describes the general wireless LAN labels in this screen.

**Table 63** Network > Interface > WLAN

| LABEL | DESCRIPTION |
|---|---|
| WLAN Device Settings | |
| Enable WLAN Device | Select this option to turn on the wireless LAN card. It is recommended that you configure the wireless security settings before you use this option to turn on a wireless LAN card. |
| 802.11 Band | Select whether you will let wireless clients connect to the ZyWALL using IEEE 802.11b, IEEE 802.11g, or both.<br><br>Select **b Only** to allow only IEEE 802.11b compliant WLAN devices to associate with the ZyWALL.<br><br>Select **g Only** to allow only IEEE 802.11g compliant WLAN devices to associate with the ZyWALL.<br><br>Select **b+g** to allow both IEEE802.11b and IEEE802.11g compliant WLAN devices to associate with the ZyWALL. The transmission rate of your ZyWALL might be reduced. |
| Channel | This allows you to set the operating channel depending on your particular region. Select a channel from the drop-down list box. |

**Table 63** Network > Interface > WLAN

| LABEL | DESCRIPTION |
|---|---|
| Super Mode | Select this to improve data throughput on the WLAN by enabling fast frame and packet bursting. |
| CTS/RTS Threshold | Use CTS/RTS to reduce data collisions on the wireless network if you have wireless clients that are associated with the same AP but out of range of one another. When enabled, a wireless client sends an RTS (Request To Send) and then waits for a CTS (Clear To Send) before it transmits. This stops wireless clients from transmitting packets at the same time (and causing data collisions).<br><br>A wireless client sends an RTS for all packets larger than the number (of bytes) that you enter here. Set the RTS/CTS equal to or higher than the fragmentation threshold to turn RTS/CTS off. |
| Fragmentation Threshold | This is the threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. |
| Output Power | Set the output power of the ZyWALL in this field. If there is a high density of APs in the area, decrease the output power of the ZyWALL to reduce interference with other APs. Select one of the following **100%**, **50%**, **25%**, **12.5%** or **Minimum**. See the product specifications for more information on your ZyWALL's output power. |
| # | This field is a sequential value, and it is not associated with any interface. |
| Name | This field displays the name of the WLAN interface. |
| SSID | This is the SSID (Service Set IDentity) of the WLAN interface. |
| IP Address | This field displays the current IP address of the WLAN interface. If the IP address is 0.0.0.0, the interface does not have an IP address yet.<br><br>This screen also shows whether the IP address is a static IP address (**STATIC**) or dynamically assigned (**DHCP**). IP addresses are always static in virtual interfaces. |
| Mask | This field displays the interface's subnet mask in dot decimal notation. |
| Security | This field displays what type of security the WLAN interface uses. |
| Add icon | This column lets you create, edit, remove, activate, and deactivate WLAN interfaces.<br><br>To create an interface, click the **Add** icon at the top of the column.<br><br>To activate or deactivate an interface, click the **Active** icon next to it. Make sure you click **Apply** to save and apply the change.<br><br>To edit an interface, click the **Edit** icon next to it. The edit screen appears.<br><br>To remove an interface, click the **Remove** icon next to it. The ZyWALL confirms you want to remove it before doing so.<br><br>To connect or disconnect an interface, click the **Connect** icon next to it. You might use this icon to test the interface or to manually establish the connection. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 10.10.1 WLAN Add/Edit Screen

Use the strongest security that every wireless client in the wireless network supports.

**Table 64** Wireless Security Levels

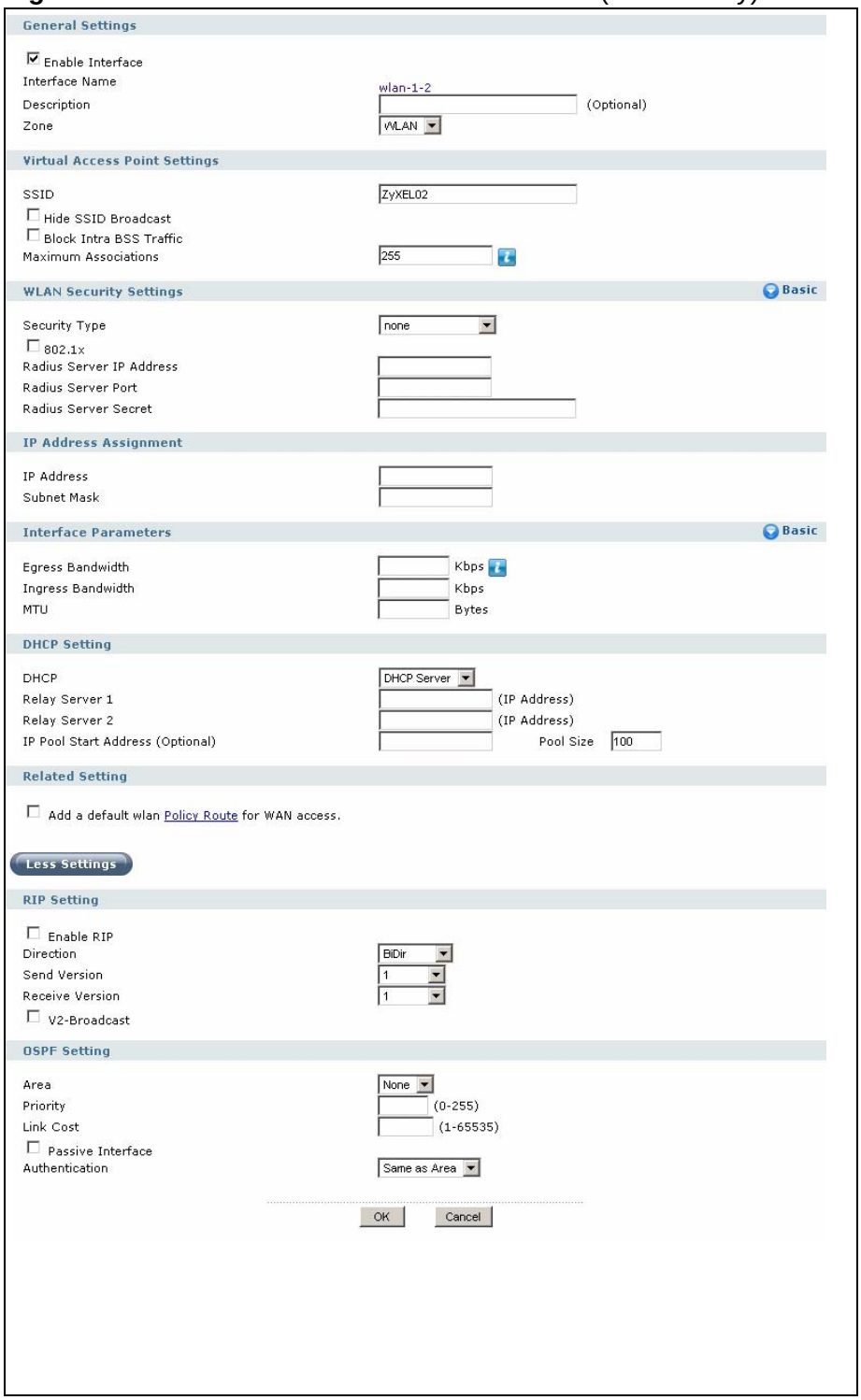
| SECURITY LEVEL | SECURITY TYPE |
|---|---|
| Weakest | No Security |
| | MAC Address Filtering |
| | WEP Encryption |
| | IEEE 802.1x EAP with RADIUS Server Authentication |
| | WPA-PSK (Wi-Fi Protected Access Pre-Shared Key) |
| | WPA (Wi-Fi Protected Access) |
| | WPA-PSK2 |
| | WPA2 |
| Strongest | |

Note: WPA2 or WPA2-PSK security is recommended.

- You can use the ZyWALL's local user database to use WPA or WPA2 without using an external RADIUS server. With WPA or WPA2, users have to log into the wireless network before using it. This is called user authentication. WPA and WPA2 are also called the enterprise version of WPA).
- WPA2-PSK and WPA-PSK do not employ user authentication and are known as the personal version of WPA.
- WEP is better than no security, but it is still possible for unauthorized devices to figure out the original information pretty quickly.

Click **Network > Interface > WLAN > Add** (or **Edit**) to open the **WLAN Edit** screen. The screen varies according to the security features you select. It displays as shown next when you set the **Security Type** to **none**.

**Figure 157** Network > Interface > WLAN > Add (No Security)



The following table describes the general wireless LAN labels.

**Table 65** Network > Interface > WLAN > Add (No Security)

| LABEL | DESCRIPTION |
|---|---|
| General Settings | |
| Enable Interface | Select this option to turn on the wireless LAN interface. |
| Interface Name | Specify a number from 1~8 to complete the name for this wireless LAN interface. |
| Description | Enter a description of this interface. It is not used elsewhere. You can use alphanumeric and ()+/:=?!*#@$_%- characters, and it can be up to 60 characters long. |
| Zone | Select the zone to which you want the WLAN interface to belong. |
| Virtual Access Point Settings | |
| SSID | (Service Set IDentity) The SSID identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. To make your wireless network more secure, change the default SSID to something that is difficult to guess. |
| Hide SSID Broadcast | Select to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning. |
| Block Intra-BSS Traffic | Select this to prevent wireless clients in this profile's BSS from communicating with one another. |
| Maximum Associations | Specify the highest number of wireless clients that are allowed to connect to the wireless interface at the same time. |
| WLAN Security Settings | Click **Advanced** to display more settings. Click **Basic** to display fewer settings. |
| Security Type | Use this field to select the type of security to use for this wireless LAN interface. Select **none** to not use any security. See the following sections for details on the other security types. |
| 802.1x | Authentication server (IEEE 802.1x) settings are available when you use no security or WEP security and click **Advanced**.<br><br>Select the check box to enable wireless user authentication through an external authentication server. |
| RADIUS Server IP Address | Enter the IP address of the external authentication server in dotted decimal notation. |
| RADIUS Server Port | Enter the RADIUS server's listening port number (the default is **1812**). |
| RADIUS Server Secret | Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the ZyWALL. The key is not sent over the network. This key must be the same on the external authentication server and ZyWALL. |
| IP Address Assignment | |
| IP Address | Enter the IP address for this interface. |

**Table 65** Network > Interface > WLAN > Add (No Security) (continued)

| LABEL | DESCRIPTION |
|---|---|
| Subnet Mask | Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network. |
| Interface Parameters | Click **Advanced** to display more settings. Click **Basic** to display fewer settings. |
| Egress Bandwidth | Enter the maximum amount of traffic, in kilobits per second, the ZyWALL can send through the interface to the network. Allowed values are 0 - 1048576. This setting is used in WAN load balancing and bandwidth management. |
| Ingress Bandwidth | This is reserved for future use.<br>Enter the maximum amount of traffic, in kilobits per second, the ZyWALL can receive from the network through the interface. Allowed values are 0 - 1048576. |
| MTU | Maximum Transmission Unit. Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the ZyWALL divides it into smaller fragments. Allowed values are 576 - 1500. Usually, this value is 1500. |
| DHCP Settings | |
| DHCP | Select what type of DHCP service the ZyWALL provides to the wireless network. Choices are:<br>**None** - the ZyWALL does not provide any DHCP services. There is already a DHCP server on the network.<br>**DHCP Relay** - the ZyWALL routes DHCP requests to one or more DHCP servers you specify. The DHCP server(s) may be on another network.<br>**DHCP Server** - the ZyWALL assigns IP addresses and provides subnet mask, gateway, and DNS server information to the network. The ZyWALL is the DHCP server for the network. |
| | These fields appear if the ZyWALL is a **DHCP Relay**. |
| Relay Server 1 | Enter the IP address of a DHCP server for the network. |
| Relay Server 2 | This field is optional. Enter the IP address of another DHCP server for the network. |
| | These fields appear if the ZyWALL is a **DHCP Server**. |
| IP Pool Start Address | Enter the IP address from which the ZyWALL begins allocating IP addresses.<br>If this field is blank, the ZyWALL assigns every IP address allowed by the interface's IP address, subnet mask, and pool size; except for the first address (network address), last address (broadcast address) and the interface's IP address. |

**Table 65** Network > Interface > WLAN > Add (No Security) (continued)

| LABEL | DESCRIPTION |
|---|---|
| Pool Size | Enter the number of IP addresses to allocate. This number must be at least one and is limited by the interface's **Subnet Mask**. For example, if the **Subnet Mask** is 255.255.255.0 and **IP Pool Start Address** is 10.10.10.10, the ZyWALL can allocate 10.10.10.10 to 10.10.10.254, or 245 IP addresses.<br><br>If this field is blank, the ZyWALL can assign every IP address allowed by the interface's IP address, subnet mask, and **IP Pool Start Address**; except for the first address (network address), last address (broadcast address) and the interface's IP address. |
| First DNS Server<br>Second DNS Server<br>Third DNS Server | Specify the IP addresses of a maximum of three DNS servers that the network can use. The ZyWALL provides these IP addresses to DHCP clients. Use one of the following ways to specify these IP addresses.<br><br>**Custom Defined** - enter a static IP address.<br><br>**From ISP** - select the DNS server that another interface received from its DHCP server.<br><br>**ZyWALL** - the ZyWALL uses the IP address of this interface and works as a DNS relay. |
| First WINS Server,<br>Second WINS Server | Type the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the DHCP clients. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using. |
| Lease time | Specify how long each computer can use the information (especially the IP address) before it has to request the information again. Choices are:<br><br>**infinite** - select this if IP addresses never expire.<br><br>**days, hours, and minutes** - select this to enter how long IP addresses are valid. |
| Edit static DHCP table | Click this to configure static IP addresses for the ZyWALL to assign to computers connected to this interface. See Section 10.6 on page 206. |
| Related Setting | |
| Add a default wlan Policy Route for WAN access. | Select this to automatically configure a policy route to allow traffic that comes in through this WLAN interface to go out through the WAN. |
| Policy Route | Click this link to go to the screen where you can manually configure a policy route to associate traffic with this interface. |
| More Settings/ Less Settings | Click this button to display a greater or lesser number of configuration fields. |
| RIP Setting | See Section 13.2 on page 286 for more information about RIP. |
| Enable RIP | Select this to enable RIP in this interface. |

**Table 65** Network > Interface > WLAN > Add (No Security) (continued)

| LABEL | DESCRIPTION |
|---|---|
| Direction | This field is effective when RIP is enabled. Select the RIP direction from the drop-down list box.<br>**BiDir** - This interface sends and receives routing information.<br>**In-Only** - This interface receives routing information.<br>**Out-Only** - This interface sends routing information. |
| Send Version | This field is effective when RIP is enabled. Select the RIP version(s) used for sending RIP packets. Choices are **1**, **2**, and **1 and 2**. |
| Receive Version | This field is effective when RIP is enabled. Select the RIP version(s) used for receiving RIP packets. Choices are **1**, **2**, and **1 and 2**. |
| V2-Broadcast | This field is effective when RIP is enabled. Select this to send RIP-2 packets using subnet broadcasting; otherwise, the ZyWALL uses multicasting. |
| OSPF Setting | See Section 13.3 on page 287 for more information about OSPF. |
| Area | Select the area in which this interface belongs. Select **None** to disable OSPF in this interface. |
| Priority | Enter the priority (between 0 and 255) of this interface when the area is looking for a Designated Router (DR) or Backup Designated Router (BDR). The highest-priority interface identifies the DR, and the second-highest-priority interface identifies the BDR. Set the priority to zero if the interface can not be the DR or BDR. |
| Link Cost | Enter the cost (between 1 and 65,535) to route packets through this interface. |
| Passive Interface | Select this to stop forwarding OSPF routing information from the selected interface. As a result, this interface only receives routing information. |
| Authentication | Select an authentication method, or disable authentication. To exchange OSPF routing information with peer border routers, you must use the same authentication method that they use. Choices are:<br>**Same-as-Area** - use the default authentication method in the area<br>**None** - disable authentication<br>**Text** - authenticate OSPF routing information using a plain-text password<br>**MD5** - authenticate OSPF routing information using MD5 encryption |
| Text Authentication Key | This field is available if the **Authentication** is **Text**. Type the password for text authentication. The key can consist of alphanumeric characters and the underscore, and it can be up to eight characters long. |
| MD5 Authentication ID | This field is available if the **Authentication** is **MD5**. Type the ID for MD5 authentication. The ID can be between 1 and 255. |
| MD5 Authentication Key | This field is available if the **Authentication** is **MD5**. Type the password for MD5 authentication. The password can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long. |

**Table 65** Network > Interface > WLAN > Add (No Security) (continued)

| LABEL | DESCRIPTION |
|---|---|
| OK | Click **OK** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving. |

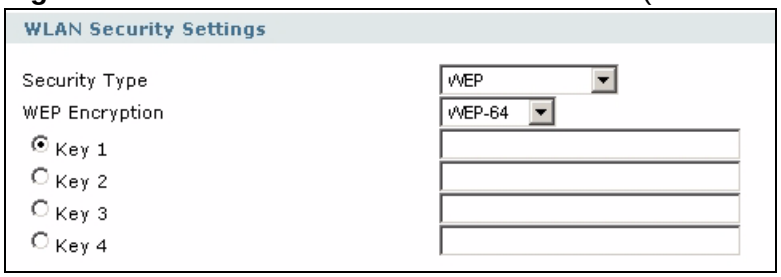
## 10.10.2 WLAN Add/Edit: WEP Security

WEP provides a mechanism for encrypting data using encryption keys. Both the ZyWALL and the wireless stations must use the same WEP key to encrypt and decrypt data. Your ZyWALL allows you to configure up to four 64-bit or 128-bit WEP keys, but only one key can be used at any one time.

Note: WEP is extremely insecure. Its encryption can be broken by an attacker, using widely-available software. It is strongly recommended that you use a more effective security mechanism. Use the strongest security mechanism that all the wireless devices in your network support. For example, use WPA-PSK or WPA2-PSK or WPA or WPA2 if your wireless devices support it. If your wireless devices support nothing stronger than WEP, use the highest encryption level available.

To configure and enable WEP encryption, click **Network > Interface > WLAN > Add** (or **Edit**) to open the **WLAN Edit** screen. Select **WEP** as the **Security Type**. The following screen shows the WEP security fields.

**Figure 158** Network > Interface > WLAN > Add (WEP Security)



The following table describes the WEP-related wireless LAN security labels. See Table 65 on page 226 for information on the 802.1x fields.

**Table 66** Network > Interface > WLAN > Add (WEP Security)

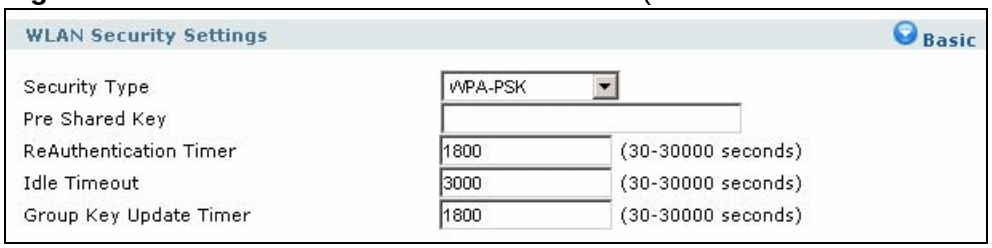
| LABEL | DESCRIPTION |
|---|---|
| WEP Encryption | WEP (Wired Equivalent Privacy) provides data encryption to prevent unauthorized wireless stations from accessing data transmitted over the wireless network.<br>Select **64-bit WEP** or **128-bit WEP** to enable data encryption. |
| Key 1 to Key 4 | If you chose **64-bit WEP** in the **WEP Encryption** field, then enter any 5 characters (ASCII string) or 5 pairs of hexadecimal characters ("0-9", "A-F") preceded by 0x for each key.<br>If you chose **128-bit WEP** in the **WEP Encryption** field, then enter 13 characters (ASCII string) or 13 pairs of hexadecimal characters ("0-9", "A-F") preceded by 0x for each key.<br><br>There are four data encryption keys to secure your data from eavesdropping by unauthorized wireless users. The values for the keys must be set up exactly the same on the access points as they are on the wireless stations. |

## 10.10.3 WLAN Add/Edit: WPA-PSK/WPA2-PSK Security

WPA-PSK or WPA2-PSK security has all of the WLAN interface's users share the same password (pre-shared key).

To configure and enable WPA-PSK or WPA2-PSK security, click **Network > Interface > WLAN > Add** (or **Edit**) to open the **WLAN Edit** screen. Select **WPA-PSK** or **WPA2-PSK** as the **Security Type**. The following screen shows the security fields.

**Figure 159** Network > Interface > WLAN > Add (WPA-PSK/WPA2-PSK Security)



The following table describes the WPA-PSK/WPA2-PSK-related wireless LAN security labels.

**Table 67** Network > Interface > WLAN > Add (WPA-PSK/WPA2-PSK Security)

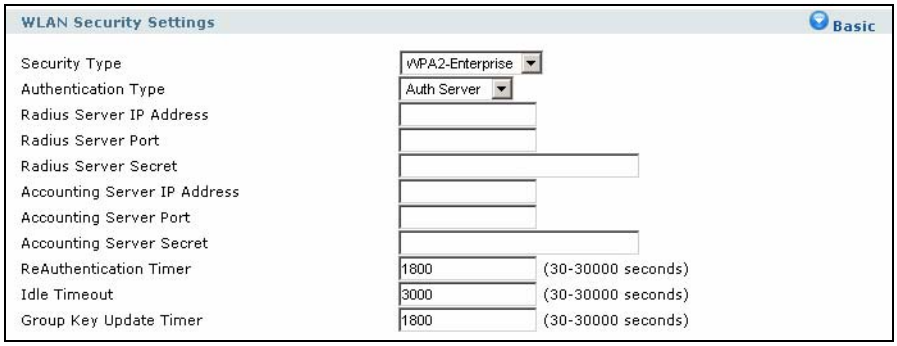
| LABEL | DESCRIPTION |
|---|---|
| Pre-Shared Key | The encryption mechanisms used for **WPA** and **WPA-PSK** are the same. The only difference between the two is that **WPA-PSK** uses a simple common password, instead of user-specific credentials.<br><br>Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols). |
| ReAuthentication Timer | Specify how often wireless stations have to resend usernames and passwords in order to stay connected.<br><br>Note: If a RADIUS server authenticates wireless stations, the reauthentication timer on the RADIUS server has priority. |
| Idle Timeout | The ZyWALL automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. |
| Group Key Update Timer | The **Group Key Update Timer** is the rate at which the AP sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the group key for an AP and all stations in a WLAN on a periodic basis. Setting of the **Group Key Update Timer** is also supported in WPA-PSK mode. |

## 10.10.4 WLAN Add/Edit: WPA/WPA2 Security

With WPA or WPA2 security, each user can have a separate user name and password. The ZyWALL uses an external RADIUS server or the ZyWALL's internal user account list to authenticate the user names and passwords.

To configure and enable WPA or WPA2 security, click **Network > Interface > WLAN > Add** (or **Edit**) to open the **WLAN Edit** screen. Select **WPA-Enterprise** or **WPA2-Enterprise** as the **Security Type**. The following figure shows the security fields.

**Figure 160** Network > Interface > WLAN > Add (WPA/WPA2 Security)



The following table describes the WPA/WPA2-related wireless LAN security labels.

**Table 68** Network > Interface > WLAN > Add (WPA/WPA2 Security)

| LABEL | DESCRIPTION |
|---|---|
| Authentication Type | Select what the ZyWALL uses to authenticate the wireless clients.<br><br>Select **Auth Method** to be able to specify an authentication method object that you have already configured. The authentication method can have the ZyWALL check a user's user name and password against the ZyWALL's local database, a remote LDAP, RADIUS, a Active Directory server, or more than one of these. See Chapter 42 on page 695 for how to create authentication method objects.<br><br>Select **Auth Server** to be able to manually specify a RADIUS server's settings in this screen instead of using an authentication method object. |
| Authentication Method | This field displays if you set the **Authentication Type** field to **Auth Method**.<br><br>Select an authentication method object that defines how the ZyWALL authenticates a wireless user. The ZyWALL's default configuration also includes an authentication method object named "default" that you can use. You can configure the "default" authentication method object, but it's default configuration uses the ZyWALL's local database for authentication. |
| TTLS Certificate | This field displays if you select **Authentication Method**. Select the certificate the ZyWALL uses to authenticate itself to the wireless clients. The certificates you can select from are the ones already configured in the **My Certificates** screen.<br><br>EAP-TTLS (Tunneled Transport Layer Service) is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection.<br><br>The wireless clients must use TTLS authentication protocol and PAP inside the TTLS secure tunnel. |
| | The following fields display if you set the **Authentication Type** field to **Auth Server**. |
| RADIUS Server IP Address | Enter the IP address of the external authentication server in dotted decimal notation. |
| RADIUS Server Port | Enter the RADIUS server's listening port number (the default is **1812**). |
| RADIUS Server Secret | Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the ZyWALL. The key is not sent over the network. This key must be the same on the external authentication server and ZyWALL. |
| ReAuthentication Timer | Specify how often wireless stations have to resend user names and passwords in order to stay connected.<br><br>Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority. |

**Table 68** Network > Interface > WLAN > Add (WPA/WPA2 Security) (continued)

| LABEL | DESCRIPTION |
|---|---|
| Idle Timeout | The ZyWALL automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the user name and password again before access to the wired network is allowed. |
| Group Key Update Timer | The **Group Key Update Timer** is the rate at which the AP sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the group key for an AP and all stations in a WLAN on a periodic basis. Setting of the **Group Key Update Timer** is also supported in WPA-PSK mode. |

# 10.11 WLAN Interface MAC Filter

The MAC filter allows you to give specific wireless clients exclusive access to the ZyWALL (allow association) or block specific devices from accessing the ZyWALL (deny association) based on the devices' MAC addresses.

To display your ZyWALL's MAC filter settings, click **Network > Interface > WLAN** > **MAC Filter**. The screen appears as shown.

**Figure 161** Network > Interface > WLAN > MAC Filter


The following table describes the labels in this screen.

**Table 69** Network > Interface > WLAN > MAC Filter

| LABEL | DESCRIPTION |
|---|---|
| Enable MAC Filter | Select or clear the check box to enable or disable MAC address filtering.<br><br>Enable MAC address filtering to have the router allow or deny access to wireless stations based on MAC addresses. Disable MAC address filtering to have the router not perform MAC filtering on the wireless stations. |
| Association | Define the filter action for the list of MAC addresses in the MAC address filter table.<br><br>Select **Deny** to block access to the router, MAC addresses not listed will be allowed to access the router. Select **Allow** to permit access to the router, MAC addresses not listed will be denied access to the router. |

**Table 69** Network > Interface > WLAN > MAC Filter

| LABEL | DESCRIPTION |
|---|---|
| # | This is the index number of the MAC address. |
| MAC Address | This displays the MAC address (in XX:XX:XX:XX:XX:XX format) of the wireless station that is allowed or denied access to the ZyWALL. |
| Description | This field displays a descriptive name for the MAC address entry. |
| Add icon | This column lets you create, edit, or remove MAC filter entries.<br>To create an entry, click the **Add** icon at the top of the column. The edit screen appears.<br>To edit an entry, click the **Edit** icon next to it. The edit screen appears.<br>To remove an entry, click the **Remove** icon next to it. The ZyWALL confirms you want to remove it before doing so. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

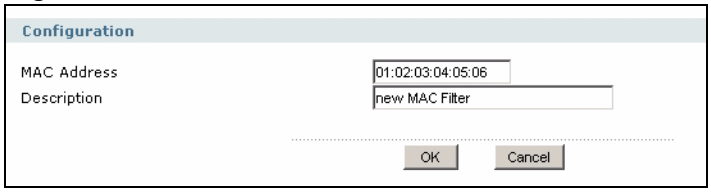
## 10.11.1 MAC Filter Add/Edit Screen

Every IEEE 802.11b or IEEE 802.11g device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC addresses of the devices to configure this screen.

If you set the filter to deny access and add the MAC address of a connected device, the ZyWALL drops the device's connection immediately. However, if you set the filter to allow only the specified MAC addresses, the ZyWALL does not immediately disconnect all connected wireless clients.

To change your ZyWALL's MAC filter settings, click **Network > Interface > WLAN** > **MAC Filter > Add** (or **Edit**). The screen appears as shown when you click **Add**. You cannot edit the MAC address if you click **Edit**.

**Figure 162** Network > Interface > WLAN > MAC Filter > Add




The following table describes the labels in this menu.

**Table 70** Network > Interface > WLAN > MAC Filter

| LABEL | DESCRIPTION |
|---|---|
| MAC Address | Enter the MAC address (in XX:XX:XX:XX:XX:XX format) of the wireless station that is to be allowed or denied access to the ZyWALL. |
| Description | Enter a descriptive name for the MAC address entry. |

**Table 70** Network > Interface > WLAN > MAC Filter

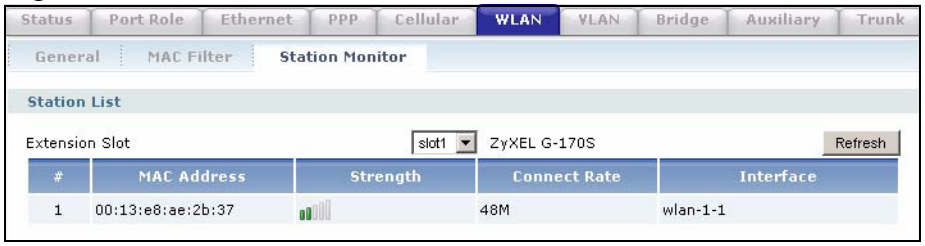
| LABEL | DESCRIPTION |
|---|---|
| OK | Click **OK** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# 10.12 WLAN Interface Station Monitor Screen

The station monitor displays the connection status of the wireless clients connected to (or trying to connect to) a IEEE 802.11b/g card installed in the ZyWALL.

To open the station monitor, click **Network > Interface > WLAN** > **Station Monitor**. The screen appears as shown.

**Figure 163** Network > Interface > WLAN > Station Monitor




The following table describes the labels in this menu.

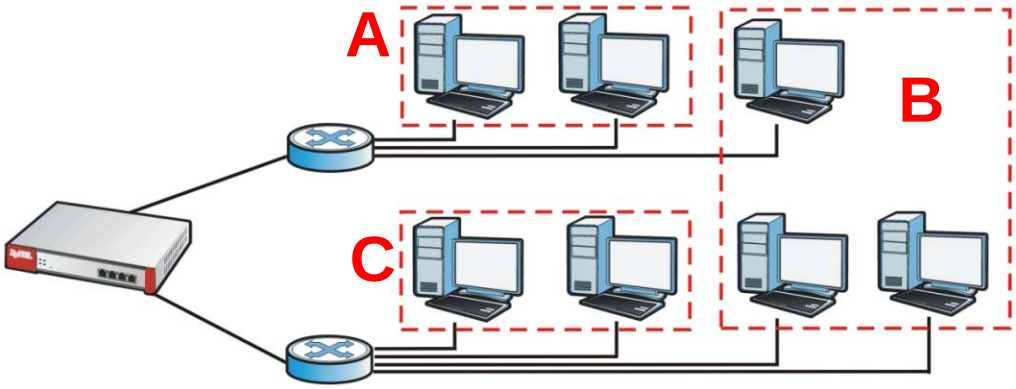
**Table 71** Network > Interface > WLAN > Station Monitor

| LABEL | DESCRIPTION |
|---|---|
| Extension Slot | Select the location where the IEEE 802.11b/g is located. |
| Refresh | Click this button to update the information in the screen. |
| # | This is the index number of the MAC address. |
| MAC Address | This displays the MAC address (in XX:XX:XX:XX:XX:XX format) of a connected wireless station. |
| Strength | This displays the strength of the wireless client's radio signal. The signal strength mainly depends on the antenna output power and the wireless client's distance from the ZyWALL. |
| Connect Rate | This displays what data transfer rate of the wireless client's connection to the ZyWALL. This field displays up to the standard IEEE 802.11g connection rate of 54 Mbps. It does not display higher, even if you enable super mode. The display on your wireless clients may vary. |
| Interface | This is the name of the wireless LAN interface on the ZyWALL to which the wireless client is connected. |

# 10.13 VLAN Interfaces

A Virtual Local Area Network (VLAN) divides a physical network into multiple logical networks. The standard is defined in IEEE 802.1q.

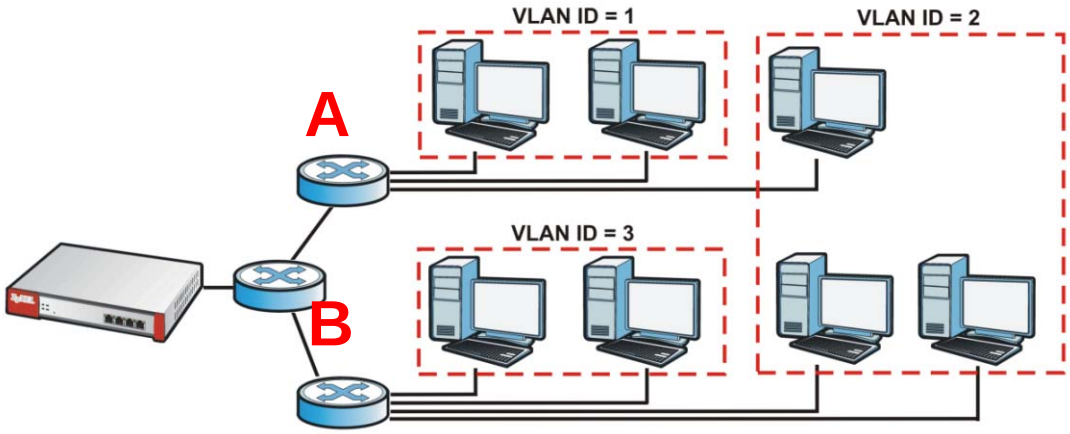
**Figure 164** Example: Before VLAN




In this example, there are two physical networks and three departments **A**, **B**, and **C**. The physical networks are connected to hubs, and the hubs are connected to the router.

Alternatively, you can divide the physical networks into three VLANs.

**Figure 165** Example: After VLAN




Each VLAN is a separate network with separate IP addresses, subnet masks, and gateways. Each VLAN also has a unique identification number (ID). The ID is a 12-bit value that is stored in the MAC header. The VLANs are connected to switches, and the switches are connected to the router. (If one switch has enough connections for the entire network, the network does not need switches **A** and **B**.)

- Traffic inside each VLAN is layer-2 communication (data link layer, MAC addresses). It is handled by the switches. As a result, the new switch is required to handle traffic inside VLAN 2. Traffic is only broadcast inside each VLAN, not each physical network.
- Traffic between VLANs (or between a VLAN and another type of network) is layer-3 communication (network layer, IP addresses). It is handled by the router.

This approach provides a few advantages.

- Increased performance - In VLAN 2, the extra switch should route traffic inside the sales department faster than the router does. In addition, broadcasts are limited to smaller, more logical groups of users.
- Higher security - If each computer has a separate physical connection to the switch, then broadcast traffic in each VLAN is never sent to computers in another VLAN.
- Better manageability - You can align network policies more appropriately for users. For example, you can create different content filtering rules for each VLAN (each department in the example above), and you can set different bandwidth limits for each VLAN. These rules are also independent of the physical network, so you can change the physical network without changing policies.

In this example, the new switch handles the following types of traffic:

- Inside VLAN 2.
- Between the router and VLAN 1.
- Between the router and VLAN 2.
- Between the router and VLAN 3.

### VLAN Interfaces Overview

In the ZyWALL, each VLAN is called a VLAN interface. As a router, the ZyWALL routes traffic between VLAN interfaces, but it does not route traffic within a VLAN interface. All traffic for each VLAN interface can go through only one Ethernet interface, though each Ethernet interface can have one or more VLAN interfaces.

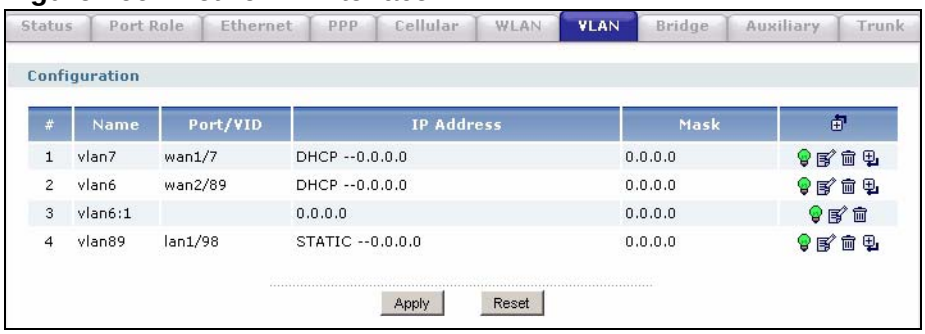
Note: Each VLAN interface is created on top of only one Ethernet interface.

Otherwise, VLAN interfaces are similar to other interfaces in many ways. They have an IP address, subnet mask, and gateway used to make routing decisions. They restrict bandwidth and packet size. They can provide DHCP services, and they can verify the gateway is available.

## 10.13.1 VLAN Summary Screen

This screen lists every VLAN interface and virtual interface created on top of VLAN interfaces. To access this screen, click **Network** > **Interface** > **VLAN**.

**Figure 166** Network > Interface > VLAN




Each field is explained in the following table.

**Table 72** Network > Interface > VLAN

| LABEL | DESCRIPTION |
|---|---|
| # | This field is a sequential value, and it is not associated with any interface. |
| Name | This field displays the name of the interface. |
| Port/VID | For VLAN interfaces, this field displays<br>• the Ethernet interface on which the VLAN interface is created<br>• the VLAN ID<br>For virtual interfaces, this field is blank. |
| IP Address | This field displays the current IP address of the interface. If the IP address is 0.0.0.0, the interface does not have an IP address yet.<br>This screen also shows whether the IP address is a static IP address (**STATIC**) or dynamically assigned (**DHCP**). IP addresses are always static in virtual interfaces. |
| Mask | This field displays the interface's subnet mask in dot decimal notation. |
| Add icon | This column lets you create, edit, remove, activate, and deactivate interfaces.<br>To create a VLAN interface, click the **Add** icon at the top of the column. The **VLAN Add/Edit** screen appears.<br>To create a virtual VLAN interface, click the **Add** icon next to the corresponding VLAN interface. The **Virtual Interface Add/Edit** screen appears. See Section 10.16 on page 256.<br>To edit an interface, click the **Edit** icon next to it. The **VLAN Add/Edit** screen or **Virtual Interface Add/Edit** screen appears accordingly.<br>To remove an interface, click the **Remove** icon next to it. The ZyWALL confirms you want to remove it before doing so.<br>To activate or deactivate an interface, click the **Active** icon next to it. Make sure you click **Apply** to save and apply the change. |

**Table 72** Network > Interface > VLAN (continued)

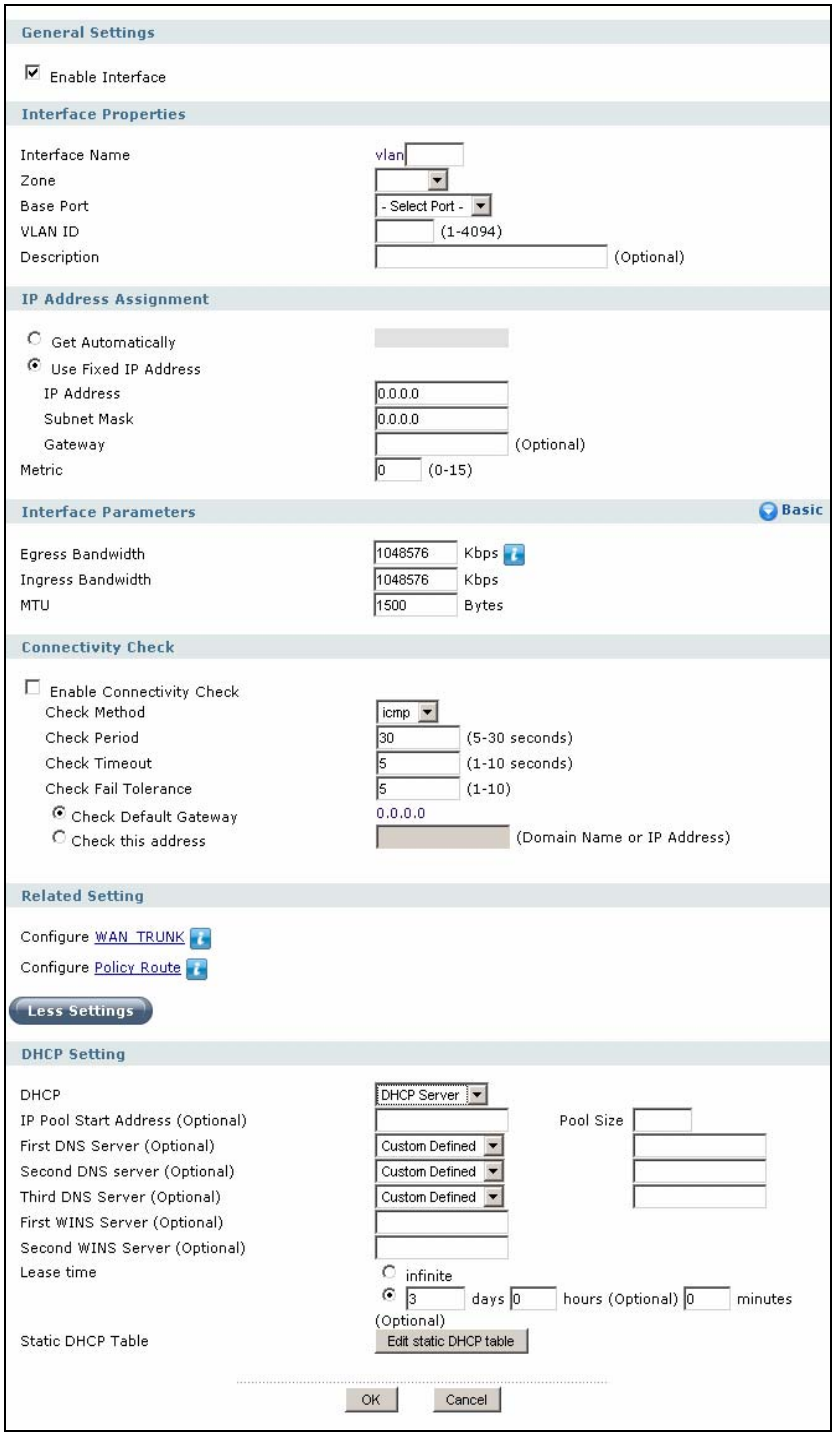
| LABEL | DESCRIPTION |
|---|---|
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 10.13.2 VLAN Add/Edit

This screen lets you configure IP address assignment, interface bandwidth parameters, DHCP settings, and connectivity check for each VLAN interface. To access this screen, click the **Add** icon at the top of the **Add** column or click an

**Edit** icon next to a VLAN interface in the **VLAN Summary** screen. The following screen appears.

**Figure 167** Network > Interface > VLAN > Edit



Each field is explained in the following table.

**Table 73** Network > Interface > VLAN > Edit

| LABEL | DESCRIPTION |
|---|---|
| General Settings | |
| Enable Interface | Select this to turn this interface on. Clear this to disable this interface. |
| Interface Properties | |
| Interface Name | This field is read-only if you are editing an existing VLAN interface. Enter the number of the VLAN interface. You can use a number from 0~4094. See Chapter 52 on page 835 the User's Guide for the total number of VLANs you can configure on the ZyWALL. For example, vlan0, vlan8, and so on. |
| Zone | Use this field to select the zone to which this interface belongs. This controls what security settings the ZyWALL applies to this interface. |
| Base Port | Select the Ethernet interface on which the VLAN interface runs. |
| VLAN ID | Enter the VLAN ID. This 12-bit number uniquely identifies each VLAN. Allowed values are 1 - 4094. (0 and 4095 are reserved.) |
| Description | Enter a description of this interface. It is not used elsewhere. You can use alphanumeric and ( )+/:=?!*#@$_%- characters, and it can be up to 60 characters long. |
| IP Address Assignment | |
| Get Automatically | Select this if this interface is a DHCP client. In this case, the DHCP server configures the IP address, subnet mask, and gateway automatically.<br><br>You should not select this if the interface is assigned to a VRRP group. See Chapter 36 on page 629. |
| Use Fixed IP Address | Select this if you want to specify the IP address, subnet mask, and gateway manually. |
| IP Address | This field is enabled if you select **Use Fixed IP Address**.<br><br>Enter the IP address for this interface. |
| Subnet Mask | This field is enabled if you select **Use Fixed IP Address**.<br><br>Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network. |
| Gateway | This field is enabled if you select **Use Fixed IP Address**.<br><br>Enter the IP address of the gateway. The ZyWALL sends packets to the gateway when it does not know how to route the packet to its destination. The gateway should be on the same network as the interface. |
| Metric | Enter the priority of the gateway (if any) on this interface. The ZyWALL decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the ZyWALL uses the one that was configured first. |

**Table 73** Network > Interface > VLAN > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Interface Parameters | |
| Egress Bandwidth | Enter the maximum amount of traffic, in kilobits per second, the ZyWALL can send through the interface to the network. Allowed values are 0 - 1048576. |
| Ingress Bandwidth | This is reserved for future use.<br>Enter the maximum amount of traffic, in kilobits per second, the ZyWALL can receive from the network through the interface. Allowed values are 0 - 1048576. |
| MTU | Maximum Transmission Unit. Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the ZyWALL divides it into smaller fragments. Allowed values are 576 - 1500. Usually, this value is 1500. |
| Connectivity Check | The ZyWALL can regularly check the connection to the gateway you specified to make sure it is still available. You specify how often to check the connection, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the ZyWALL stops routing to the gateway. The ZyWALL resumes routing to the gateway the first time the gateway passes the connectivity check. |
| Enable Connectivity Check | Select this to turn on the connection check. |
| Check Method | Select the method that the gateway allows.<br>Select **icmp** to have the ZyWALL regularly ping the gateway you specify to make sure it is still available.<br>Select **tcp** to have the ZyWALL regularly perform a TCP handshake with the gateway you specify to make sure it is still available. |
| Check Period | Enter the number of seconds between connection check attempts. |
| Check Timeout | Enter the number of seconds to wait for a response before the attempt is a failure. |
| Check Fail Tolerance | Enter the number of consecutive failures before the ZyWALL stops routing through the gateway. |
| Check Default Gateway | Select this to use the default gateway for the connectivity check. |
| Check this address | Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it. |
| Check Port | This field only displays when you set the **Check Method** to **tcp**. Specify the port number to use for a TCP connectivity check. |
| Related Setting | |
| Configure WAN TRUNK | Click **WAN TRUNK** to go to a screen where you can set this VLAN to be part of a WAN trunk for load balancing. |
| Configure Policy Route | Click **Policy Route** to go to the screen where you can manually configure a policy route to associate traffic with this VLAN. |

**Table 73** Network > Interface > VLAN > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| More Settings/ Less Settings | Click this button to display a greater or lesser number of configuration fields. |
| DHCP Setting | The DHCP settings are available for the OPT, LAN and DMZ interfaces. |
| DHCP | Select what type of DHCP service the ZyWALL provides to the network. Choices are:<br>**None** - the ZyWALL does not provide any DHCP services. There is already a DHCP server on the network.<br>**DHCP Relay** - the ZyWALL routes DHCP requests to one or more DHCP servers you specify. The DHCP server(s) may be on another network.<br>**DHCP Server** - the ZyWALL assigns IP addresses and provides subnet mask, gateway, and DNS server information to the network. The ZyWALL is the DHCP server for the network. |
| | These fields appear if the ZyWALL is a **DHCP Relay**. |
| Relay Server 1 | Enter the IP address of a DHCP server for the network. |
| Relay Server 2 | This field is optional. Enter the IP address of another DHCP server for the network. |
| | These fields appear if the ZyWALL is a **DHCP Server**. |
| IP Pool Start Address | Enter the IP address from which the ZyWALL begins allocating IP addresses. If you want to assign a static IP address to a specific computer, click **Add Static DHCP**.<br>If this field is blank, the **Pool Size** must also be blank. In this case, the ZyWALL can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address. |
| Pool Size | Enter the number of IP addresses to allocate. This number must be at least one and is limited by the interface's **Subnet Mask**. For example, if the **Subnet Mask** is 255.255.255.0 and **IP Pool Start Address** is 10.10.10.10, the ZyWALL can allocate 10.10.10.10 to 10.10.10.254, or 245 IP addresses.<br>If this field is blank, the **IP Pool Start Address** must also be blank. In this case, the ZyWALL can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address. |
| First DNS Server<br>Second DNS Server<br>Third DNS Server | Specify the IP addresses up to three DNS servers for the DHCP clients to use. Use one of the following ways to specify these IP addresses.<br>**Custom Defined** - enter a static IP address.<br>**From ISP** - select the DNS server that another interface received from its DHCP server.<br>**ZyWALL** - the DHCP clients use the IP address of this interface and the ZyWALL works as a DNS relay. |

**Table 73** Network > Interface > VLAN > Edit (continued)

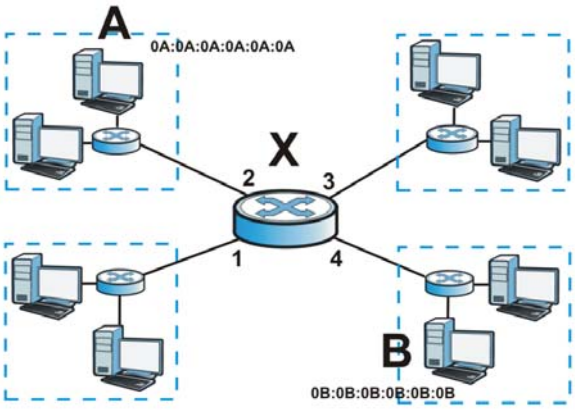
| LABEL | DESCRIPTION |
|---|---|
| First WINS Server, Second WINS Server | Type the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the DHCP clients. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using. |
| Lease time | Specify how long each computer can use the information (especially the IP address) before it has to request the information again. Choices are:<br>**infinite** - select this if IP addresses never expire<br>**days, hours, and minutes** - select this to enter how long IP addresses are valid. |
| Enable IP/MAC Binding | Select this option to have the ZyWALL enforce links between specific IP addresses and specific MAC addresses for this VLAN. This stops anyone else from manually using a bound IP address on another device connected to this interface. Use this to make use only the intended users get to use specific IP addresses. |
| Enable Logs for IP/MAC Binding Violation | Select this option to have the ZyWALL generate a log if a device connected to this VLAN attempts to use an IP address that is bound to another device's MAC address. |
| Edit static DHCP table | Click this to configure static IP addresses for the ZyWALL to assign to computers connected to this interface. See Section 10.6 on page 206. |
| OK | Click **OK** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# 10.14 Bridge Interfaces

This section introduces bridges and bridge interfaces and then explains the screens for bridge interfaces.

## Bridge Overview

A bridge creates a connection between two or more network segments at the layer-2 (MAC address) level. In the following example, bridge X connects four network segments.




When the bridge receives a packet, the bridge records the source MAC address and the port on which it was received in a table. It also looks up the destination MAC address in the table. If the bridge knows on which port the destination MAC address is located, it sends the packet to that port. If the destination MAC address is not in the table, the bridge broadcasts the packet on every port (except the one on which it was received).

In the example above, computer A sends a packet to computer B. Bridge X records the source address 0A:0A:0A:0A:0A:0A and port 2 in the table. It also looks up 0B:0B:0B:0B:0B:0B in the table. There is no entry yet, so the bridge broadcasts the packet on ports 1, 3, and 4.

**Table 74** Example: Bridge Table After Computer A Sends a Packet to Computer B

| MAC ADDRESS | PORT |
|---|---|
| 0A:0A:0A:0A:0A:0A | 2 |

If computer B responds to computer A, bridge X records the source address 0B:0B:0B:0B:0B:0B and port 4 in the table. It also looks up 0A:0A:0A:0A:0A:0A in the table and sends the packet to port 2 accordingly.

**Table 75** Example: Bridge Table After Computer B Responds to Computer A

| MAC ADDRESS | PORT |
|---|---|
| 0A:0A:0A:0A:0A:0A | 2 |
| 0B:0B:0B:0B:0B:0B | 4 |

## Bridge Interface Overview

A bridge interface creates a software bridge between the members of the bridge interface. It also becomes the ZyWALL's interface for the resulting network.

Unlike the device-wide bridge mode in ZyNOS-based ZyWALLs, this ZyWALL can bridge traffic between some interfaces while it routes traffic for other interfaces. The bridge interfaces also support more functions, like interface bandwidth parameters, DHCP settings, and connectivity check. To use the whole ZyWALL as a transparent bridge, add all of the ZyWALL's interfaces to a bridge interface.

A bridge interface may consist of the following members:

- Zero or one WLAN interfaces
- Zero or one VLAN interfaces (and any associated virtual VLAN interfaces)
- Any number of Ethernet interfaces (and any associated virtual Ethernet interfaces)

When you create a bridge interface, the ZyWALL removes the members' entries from the routing table and adds the bridge interface's entries to the routing table. For example, this table shows the routing table before and after you create bridge interface br0 (250.250.250.0/23) between lan1 and vlan1.

**Table 76** Example: Routing Table Before and After Bridge Interface br0 Is Created

| IP ADDRESS(ES) | DESTINATION |
|---|---|
| 210.210.210.0/24 | lan1 |
| 210.211.1.0/24 | lan1:1 |
| 221.221.221.0/24 | vlan0 |
| 222.222.222.0/24 | vlan1 |
| 230.230.230.192/26 | wan2 |
| 241.241.241.241/32 | dmz |
| 242.242.242.242/32 | dmz |

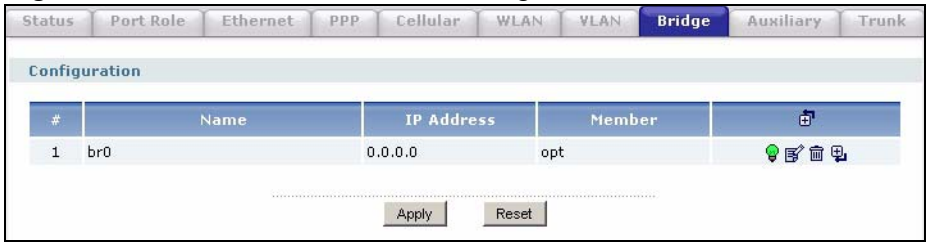
| IP ADDRESS(ES) | DESTINATION |
|---|---|
| 221.221.221.0/24 | vlan0 |
| 230.230.230.192/26 | wan2 |
| 241.241.241.241/32 | dmz |
| 242.242.242.242/32 | dmz |
| 250.250.250.0/23 | br0 |

In this example, virtual Ethernet interface lan1:1 is also removed from the routing table when lan1 is added to br0. Virtual interfaces are automatically added to or remove from a bridge interface when the underlying interface is added or removed.

## 10.14.1 Bridge Summary

This screen lists every bridge interface and virtual interface created on top of bridge interfaces. To access this screen, click **Network** > **Interface** > **Bridge**.

**Figure 168** Network > Interface > Bridge



Each field is described in the following table.

**Table 77** Network > Interface > Bridge

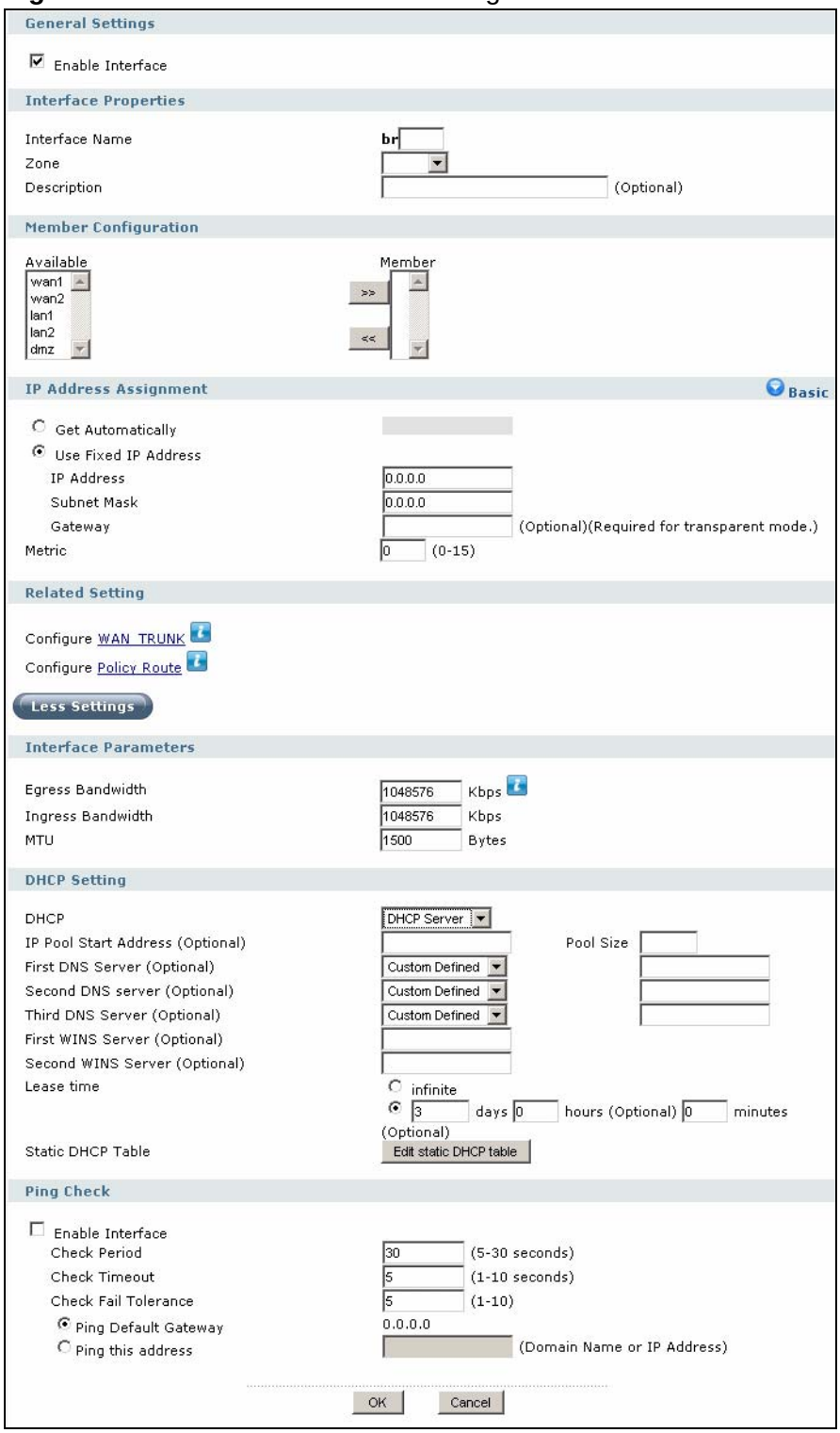
| LABEL | DESCRIPTION |
|---|---|
| # | This field is a sequential value, and it is not associated with any interface. |
| Name | This field displays the name of the interface. |
| IP Address | This field displays the current IP address of the interface. If the IP address is 0.0.0.0, the interface does not have an IP address yet.<br><br>This screen also shows whether the IP address is a static IP address (**STATIC**) or dynamically assigned (**DHCP**). IP addresses are always static in virtual interfaces. |
| Member | This field displays the Ethernet interfaces and VLAN interfaces in the bridge interface. It is blank for virtual interfaces. |
| Add icon | This column lets you create, edit, remove, activate, and deactivate interfaces.<br><br>To create a bridge interface, click the **Add** icon at the top of the column. The **Bridge Add/Edit** screen appears.<br><br>To create a virtual interface, click the **Add** icon next to the corresponding bridge interface. The **Virtual Interface Add/Edit** screen appears. See Section 10.16 on page 256.<br><br>To edit an interface, click the **Edit** icon next to it. The **Bridge Add/Edit** screen or **Virtual Interface Add/Edit** screen appears accordingly.<br><br>To remove an interface, click the **Remove** icon next to it. The ZyWALL confirms you want to remove it before doing so.<br><br>To activate or deactivate an interface, click the **Active** icon next to it. Make sure you click **Apply** to save and apply the change. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 10.14.2 Bridge Add/Edit

This screen lets you configure IP address assignment, interface bandwidth parameters, DHCP settings, and connectivity check for each bridge interface. To access this screen, click the **Add** icon at the top of the **Add** column in the **Bridge**

**Summary** screen, or click an **Edit** icon in the **Bridge Summary** screen. The following screen appears.

**Figure 169** Network > Interface > Bridge > Edit



Each field is described in the table below.

**Table 78** Network > Interface > Bridge > Edit

| LABEL | DESCRIPTION |
|---|---|
| General Settings | |
| Enable Interface | Select this to enable this interface. Clear this to disable this interface. |
| Interface Properties | |
| Interface Name | This field is read-only if you are editing the interface. Enter the name of the bridge interface. The format is br*x*, where *x* is 0 - 11. For example, br0, br3, and so on. |
| Zone | Use this field to select the zone to which this interface belongs. |
| Description | Enter a description of this interface. It is not used elsewhere. You can use alphanumeric and ( )+/:=?!*#@$_%- characters, and it can be up to 60 characters long. |
| Member Configuration | |
| Available | This field displays Ethernet interfaces and VLAN interfaces that can become part of the bridge interface. An interface is not available in the following situations:<br>• There is a virtual interface on top of it<br>• It is already used in a different bridge interface<br>Select one, and click the **>>** arrow to add it to the bridge interface. Each bridge interface can only have one VLAN interface. |
| Member | This field displays the interfaces that are part of the bridge interface. Select one, and click the **<<** arrow to remove it from the bridge interface. |
| IP Address Assignment | |
| Get Automatically | Select this if this interface is a DHCP client. In this case, the DHCP server configures the IP address, subnet mask, and gateway automatically. |
| Use Fixed IP Address | Select this if you want to specify the IP address, subnet mask, and gateway manually. |
| IP Address | This field is enabled if you select **Use Fixed IP Address**.<br>Enter the IP address for this interface. |
| Subnet Mask | This field is enabled if you select **Use Fixed IP Address**.<br>Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network. |
| Gateway | This field is enabled if you select **Use Fixed IP Address**.<br>Enter the IP address of the gateway. The ZyWALL sends packets to the gateway when it does not know how to route the packet to its destination. The gateway should be on the same network as the interface. |

**Table 78** Network > Interface > Bridge > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Metric | Enter the priority of the gateway (if any) on this interface. The ZyWALL decides which gateway to use based on this priority. The lower the number, the higher the priority. If two or more gateways have the same priority, the ZyWALL uses the one that was configured first. |
| Related Setting | |
| Configure WAN TRUNK | Click **WAN TRUNK** to go to a screen where you can configure the interface as part of a WAN trunk for load balancing. |
| Configure Policy Route | Click **Policy Route** to go to the screen where you can manually configure a policy route to associate traffic with this interface. |
| More Settings/ Less Settings | Click this button to display a greater or lesser number of configuration fields. |
| Interface Parameters | |
| Egress Bandwidth | Enter the maximum amount of traffic, in kilobits per second, the ZyWALL can send through the interface to the network. Allowed values are 0 - 1048576. |
| Ingress Bandwidth | This is reserved for future use.<br>Enter the maximum amount of traffic, in kilobits per second, the ZyWALL can receive from the network through the interface. Allowed values are 0 - 1048576. |
| MTU | Maximum Transmission Unit. Type the maximum size of each data packet, in bytes, that can move through this interface. If a larger packet arrives, the ZyWALL divides it into smaller fragments. Allowed values are 576 - 1500. Usually, this value is 1500. |
| DHCP Settings | |
| DHCP | Select what type of DHCP service the ZyWALL provides to the network. Choices are:<br>**None** - the ZyWALL does not provide any DHCP services. There is already a DHCP server on the network.<br>**DHCP Relay** - the ZyWALL routes DHCP requests to one or more DHCP servers you specify. The DHCP server(s) may be on another network.<br>**DHCP Server** - the ZyWALL assigns IP addresses and provides subnet mask, gateway, and DNS server information to the network. The ZyWALL is the DHCP server for the network. |
| | These fields appear if the ZyWALL is a **DHCP Relay**. |
| Relay Server 1 | Enter the IP address of a DHCP server for the network. |
| Relay Server 2 | This field is optional. Enter the IP address of another DHCP server for the network. |
| | These fields appear if the ZyWALL is a **DHCP Server**. |

**Table 78** Network > Interface > Bridge > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| IP Pool Start Address | Enter the IP address from which the ZyWALL begins allocating IP addresses. If you want to assign a static IP address to a specific computer, click **Add Static DHCP**.<br><br>If this field is blank, the **Pool Size** must also be blank. In this case, the ZyWALL can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address. |
| Pool Size | Enter the number of IP addresses to allocate. This number must be at least one and is limited by the interface's **Subnet Mask**. For example, if the **Subnet Mask** is 255.255.255.0 and **IP Pool Start Address** is 10.10.10.10, the ZyWALL can allocate 10.10.10.10 to 10.10.10.254, or 245 IP addresses.<br><br>If this field is blank, the **IP Pool Start Address** must also be blank. In this case, the ZyWALL can assign every IP address allowed by the interface's IP address and subnet mask, except for the first address (network address), last address (broadcast address) and the interface's IP address. |
| First DNS Server<br>Second DNS Server<br>Third DNS Server | Specify the IP addresses up to three DNS servers for the DHCP clients to use. Use one of the following ways to specify these IP addresses.<br><br>**Custom Defined** - enter a static IP address.<br><br>**From ISP** - select the DNS server that another interface received from its DHCP server.<br><br>**ZyWALL** - the DHCP clients use the IP address of this interface and the ZyWALL works as a DNS relay. |
| First WINS Server, Second WINS Server | Type the IP address of the WINS (Windows Internet Naming Service) server that you want to send to the DHCP clients. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using. |
| Lease time | Specify how long each computer can use the information (especially the IP address) before it has to request the information again. Choices are:<br><br>**infinite** - select this if IP addresses never expire<br><br>**days, hours, and minutes** - select this to enter how long IP addresses are valid. |
| Enable IP/MAC Binding | Select this option to have this interface enforce links between specific IP addresses and specific MAC addresses. This stops anyone else from manually using a bound IP address on another device connected to this interface. Use this to make use only the intended users get to use specific IP addresses. |
| Enable Logs for IP/MAC Binding Violation | Select this option to have the ZyWALL generate a log if a device connected to this interface attempts to use an IP address that is bound to another device's MAC address. |
| Edit static DHCP table | Click this to configure static IP addresses for the ZyWALL to assign to computers connected to this interface. See Section 10.6 on page 206. |

**Table 78** Network > Interface > Bridge > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Connectivity Check | The interface can regularly check the connection to the gateway you specified to make sure it is still available. You specify how often the interface checks the connection, how long to wait for a response before the attempt is a failure, and how many consecutive failures are required before the ZyWALL stops routing to the gateway. The ZyWALL resumes routing to the gateway the first time the gateway passes the connectivity check. |
| Enable Connectivity Check | Select this to turn on the connection check. |
| Check Method | Select the method that the gateway allows.<br>Select **icmp** to have the ZyWALL regularly ping the gateway you specify to make sure it is still available.<br>Select **tcp** to have the ZyWALL regularly perform a TCP handshake with the gateway you specify to make sure it is still available. |
| Check Period | Enter the number of seconds between connection check attempts. |
| Check Timeout | Enter the number of seconds to wait for a response before the attempt is a failure. |
| Check Fail Tolerance | Enter the number of consecutive failures before the ZyWALL stops routing through the gateway. |
| Check Default Gateway | Select this to use the default gateway for the connectivity check. |
| Check this address | Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it. |
| Check Port | This field only displays when you set the **Check Method** to **tcp**. Specify the port number to use for a TCP connectivity check. |
| OK | Click **OK** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# 10.15 Auxiliary Interface

This section introduces the auxiliary interface and then explains the screen for it.

## 10.15.1 Auxiliary Interface Overview

Use the auxiliary interface to dial out from the ZyWALL's auxiliary port. For example, you might use this interface as a backup WAN interface.

You have to connect an external modem to the ZyWALL's auxiliary port to use the auxiliary interface.

Note: You have to connect an external modem to the auxiliary port.

The ZyWALL uses the auxiliary interface to dial out in two situations.

1 You click the **Connect** icon on the ZyWALL **Status** screen.

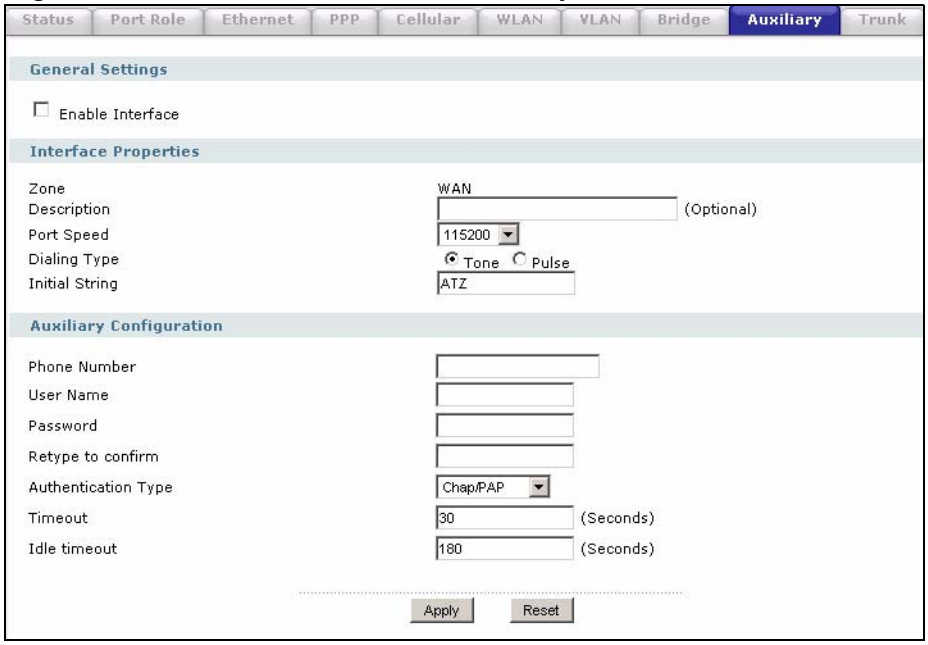
2 The load auxiliary interface must connect to satisfy load-balancing requirements. You have to add the auxiliary interface to a trunk first.

When the ZyWALL hangs up the call, it drops the Data Terminal Ready (DTR) signal and issues the command ATH.

## 10.15.2 Auxiliary

Use the **Auxiliary** screen to configure the ZyWALL's auxiliary interface. Click **Network > Interface > Auxiliary** to open it.

**Figure 170** Network > Interface > Auxiliary




Each field is described in the table below.

**Table 79** Network > Interface > Auxiliary

| LABEL | DESCRIPTION |
|---|---|
| General Settings | |
| Enable Interface | Select this to turn on the auxiliary dial up interface. The interface does not dial out, however, unless it is part of a trunk and load-balancing conditions are satisfied. |
| Interface Properties | |
| Zone | This field is read-only and displays the zone to which the auxiliary interface belongs. |

**Table 79** Network > Interface > Auxiliary (continued)

| LABEL | DESCRIPTION |
|---|---|
| Description | Enter a description of this interface. It is not used elsewhere. You can use alphanumeric and ( )+/:=?!*#@$_%- characters, and it can be up to 60 characters long. |
| Port Speed | Select the speed of the connection between the ZyWALL and external computer. |
| Dialing Type | **Tone** - select this if the telephone uses tone-based dialing.<br>**Pulse** - select this if the telephone uses pulse-based dialing. |
| Initial String | Enter the AT command string to initialize the external modem. ATZ is the most common string, but you should check the manual for the external modem for additional commands. |
| Auxiliary Configuration | |
| Phone Number | Enter the phone number to dial here. You can use 1-20 numbers, commas (,), or plus signs (+). Use a comma to pause during dialing. Use a plus sign to tell the external modem to make an international call. |
| User Name | Enter the user name required for authentication. |
| Password | Enter the password required for authentication. |
| Retype to confirm | Enter the password again to make sure you have not typed it incorrectly. |
| Authentication Type | Select the authentication protocol to use for outgoing calls. Choices are:<br>**CHAP/PAP** - Your ZyWALL accepts either CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol), as requested by the computer you are dialing.<br>**CHAP** - Your ZyWALL accepts CHAP only.<br>**PAP** - Your ZyWALL accepts PAP only.<br>**MSCHAP** - Your ZyWALL accepts MSCHAP only.<br>**MSCHAP-V2** - Your ZyWALL accepts MSCHAP-V2 only. |
| Timeout | Type the number of seconds the ZyWALL tries to set up a connection before it stops. Allowed values are 30 - 120. |
| Idle timeout | Type the number of seconds the ZyWALL should wait for traffic before it automatically disconnects the connection. Set this field to zero to disable the idle timeout. Allowed values are 0 - 360. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# 10.16 Virtual Interfaces

Use virtual interfaces to tell the ZyWALL where to route packets. Virtual interfaces can also be used in VPN gateways (see Chapter 21 on page 363) and VRRP groups (see Chapter 36 on page 629).

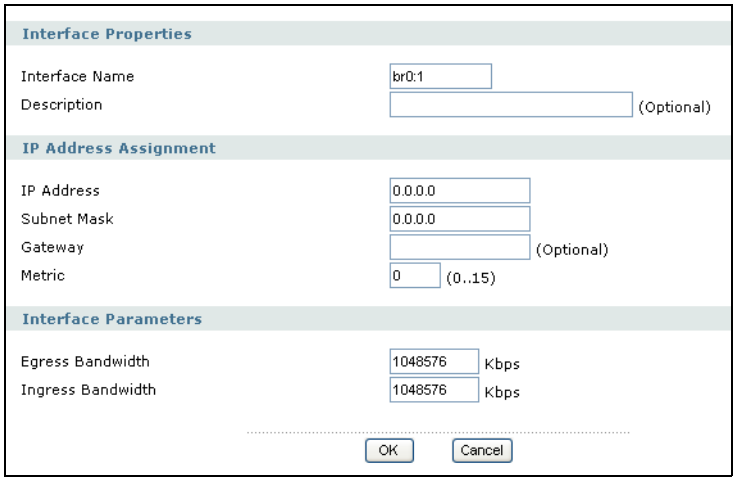
Virtual interfaces can be created on top of Ethernet interfaces, VLAN interfaces, or bridge interfaces. Virtual VLAN interfaces recognize and use the same VLAN ID. Otherwise, there is no difference between each type of virtual interface. Network policies (for example, firewall rules) that apply to the underlying interface automatically apply to the virtual interface as well.

Like other interfaces, virtual interfaces have an IP address, subnet mask, and gateway used to make routing decisions. However, you have to manually specify the IP address and subnet mask; virtual interfaces cannot be DHCP clients. Like other interfaces, you can restrict bandwidth through virtual interfaces, but you cannot change the MTU. The virtual interface uses the same MTU that the underlying interface uses. Unlike other interfaces, virtual interfaces do not provide DHCP services, and they do not verify that the gateway is available.

## 10.16.1 Virtual Interfaces Add/Edit

This screen lets you configure IP address assignment and interface parameters for virtual interfaces. To access this screen, click an **Add** icon next to an Ethernet interface, VLAN interface, or bridge interface in the respective interface summary screen.

**Figure 171** Network > Interface > Add



Each field is described in the table below.

**Table 80** Network > Interface > Add

| LABEL | DESCRIPTION |
|---|---|
| Interface Properties | |
| Interface Name | This field is read-only. It displays the name of the virtual interface, which is automatically derived from the underlying Ethernet interface, VLAN interface, or bridge interface. |
| Description | Enter a description of this interface. It is not used elsewhere. You can use alphanumeric and ( )+/:=?!*#@$_%- characters, and it can be up to 60 characters long. |
| IP Address Assignment | |
| IP Address | Enter the IP address for this interface. |
| Subnet Mask | Enter the subnet mask of this interface in dot decimal notation. The subnet mask indicates what part of the IP address is the same for all computers in the network. |
| Interface Parameters | |
| Egress Bandwidth | Enter the maximum amount of traffic, in kilobits per second, the ZyWALL can send through the interface to the network. Allowed values are 0 - 1048576. |
| Ingress Bandwidth | This is reserved for future use.<br>Enter the maximum amount of traffic, in kilobits per second, the ZyWALL can receive from the network through the interface. Allowed values are 0 - 1048576. |
| OK | Click **OK** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# 10.17 Interface Technical Reference

Here is more detailed information about interfaces on the ZyWALL.

### IP Address Assignment

Most interfaces have an IP address and a subnet mask. This information is used to create an entry in the routing table.

**Figure 172** Example: Entry in the Routing Table Derived from Interfaces

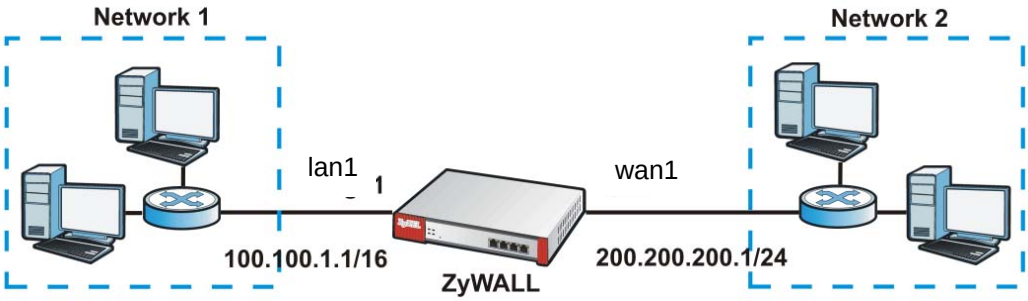



**Table 81** Example: Routing Table Entries for Interfaces

| IP ADDRESS(ES) | DESTINATION |
|---|---|
| 100.100.1.1/16 | lan1 |
| 200.200.200.1/24 | wan1 |

For example, if the ZyWALL gets a packet with a destination address of 100.100.25.25, it routes the packet to interface lan1. If the ZyWALL gets a packet with a destination address of 200.200.200.200, it routes the packet to interface wan1.

In most interfaces, you can enter the IP address and subnet mask manually. In PPPoE/PPTP interfaces, however, the subnet mask is always 255.255.255.255 because it is a point-to-point interface. For these interfaces, you can only enter the IP address.

In many interfaces, you can also let the IP address and subnet mask be assigned by an external DHCP server on the network. In this case, the interface is a DHCP client. Virtual interfaces, however, cannot be DHCP clients. You have to assign the IP address and subnet mask manually.

In general, the IP address and subnet mask of each interface should not overlap, though it is possible for this to happen with DHCP clients.

In the example above, if the ZyWALL gets a packet with a destination address of 5.5.5.5, it might not find any entries in the routing table. In this case, the packet is dropped. However, if there is a default router to which the ZyWALL should send this packet, you can specify it as a gateway in one of the interfaces. For example, if there is a default router at 200.200.200.100, you can create a gateway at

200.200.200.100 on ge2. In this case, the ZyWALL creates the following entry in the routing table.

**Table 82** Example: Routing Table Entry for a Gateway

| IP ADDRESS(ES) | DESTINATION |
|---|---|
| 0.0.0.0/0 | 200.200.200.100 |

The gateway is an optional setting for each interface. If there is more than one gateway, the ZyWALL uses the gateway with the lowest metric, or cost. If two or more gateways have the same metric, the ZyWALL uses the one that was set up first (the first entry in the routing table). In PPPoE/PPTP interfaces, the other computer is the gateway for the interface by default. In this case, you should specify the metric.

If the interface gets its IP address and subnet mask from a DHCP server, the DHCP server also specifies the gateway, if any.

### Interface Parameters

The ZyWALL restricts the amount of traffic into and out of the ZyWALL through each interface.

- Egress bandwidth sets the amount of traffic the ZyWALL sends out through the interface to the network.
- Ingress bandwidth sets the amount of traffic the ZyWALL allows in through the interface from the network.[1]

If you set the bandwidth restrictions very high, you effectively remove the restrictions.

The ZyWALL also restricts the size of each data packet. The maximum number of bytes in each packet is called the maximum transmission unit (MTU). If a packet is larger than the MTU, the ZyWALL divides it into smaller fragments. Each fragment is sent separately, and the original packet is re-assembled later. The smaller the MTU, the more fragments sent, and the more work required to re-assemble packets correctly. On the other hand, some communication channels, such as Ethernet over ATM, might not be able to handle large data packets.

### DHCP Settings

Dynamic Host Configuration Protocol (DHCP, RFC 2131, RFC 2132) provides a way to automatically set up and maintain IP addresses, subnet masks, gateways, and some network information (such as the IP addresses of DNS servers) on

1. At the time of writing, the ZyWALL does not support ingress bandwidth management.

computers in the network. This reduces the amount of manual configuration you have to do and usually uses available IP addresses more efficiently.

In DHCP, every network has at least one DHCP server. When a computer (a DHCP client) joins the network, it submits a DHCP request. The DHCP servers get the request; assign an IP address; and provide the IP address, subnet mask, gateway, and available network information to the DHCP client. When the DHCP client leaves the network, the DHCP servers can assign its IP address to another DHCP client.

In the ZyWALL, some interfaces can provide DHCP services to the network. In this case, the interface can be a DHCP relay or a DHCP server.

As a DHCP relay, the interface routes DHCP requests to DHCP servers on different networks. You can specify more than one DHCP server. If you do, the interface routes DHCP requests to all of them. It is possible for an interface to be a DHCP relay and a DHCP client simultaneously.

As a DHCP server, the interface provides the following information to DHCP clients.

- IP address - If the DHCP client's MAC address is in the ZyWALL's static DHCP table, the interface assigns the corresponding IP address. If not, the interface assigns IP addresses from a pool, defined by the starting address of the pool and the pool size.

**Table 83** Example: Assigning IP Addresses from a Pool

| START IP ADDRESS | POOL SIZE | RANGE OF ASSIGNED IP ADDRESS |
|---|---|---|
| 50.50.50.33 | 5 | 50.50.50.33 - 50.50.50.37 |
| 75.75.75.1 | 200 | 75.75.75.1 - 75.75.75.200 |
| 99.99.1.1 | 1023 | 99.99.1.1 - 99.99.4.255 |
| 120.120.120.100 | 100 | 120.120.120.100 - 120.120.120.199 |

  The ZyWALL cannot assign the first address (network address) or the last address (broadcast address) in the subnet defined by the interface's IP address and subnet mask. For example, in the first entry, if the subnet mask is 255.255.255.0, the ZyWALL cannot assign 50.50.50.0 or 50.50.50.255. If the subnet mask is 255.255.0.0, the ZyWALL cannot assign 50.50.0.0 or 50.50.255.255. Otherwise, it can assign every IP address in the range, except the interface's IP address.

  If you do not specify the starting address or the pool size, the interface the maximum range of IP addresses allowed by the interface's IP address and subnet mask. For example, if the interface's IP address is 9.9.9.1 and subnet mask is 255.255.255.0, the starting IP address in the pool is 9.9.9.2, and the pool size is 253.

- Subnet mask - The interface provides the same subnet mask you specify for the interface. See IP Address Assignment on page 258.
- Gateway - The interface provides the same gateway you specify for the interface. See IP Address Assignment on page 258.

- DNS servers - The interface provides IP addresses for up to three DNS servers that provide DNS services for DHCP clients. You can specify each IP address manually (for example, a company's own DNS server), or you can refer to DNS servers that other interfaces received from DHCP servers (for example, a DNS server at an ISP). These other interfaces have to be DHCP clients.

It is not possible for an interface to be the DHCP server and a DHCP client simultaneously.

### WINS

WINS (Windows Internet Naming Service) is a Windows implementation of NetBIOS Name Server (NBNS) on Windows. It keeps track of NetBIOS computer names. It stores a mapping table of your network's computer names and IP addresses. The table is dynamically updated for IP addresses assigned by DHCP. This helps reduce broadcast traffic since computers can query the server instead of broadcasting a request for a computer name's IP address. In this way WINS is similar to DNS, although WINS does not use a hierarchy (unlike DNS). A network can have more than one WINS server. Samba can also serve as a WINS server.

### PPPoE/PPTP Overview

Point-to-Point Protocol over Ethernet (PPPoE, RFC 2516) and Point-to-Point Tunneling Protocol (PPTP, RFC 2637) are usually used to connect two computers over phone lines or broadband connections. PPPoE is often used with cable modems and DSL connections. It provides the following advantages:

- The access and authentication method works with existing systems, including RADIUS.
- You can access one of several network services. This makes it easier for the service provider to offer the service
- PPPoE does not usually require any special configuration of the modem.

PPTP is used to set up virtual private networks (VPN) in unsecure TCP/IP environments. It sets up two sessions.

1. The first one runs on TCP port 1723. It is used to start and manage the second one.
2. The second one uses Generic Routing Encapsulation (GRE, RFC 2890) to transfer information between the computers.

PPTP is convenient and easy-to-use, but you have to make sure that firewalls support both PPTP sessions.

# 11 Trunks

## 11.1 Overview

Use trunks for WAN traffic load balancing to increase overall network throughput and reliability. Load balancing divides traffic loads between multiple interfaces. This allows you to improve quality of service and maximize bandwidth utilization for multiple ISP links.

Maybe you have two Internet connections with different bandwidths. You could set up a trunk that uses spillover or weighted round robin load balancing so time-sensitive traffic (like video) usually goes through the higher-bandwidth interface. For other traffic, you might want to use least load first load balancing to even out the distribution of the traffic load.

Suppose ISP A has better connections to Europe while ISP B has better connections to Australia. You could use policy routes and trunks to have traffic for your European branch office primarily use ISP A and traffic for your Australian branch office primarily use ISP B.

Or maybe one of the ZyWALL's interfaces is connected to an ISP that is also your Voice over IP (VoIP) service provider. You can use policy routing to send the VoIP traffic through a trunk with the interface connected to the VoIP service provider set to active and another interface (connected to another ISP) set to passive. This way VoIP traffic goes through the interface connected to the VoIP service provider whenever the interface's connection is up.

### 11.1.1 What You Can Do in the Trunk Screens

- Use the **Trunk** summary screen (Section 11.2 on page 267) to configure link sticking and view the list of configured trunks and which load balancing algorithm each trunk uses.
- Use the **Trunk Edit** screen (Section 11.3 on page 268) to configure which interfaces belong to each trunk and the load balancing algorithm each trunk uses.

## 11.1.2 What You Need to Know About Trunks

- Add WAN interfaces to trunks to have multiple connections share the traffic load.
- If one WAN interface's connection goes down, the ZyWALL sends traffic through another member of the trunk.
- For example, you connect one WAN interface to one ISP and connect a second WAN interface to a second ISP. The ZyWALL balances the WAN traffic load between the connections. If one interface's connection goes down, the ZyWALL can automatically send its traffic through another interface.

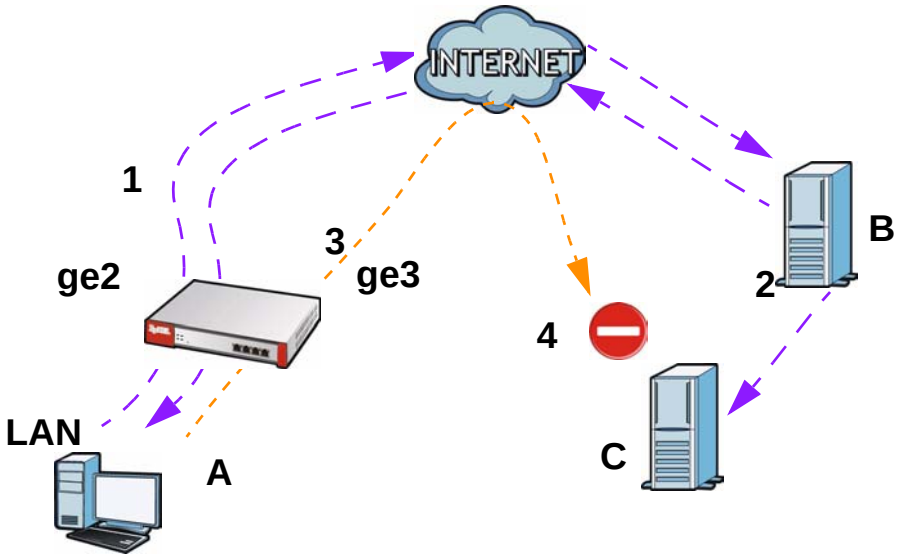
You can also use trunks with policy routing to send specific traffic types through the best WAN interface for that type of traffic.

- If that interface's connection goes down, the ZyWALL can still send its traffic through another interface.
- You can define multiple trunks for the same physical interfaces.

### Link Sticking

You can have the ZyWALL send each local computer's traffic through a single WAN interface for a specified period of time. This is useful when a redirect server forwards a user request for a file and informs the file server that a particular WAN IP address is requesting the file. If the user's subsequent sessions came from a different WAN IP address, the file server would deny the request. Here is an example.

**Figure 173** Link Sticking




1 LAN user **A** tries to download a file from server **B** on the Internet. The ZyWALL uses ge2 to send the request to server **B**.

2 However remote server **B** is actually a redirect server. So server **B** sends a file list to LAN user **A**. The file list lets LAN user **A**'s computer know that the desired file is actually on file server (**C**). At the same time, register server **B** informs file server **C** that a computer located at the ge2's IP address will download a file.

3 The ZyWALL is using active/active load balancing. So when LAN user **A** tries to retrieve the file from file server **C**, the request goes out through ge3.

4 File server **C** finds that the request comes from ge3's IP address instead of ge2's IP address and rejects the request.

5 If link sticking had been configured, the ZyWALL would have still used ge2 to send LAN user **A**'s request to file server **C** and the file server would have given the file to **A**.

### Load Balancing Algorithms

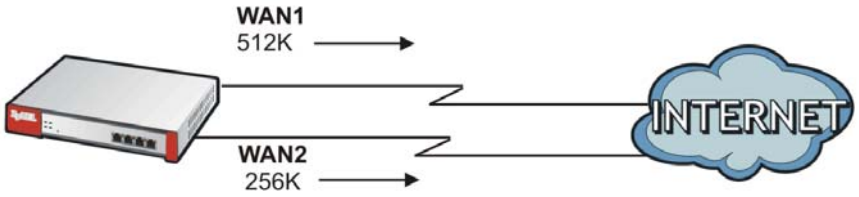
The following sections describe the load balancing algorithms the ZyWALL can use to decide which interface the traffic (from the LAN) should use for a session[2]. The available bandwidth you configure on the ZyWALL refers to the actual bandwidth provided by the ISP and the measured bandwidth refers to the bandwidth an interface is currently using.

### Least Load First

The least load first algorithm uses the current (or recent) outbound bandwidth utilization of each trunk member interface as the load balancing index(es) when making decisions about to which interface a new session is to be distributed. The outbound bandwidth utilization is defined as the measured outbound throughput over the available outbound bandwidth.

Here the ZyWALL has two WAN interfaces connected to the Internet. The configured available outbound bandwidths for WAN 1 and WAN 2 are 512K and 256K respectively.

**Figure 174** Least Load First Example




The outbound bandwidth utilization is used as the load balancing index. In this example, the measured (current) outbound throughput of WAN 1 is 412K and

2. In the load balancing section, a session may refer to normal connection-oriented, UDP and SNMP2 traffic.

WAN 2 is 198K. The ZyWALL calculates the load balancing index as shown in the table below.

Since WAN 2 has a smaller load balancing index (meaning that it is less utilized than WAN 1), the ZyWALL will send the subsequent new session traffic through WAN 2.

**Table 84** Least Load First Example

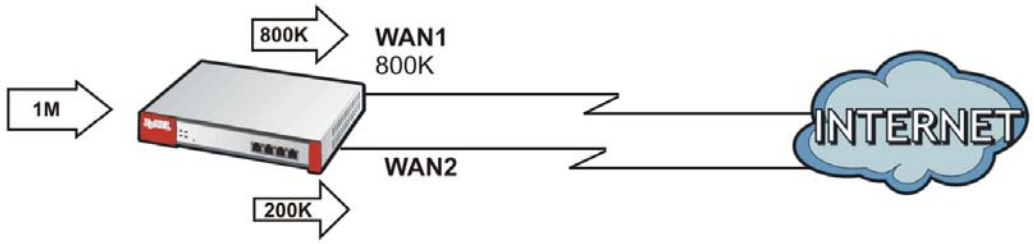
| INTERFACE | OUTBOUND | | LOAD BALANCING INDEX (M/A) |
|---|---|---|---|
| | AVAILABLE (A) | MEASURED (M) | |
| WAN 1 | 512 K | 412 K | 0.8 |
| WAN 2 | 256 K | 198 K | 0.77 |

## Weighted Round Robin

The Weighted Round Robin (WRR) algorithm is best suited for situations when the bandwidths set for the two WAN interfaces are different. Similar to the Round Robin (RR) algorithm (see Section 11.4 on page 270), the Weighted Round Robin (WRR) algorithm sets the ZyWALL to send traffic through each WAN interface in turn. In addition, the WAN interfaces are assigned weights. An interface with a larger weight gets more of the traffic than an interface with a smaller weight.

For example, in the figure below, the configured available bandwidth of ge2 is 1M and ge3 is 512K. You can set the ZyWALL to distribute the network traffic between the two interfaces by setting the weight of ge2 and ge3 to 2 and 1 respectively. The ZyWALL assigns the traffic of two sessions to ge2 for every session's traffic assigned to ge3.

**Figure 175** Weighted Round Robin Algorithm Example



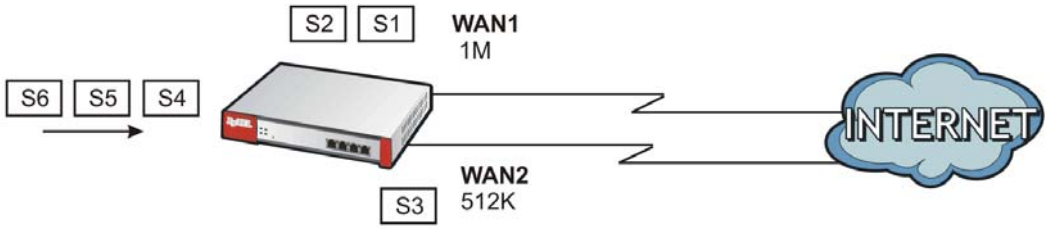

## Spillover

The spillover load balancing algorithm sends network traffic to the first interface in the trunk member list until the interface's maximum allowable load is reached, then sends the excess network traffic of new sessions to the next interface in the trunk member list. This continues as long as there are more member interfaces and traffic to be sent through them.

Suppose the first trunk member interface uses an unlimited access Internet connection and the second is billed by usage. Spillover load balancing only uses the second interface when the traffic load exceeds the threshold on the first interface. This fully utilizes the bandwidth of the first interface to reduce Internet usage fees and avoid overloading the interface.

In this example figure, the upper threshold of the first interface is set to 800K. The ZyWALL sends network traffic of new sessions that exceed this limit to the secondary WAN interface.

**Figure 176** Spillover Algorithm Example



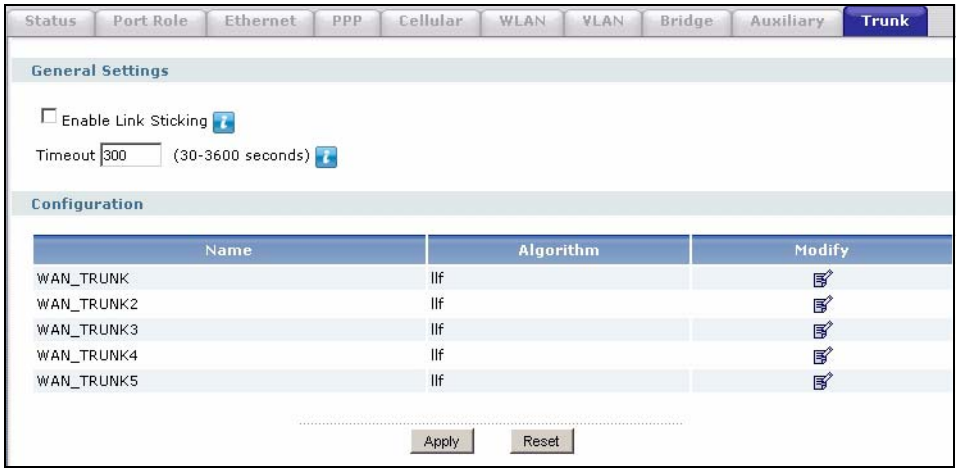

### Finding Out More

- See Section 5.4.3 on page 88 for related information on the **Trunk** screens.
- See Section 11.4 on page 270 for more background information on trunks.
- See Section 6.3 on page 108 for an example of how to configure load balancing.

## 11.2 The Trunk Summary Screen

Click **Network > Interface > Trunk** to open the **Trunk** screen. This screen lists the configured trunks and the load balancing algorithm that each is configured to use.

**Figure 177** Network > Interface > Trunk



The following table describes the items in this screen.

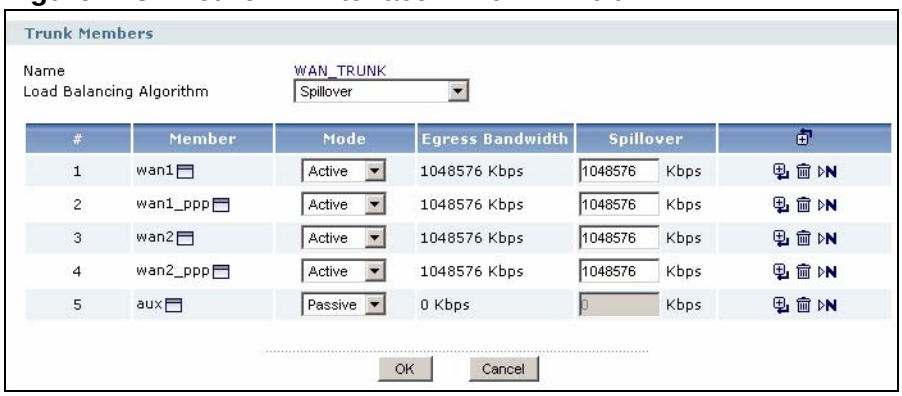
**Table 85** Network > Interface > Trunk

| LABEL | DESCRIPTION |
|---|---|
| Enable Link Sticking | Select this option to have the ZyWALL send all of each local computer's traffic through one WAN interface for the number of seconds that you specify.<br><br>This is useful when a redirect server forwards a local user's request for a file and informs the file server that a particular WAN IP address is requesting the file. If the user's subsequent sessions came from a different WAN IP address, the file server would deny the request. See Link Sticking on page 264 for an example.<br><br>This setting applies when you use load balancing and have multiple WAN interfaces set to active mode. |
| Timeout | Specify for how long the ZyWALL is to send all of each local computer's traffic through one WAN interface. |
| Name | This field displays the label that you specified to identify the trunk. |
| Algorithm | This field displays the load balancing method that the trunk is set to use. |
| Add icon | This column lets you edit trunks.<br><br>To edit a trunk, click the **Edit** icon next to it. The **Trunk Members** screen appears. |
| Apply | Click this button to save your changes to the ZyWALL. |
| Reset | Click this button to return the screen to its last-saved settings. |

# 11.3 Configuring a Trunk

Click **Network > Interface > Trunk** and then the **Edit** icon to open the **Trunk Edit** screen.

**Figure 178** Network > Interface > Trunk > Edit



Each field is described in the table below.

**Table 86** Network > Interface > Trunk > Edit

| LABEL | DESCRIPTION |
|---|---|
| Name | This is the descriptive name for this trunk. |
| Load Balancing Algorithm | Select a load balancing method to use from the drop-down list box.<br>Select **Weighted Round Robin** to balance the traffic load between interfaces based on their respective weights. Weighted round robin is activated only when the first group member interface has more traffic than it can handle.<br>Select **Least Load First** to send new session traffic through the least utilized trunk member.<br>Select **Spillover** to send network traffic through the first interface in the group member list until there is enough traffic that the second interface needs to be used (and so on). |
| # | This column displays the priorities of the group's interfaces. The order of the interfaces in the list is important since they are used in the order they are listed. |
| Member | Click this icon to open a screen where you can select an interface to be a group member. |
| Mode | Select **Active** to have the ZyWALL always attempt to use this connection.<br>Select **Passive** to have the ZyWALL only use this connection when all of the connections set to active are down. You can only set one of a group's interfaces to passive mode. |
| Weight | This field displays with the weighted round robin load balancing algorithm. Specify the weight (1~10) for the interface. The weights of the different member interfaces form a ratio. This ratio determines how much traffic the ZyWALL sends through each member interface. The higher an interface's weight is (relative to the weights of the interfaces), the more traffic the ZyWALL sends through that interface. |
| Ingress Bandwidth | This field displays with the least load first load balancing algorithm. It displays the maximum number of kilobits of data the ZyWALL is to allow to come in through the interface per second. |
| Egress Bandwidth | This field displays with the least load first or spillover load balancing algorithm.It displays the maximum number of kilobits of data the ZyWALL is to send out through the interface per second. |
| Spillover | This field displays with the spillover load balancing algorithm. Specify the maximum bandwidth of traffic in kilobits per second (1~1048576) to send out through the interface before using another interface. When this spillover bandwidth limit is exceeded, the ZyWALL sends new session traffic through the next interface. The traffic of existing sessions still goes through the interface on which they started.<br>The ZyWALL uses the group member interfaces in the order that they are listed. |

**Table 86** Network > Interface > Trunk > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Add icon | This column lets you add, remove and move trunk members.<br>To add an interface to the trunk, click an **Add** icon. The **Trunk Member Select** screen appears.<br>To remove an interface from a trunk, click the **Remove** icon next to it. The ZyWALL confirms you want to remove it before doing so.<br>To move an interface to a different number in the list, click the **Move** icon next to it. In the field that appears, specify the number to which you want to move the interface. |
| OK | Click **OK** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# 11.4 Trunk Technical Reference

### Round Robin Load Balancing Algorithm

Round Robin scheduling services queues on a rotating basis and is activated only when an interface has more traffic than it can handle. A queue is given an amount of bandwidth irrespective of the incoming traffic on that interface. This queue then moves to the back of the list. The next queue is given an equal amount of bandwidth, and then moves to the end of the list; and so on, depending on the number of queues being used. This works in a looping fashion until a queue is empty.

# 12

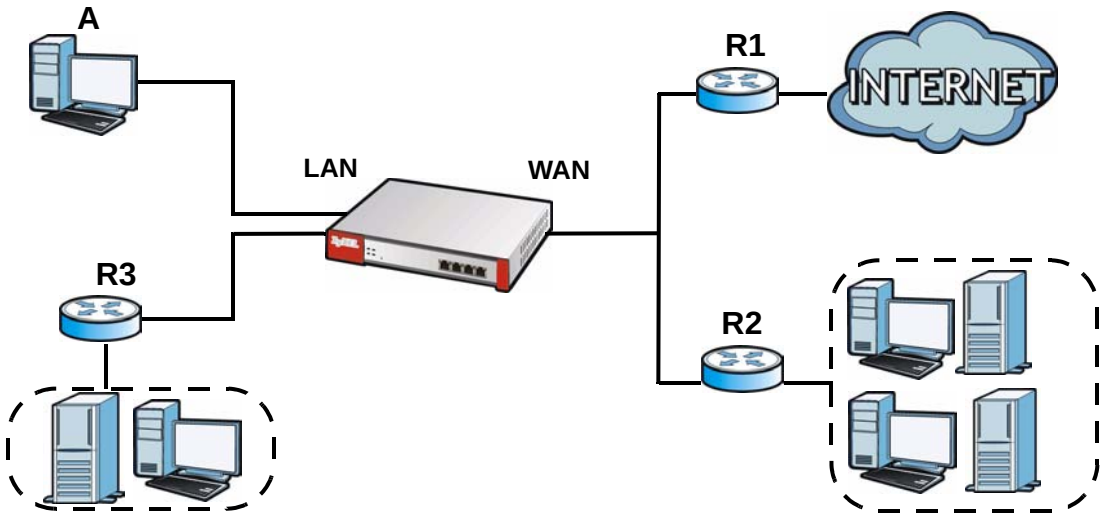
# Policy and Static Routes

## 12.1 Policy and Static Routes Overview

Use policy routes and static routes to override the ZyWALL's default routing behavior in order to send packets through the appropriate the interface or VPN tunnel.

For example, the next figure shows a computer (**A**) connected to the ZyWALL's LAN interface. The ZyWALL routes most traffic from **A** to the Internet through the ZyWALL's default gateway (**R1**). You create one policy route to connect to services offered by your ISP behind router **R2**. You create another policy route to communicate with a separate network behind another router (**R3**) connected to the LAN.

**Figure 179** Example of Policy Routing Topology




You also use policy routes to send traffic through VPN tunnels. Using the VPN wizard automatically configures a corresponding policy route, but you must manually configure a policy route if you use the main VPN screens to configure a VPN connection.

Note: You can generally just use policy routes. You only need to use static routes if you have a large network with multiple routers where you use RIP or OSPF to propagate routing information to other routers.

## 12.1.1 What You Can Do in the Routing Screens

- Use the **Policy Route** screens (see Section 12.2 on page 273) to list and configure policy routes.
- Use the **Static Route** screens (see Section 12.3 on page 279) to list and configure static routes.

## 12.1.2 What You Need to Know About Policy and Static Routes

### Policy Routing

Traditionally, routing is based on the destination address only and the ZyWALL takes the shortest path to forward a packet. IP Policy Routing (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to incoming packets on a per interface basis, prior to the normal routing.

### How You Can Use Policy Routing

- Source-Based Routing – Network administrators can use policy-based routing to direct traffic from different users through different connections.
- Bandwidth Shaping – You can allocate bandwidth to traffic that matches routing policies and prioritize traffic (however the application patrol's bandwidth management is more flexible and recommended for TCP and UDP traffic). Use policy routes to manage other types of traffic (like ICMP traffic) and send traffic through VPN tunnels.

Note: Bandwidth management in policy routes has priority over application patrol bandwidth management.

- Cost Savings – IPPR allows organizations to distribute interactive traffic on high-bandwidth, high-cost paths while using low-cost paths for batch traffic.
- Load Sharing – Network administrators can use IPPR to distribute traffic among multiple paths.
- NAT - The ZyWALL performs NAT by default for traffic going to or from the **WAN** interfaces. A routing policy's SNAT allows network administrators to have traffic received on a specified interface use a specified IP address as the source IP address.
- A NAT loopback policy route lets local users use a domain name to access a virtual server.

  When creating a virtual server that local users will use a domain name to access, you can select an option to configure a NAT loopback policy route.

### Static Routes

The ZyWALL usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the ZyWALL send data to devices not reachable through the default gateway, use static routes. Configure static routes if you need to use RIP or OSPF to propagate the routing information to other routers. See Chapter 13 on page 285 for more on RIP and OSPF.

### Policy Routes Versus Static Routes

- Policy routes are more flexible than static routes. You can select more criteria for the traffic to match and can also use schedules, NAT, and bandwidth management.
- Policy routes are only used within the ZyWALL itself. Static routes can be propagated to other routers using RIP or OSPF.
- Policy routes take priority over static routes. If you need to use a routing policy on the ZyWALL and propagate it to other routers, you could configure a policy route and an equivalent static route.

### Finding Out More

- See Section 5.4.10 on page 90 for related information on the policy route screens.
- See Section 12.4 on page 281 for more background information on policy routing.
- See Section 6.5.3 on page 126 for an example of configuring a policy route for an IPSec VPN tunnel.

## 12.2 Policy Route Screen

Click **Network > Routing** to open the **Policy Route** screen. Use this screen to see the configured policy routes and turn policy routing based bandwidth management on or off.

A policy route defines the matching criteria and the action to take when a packet meets the criteria. The action is taken only when all the criteria are met. The criteria can include the user name, source address and incoming interface, destination address, schedule, IP protocol (ICMP, UDP, TCP, etc.) and port.

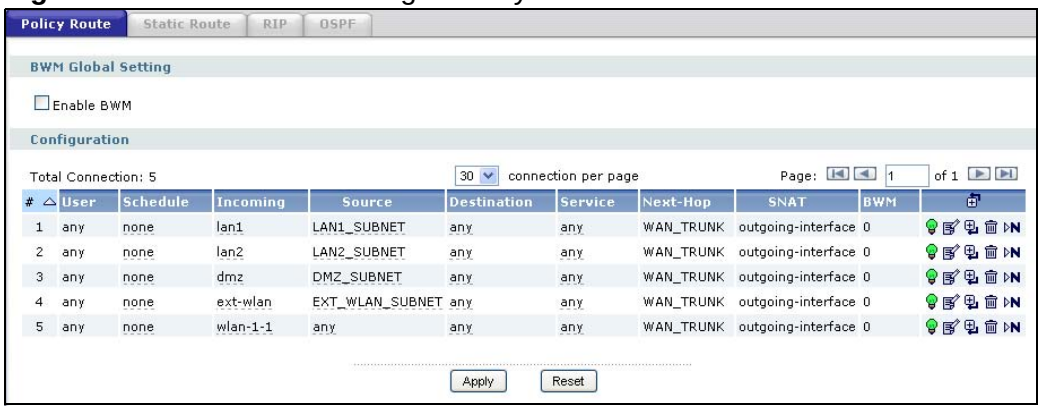
The actions that can be taken include:

- Routing the packet to a different gateway, outgoing interface, VPN tunnel, or trunk.
- Limiting the amount of bandwidth available and setting a priority for traffic.

IPPR follows the existing packet filtering facility of RAS in style and in implementation.

Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

**Figure 180** Network > Routing > Policy Route




The following table describes the labels in this screen.

**Table 87** Network > Routing > Policy Route

| LABEL | DESCRIPTION |
|---|---|
| Enable BWM | This is a global setting for enabling or disabling bandwidth management on the ZyWALL. You must enable this setting to have individual policy routes or application patrol policies apply bandwidth management.<br><br>This same setting also appears in the **AppPatrol > General** screen. Enabling or disabling it in one screen also enables or disables it in the other screen. |
| Total Connection | This field displays the total number of policy routes. |
| connection per page | Select how many entries you want to display on each page. |
| Page x of x | This is the number of the page of entries currently displayed and the total number of pages of entries. Type a page number to go to or use the arrows to navigate the pages of entries. |
| # | This is the number of an individual policy route. |
| User | This is the name of the user (group) object from which the packets are sent. **any** means all users. |
| Schedule | This is the name of the schedule object. **none** means the route is active at all times if enabled. |
| Incoming | This is the interface on which the packets are received. |
| Source | This is the name of the source IP address (group) object. **any** means all IP addresses. |
| Destination | This is the name of the destination IP address (group) object. **any** means all IP addresses. |
| Service | This is the name of the service object. **any** means all services. |

**Table 87** Network > Routing > Policy Route (continued)

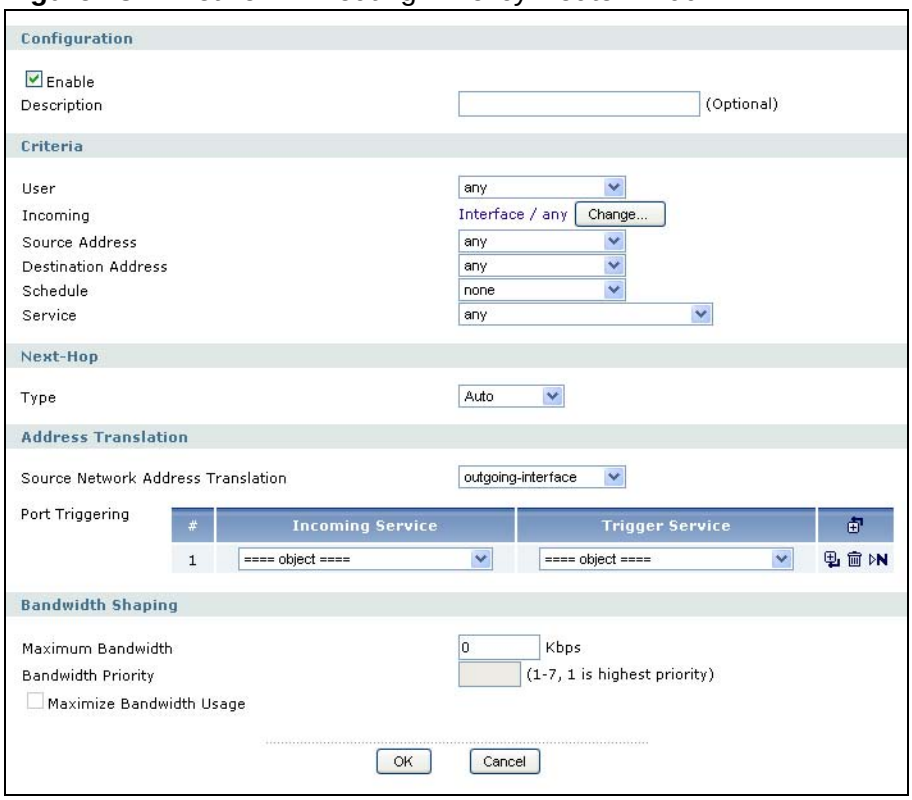
| LABEL | DESCRIPTION |
|---|---|
| Next-Hop | This is the next hop to which packets are directed. It helps forward packets to their destinations and can be a router, VPN tunnel, outgoing interface or trunk. |
| SNAT | This is the source IP address that the route uses.<br>It displays **none** if the ZyWALL does not perform NAT for this route. |
| BWM | This is the maximum bandwidth allotted to the policy. **0** means there is no bandwidth limitation for this route. |
| Add icon | Click the **Add** icon in the heading row to add a new first entry.<br>The **Active** icon displays whether the rule is enabled or not. Click the **Active** icon to activate or deactivate the policy. Make sure you click **Apply** to save and apply the change.<br>Click the **Edit** icon to go to the screen where you can edit the routing policy on the ZyWALL.<br>Click the **Add** icon in an entry to add a rule below the current entry.<br>Click the **Remove** icon to delete an existing routing policy from the ZyWALL. A window displays asking you to confirm that you want to delete the routing policy.<br>In a numbered list, click the **Move to N** icon to display a field to type a number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed.<br>The ordering of your rules is important as they are applied in order of their numbering. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 12.2.1 Policy Route Edit Screen

Click **Network > Routing** to open the **Policy Route** screen. Then click the **Add** or **Edit** icon to open the **Policy Route Edit** screen. Use this screen to configure or edit a policy route.

See NAT Loopback Example on page 318 for an example of NAT loopback.

**Figure 181** Network > Routing > Policy Route > Add




The following table describes the labels in this screen.

**Table 88** Network > Routing > Policy Route > Edit

| LABEL | DESCRIPTION |
|---|---|
| Configuration | |
| Enable | Select this to activate the policy. |
| Description | Enter a descriptive name of up to 31 printable ASCII characters for the policy. |
| Criteria | |
| User | Select a user name or user group from which the packets are sent. Select **Create Object** to configure a new user account (see Section 37.2.1 on page 652 for details). |
| Incoming Interface | Click **Change...** to select an interface or VPN tunnel through which the incoming packets are received. |
| Source Address | Select a source IP address object or select **Create Object** to configure a new one. |
| Destination Address | Select a destination IP address object or select **Create Object** to configure a new one. If the next hop is a dynamic VPN tunnel and you enable **Auto Destination Address**, the ZyWALL uses the local network of the peer router that initiated an incoming dynamic IPSec tunnel as the destination address of the policy instead of your configuration here. |

**Table 88** Network > Routing > Policy Route > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Schedule | Select a schedule or select **Create Object** to configure a new one (see Chapter 40 on page 677 for details). **none** means the route is active at all times if enabled. |
| Service | Select a service or service group from the drop-down list box. Select **Create Object** to add a new service. See Section 39.2.1 on page 674 for more information. |
| Next-Hop | |
| Type | Select **Auto** to have the ZyWALL use the routing table to find a next-hop and forward the matched packets automatically.<br><br>Select **Gateway** to route the matched packets to the next-hop router or switch you specified in the **Gateway** field. You have to set up the next-hop router or switch as a HOST address object first.<br><br>Select **VPN Tunnel** to route the matched packets via the specified VPN tunnel.<br><br>Select **Trunk** to route the matched packets through the interfaces in the trunk group based on the load balancing algorithm.<br><br>Select **Interface** to route the matched packets through the specified outgoing interface to a gateway (which is connected to the interface). |
| Gateway | This field displays when you select **Gateway** in the **Type** field. Select a HOST address object. The gateway is an immediate neighbor of your ZyWALL that will forward the packet to the destination. The gateway must be a router or switch on the same segment as your ZyWALL's interface(s). |
| VPN Tunnel | This field displays when you select **VPN Tunnel** in the **Type** field. Select a VPN tunnel through which the packets are sent to the remote network that is connected to the ZyWALL directly. |
| Auto Destination Address | This field displays when you select **VPN Tunnel** in the **Type** field. Select this to have the ZyWALL use the local network of the peer router that initiated an incoming dynamic IPSec tunnel as the destination address of the policy.<br><br>Leave this cleared if you want to manually specify the destination address. |
| Trunk | This field displays when you select **Trunk** in the **Type** field. Select a trunk group to have the ZyWALL send the packets via the interfaces in the group. |
| Interface | This field displays when you select **Interface** in the **Type** field. Select an interface to have the ZyWALL send traffic that matches the policy route through the specified interface. |
| Address Translation | Use this section to configure NAT for the policy route. This section does not apply to policy routes that use a VPN tunnel as the next hop. |

**Table 88** Network > Routing > Policy Route > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Source Network Address Translation | Select **none** to not use NAT for the route.<br><br>Select **outgoing-interface** to use the IP address of the outgoing interface as the source IP address of the packets that matches this route. If you select **outgoing-interface**, you can also configure port trigger settings for this interface.<br><br>To use SNAT for a virtual interface that is in the same WAN trunk as the physical interface to which the virtual interface is bound, the virtual interface and physical interface must be in different subnets.<br><br>Otherwise, select a pre-defined address (group) to use as the source IP address(es) of the packets that match this route.<br><br>Select **Create Object** to configure a new address (group) to use as the source IP address(es) of the packets that match this route. |
| Port Triggering | Configure trigger port forwarding to allow computers on the LAN to dynamically take turns using a service that uses a dedicated range of ports on the client side and a dedicated range of ports on the server side.<br><br>Note: You need to create a firewall rule to allow an incoming service before using a port triggering rule. |
| # | This is the rule index number. |
| Incoming Service | Select the service that the client computer sends to a remote server.<br><br>The incoming service should have the same service or protocol type as what you configured in the **Service** field. |
| Trigger Service | Select a service that a remote server sends. It causes (triggers) the ZyWALL to forward the traffic (received on the **outgoing interface**) to the client computer that requested the service. |
| Add icon | Click the **Add** icon in the heading row to add a new first entry.<br><br>Click the **Add** icon in an entry to add a rule below the current entry.<br><br>Click the **Remove** icon to delete an existing rule from the ZyWALL. A window displays asking you to confirm that you want to delete the rule.<br><br>In a numbered list, click the **Move to N** icon to display a field to type a number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed.<br><br>The ordering of your rules is important as they are applied in order of their numbering. |
| Bandwidth Shaping | This allows you to allocate bandwidth to a route and prioritize traffic that matches the routing policy.<br><br>You must also enable bandwidth management in the main policy route screen (**Network > Routing > Policy Route**) in order to apply bandwidth shaping. |

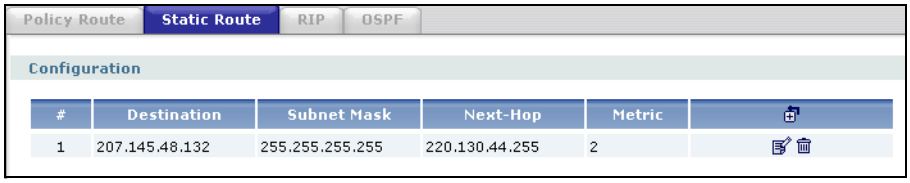
**Table 88** Network > Routing > Policy Route > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Maximum Bandwidth | Specify the maximum bandwidth (from 1 to 1048576) allowed for the route in kbps. If you enter **0** here, there is no bandwidth limitation for the route.<br><br>If the sum of the bandwidths for routes using the same next hop is higher than the actual transmission speed, lower priority traffic may not be sent if higher priority traffic uses all of the actual bandwidth.<br><br>To reserve bandwidth for traffic that does not match any of the policy routes, leave some of the interface's bandwidth unbudgeted and do not enable **Maximize Bandwidth Usage**. |
| Bandwidth Priority | Enter a number between 1 and 7 to set the priority for traffic. The smaller the number, the higher the priority. If you set the maximum bandwidth to **0**, the bandwidth priority will be changed to **0** after you click **OK**. That means the route has the highest priority and will get all the bandwidth it needs up to the maximum available.<br><br>A route with higher priority is given bandwidth before a route with lower priority.<br><br>If you set routes to have the same priority, then bandwidth is divided equally amongst those routes. |
| Maximize Bandwidth Usage | Select this check box to have the ZyWALL divide up all of the interface's unallocated and/or unused bandwidth among the policy routes that require bandwidth. Do not select this if you want to reserve bandwidth for traffic that does not match any of the policy routes. |
| OK | Click **OK** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# 12.3 IP Static Route Screen

Click **Network > Routing > Static Route** to open the **Static Route** screen. This screen displays the configured static routes. Configure static routes to be able to use RIP or OSPF to propagate the routing information to other routers.

**Figure 182** Network > Routing > Static Route



The following table describes the labels in this screen.

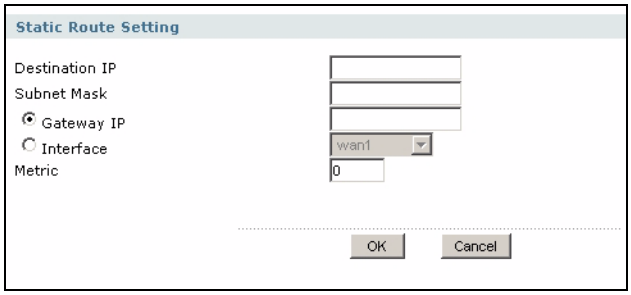
**Table 89** Network > Routing > Static Route

| LABEL | DESCRIPTION |
|---|---|
| # | This is the number of an individual static route. |
| Destination | This is the destination IP address. |
| Subnet Mask | This is the IP subnet mask. |
| Next-Hop | This is the IP address of the next-hop gateway or the interface through which the traffic is routed. The gateway is a router or switch on the same segment as your ZyWALL's interface(s). The gateway helps forward packets to their destinations. |
| Metric | This is the route's priority among the ZyWALL's routes. The smaller the number, the higher priority the route has. |
| Add icon | Click the **Add** icon to go to the screen where you can set up a static route on the ZyWALL.<br>Click the **Edit** icon to go to the screen where you can edit the static route on the ZyWALL.<br>Click the **Remove** icon to delete an existing static route from the ZyWALL. A window displays asking you to confirm that you want to delete the routing policy. |

## 12.3.1 Static Route Add/Edit Screen

Select a static route index number and click **Add** or **Edit**. The screen shown next appears. Use this screen to configure the required information for a static route.

**Figure 183** Network > Routing > Static Route > Add




The following table describes the labels in this screen.

**Table 90** Network > Routing > Static Route > Add

| LABEL | DESCRIPTION |
|---|---|
| Destination IP | This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID. |
| Subnet Mask | Enter the IP subnet mask here. |

**Table 90** Network > Routing > Static Route > Add (continued)

| LABEL | DESCRIPTION |
|---|---|
| Gateway IP | Select the radio button and enter the IP address of the next-hop gateway. The gateway is a router or switch on the same segment as your ZyWALL's interface(s). The gateway helps forward packets to their destinations. |
| Interface | Select the radio button and a predefined interface through which the traffic is sent. |
| Metric | Metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be 0~127. In practice, 2 or 3 is usually a good number. |
| OK | Click **OK** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# 12.4 Policy Routing Technical Reference

Here is more detailed information about some of the features you can configure in policy routing.

## NAT and SNAT

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address in a packet in one network to a different IP address in another network. Use SNAT (Source NAT) to change the source IP address in one network to a different IP address in another network.

## Port Triggering

Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding, you set the port(s) and IP address to forward a service (coming in from the remote server) to a client computer. The problem is that port forwarding only forwards a service to a single IP address. In order to use the same service on a different computer, you have to manually replace the client computer's IP address with another client computer's IP address.

Port triggering allows the client computer to take turns using a service dynamically. Whenever a client computer’s packets match the routing policy, it can use the pre-defined port triggering setting to connect to the remote server without manually configuring a port forwarding rule for each client computer.

Port triggering is used especially when the remote server responses using a different port from the port the client computer used to request a service. The ZyWALL records the IP address of a client computer that sends traffic to a remote server to request a service (incoming service). When the ZyWALL receives a new connection (trigger service) from the remote server, the ZyWALL forwards the traffic to the IP address of the client computer that sent the request.

In the following example, you configure two services for port triggering:

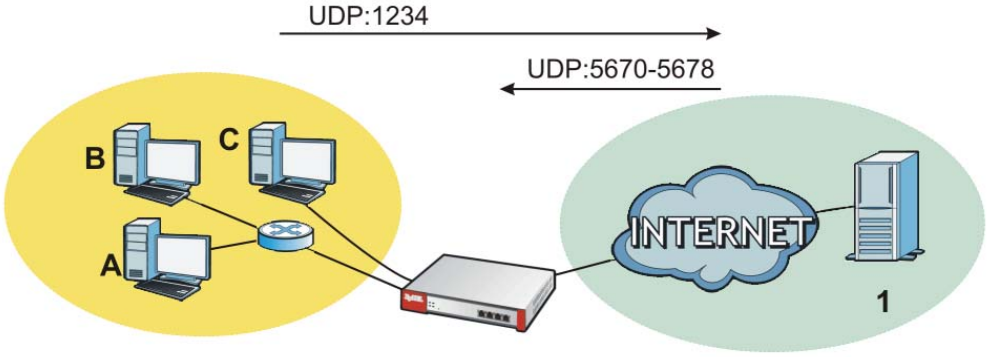
Incoming service: Game (UDP: 1234)
Trigger service: Game-1 (UDP: 5670-5678)

1 Computer **A** wants to play a multiplayer online game and tries to connect to game server **1** using port 1234. The ZyWALL records the IP address of computer **A** when the packets match a policy with SNAT configured.

2 Game server **1** responds using a port number ranging between 5670 - 5678. The ZyWALL allows and forwards the traffic to computer **A**.

3 Computer **A** and game server **1** are connected to each other until the connection is closed or times out. Any other computers (such as **B** or **C**) cannot connect to remote server **1** using the same port triggering rule as computer **A** unless they are using a different next hop (gateway, outgoing interface, VPN tunnel or trunk) from computer **A** or until the connection is closed or times out.

**Figure 184** Trigger Port Forwarding Example




## Maximize Bandwidth Usage

The maximize bandwidth usage option allows the ZyWALL to divide up any available bandwidth on the interface (including unallocated bandwidth and any allocated bandwidth that a policy route is not using) among the policy routes that require more bandwidth.

When you enable maximize bandwidth usage, the ZyWALL first makes sure that each policy route gets up to its bandwidth allotment. Next, the ZyWALL divides up

an interface's available bandwidth (bandwidth that is unbudgeted or unused by the policy routes) depending on how many policy routes require more bandwidth and on their priority levels. When only one policy route requires more bandwidth, the ZyWALL gives the extra bandwidth to that policy route.

When multiple policy routes require more bandwidth, the ZyWALL gives the highest priority policy routes the available bandwidth first (as much as they require, if there is enough available bandwidth), and then to lower priority policy routes if there is still bandwidth available. The ZyWALL distributes the available bandwidth equally among policy routes with the same priority level.

# 13

# Routing Protocols

## 13.1 Routing Protocols Overview

Routing protocols give the ZyWALL routing information about the network from other routers. The ZyWALL stores this routing information in the routing table it uses to make routing decisions. In turn, the ZyWALL can also use routing protocols to propagate routing information to other routers. See Section 5.5 on page 96 for related information on the RIP and OSPF screens.

Routing protocols are usually only used in networks using multiple routers like campuses or large enterprises.

### 13.1.1 What You Can Do in the RIP and OSPF Screens

- Use the **RIP** screen (see Section 13.2 on page 286) to configure the ZyWALL to use RIP to receive and/or send routing information.
- Use the **OSPF** screen (see Section 13.3 on page 287) to configure general OSPF settings and manage OSPF areas.
- Use the **OSPF Area Add/Edit** screen (see Section 13.3.2 on page 293) to create or edit an OSPF area.

### 13.1.2 What You Need to Know About Routing Protocols

The ZyWALL supports two standards, RIP and OSPF, for routing protocols. RIP and OSPF are compared here and discussed further in the rest of the chapter.

**Table 91** RIP vs. OSPF

| | RIP | OSPF |
|---|---|---|
| Network Size | Small (with up to 15 routers) | Large |
| Metric | Hop count | Bandwidth, hop count, throughput, round trip time and reliability. |
| Convergence | Slow | Fast |

#### Finding Out More

See Section 13.4 on page 295 for background information on routing protocols.

# 13.2 The RIP Screen

RIP (Routing Information Protocol, RFC 1058 and RFC 1389) allows a device to exchange routing information with other routers. RIP is a vector-space routing protocol, and, like most such protocols, it uses hop count to decide which route is the shortest. Unfortunately, it also broadcasts its routes asynchronously to the network and converges slowly. Therefore, RIP is more suitable for small networks (up to 15 routers).

- In the ZyWALL, you can configure two sets of RIP settings before you can use it in an interface.
- First, the **Authentication** field specifies how to verify that the routing information that is received is the same routing information that is sent. This is discussed in more detail in Authentication Types on page 295.
- Second, the ZyWALL can also **redistribute** routing information from non-RIP networks, specifically OSPF networks and static routes, to the RIP network. Costs might be calculated differently, however, so you use the **Metric** field to specify the cost in RIP terms.
- RIP uses UDP port 520.

Use the **RIP** screen to specify the authentication method and maintain the policies for redistribution.

Click **Network** > **Routing > RIP** to open the following screen.

**Figure 185** Network > Routing > RIP

The following table describes the labels in this screen.

**Table 92** Network > Routing Protocol > RIP

| LABEL | DESCRIPTION |
|---|---|
| Authentication | |
| Authentication | Select the authentication method used in the RIP network. This authentication protects the integrity, but not the confidentiality, of routing updates.<br>**None** uses no authentication.<br>**Text** uses a plain text password that is sent over the network (not very secure).<br>**MD5** uses an MD5 password and authentication ID (most secure). |
| Text Authentication Key | This field is available if the **Authentication** is **Text**. Type the password for text authentication. The key can consist of alphanumeric characters and the underscore, and it can be up to 8 characters long. |
| MD5 Authentication ID | This field is available if the **Authentication** is **MD5**. Type the ID for MD5 authentication. The ID can be between 1 and 255. |
| MD5 Authentication Key | This field is available if the **Authentication** is **MD5**. Type the password for MD5 authentication. The password can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long. |
| Redistribute | |
| Active | Select this check box to advertise routes that were learned from the indicated **Name**. |
| Name | This field displays other sources of routing information that the ZyWALL can advertise in the RIP network. |
| Metric | Type the cost for routes provided by the indicated source. The metric represents the “cost” of transmission for routing purposes. RIP routing uses hop count as the measurement of cost, with 1 usually used for directly connected networks. The number does not have to be precise, but it must be between 0 and 16. In practice, 2 or 3 is usually used. |
| Apply | Click this button to save your changes to the ZyWALL. |
| Reset | Click this button to return the screen to its last-saved settings. |

# 13.3 The OSPF Screen

OSPF (Open Shortest Path First, RFC 2328) is a link-state protocol designed to distribute routing information within a group of networks, called an Autonomous System (AS). OSPF offers some advantages over vector-space routing protocols like RIP.

- OSPF supports variable-length subnet masks, which can be set up to use available IP addresses more efficiently.

- OSPF filters and summarizes routing information, which reduces the size of routing tables throughout the network.
- OSPF responds to changes in the network, such as the loss of a router, more quickly.
- OSPF considers several factors, including bandwidth, hop count, throughput, round trip time, and reliability, when it calculates the shortest path.
- OSPF converges more quickly than RIP.

Naturally, OSPF is also more complicated than RIP, so OSPF is usually more suitable for large networks.

OSPF uses IP protocol 89.

### OSPF Areas

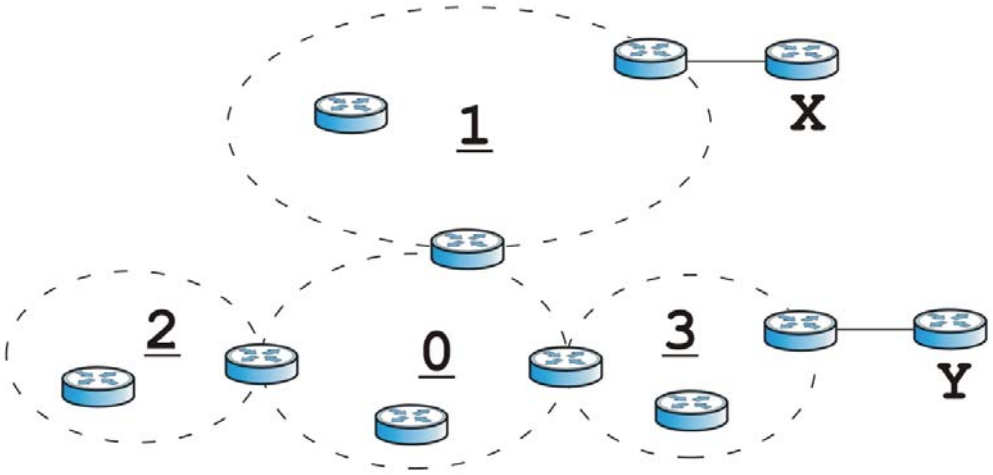
An OSPF Autonomous System (AS) is divided into one or more areas. Each area represents a group of adjacent networks and is identified by a 32-bit ID. In OSPF, this number may be expressed as an integer or as an IP address.

There are several types of areas.

- The backbone is the transit area that routes packets between other areas. All other areas are connected to the backbone.
- A normal area is a group of adjacent networks. A normal area has routing information about the OSPF AS, any networks outside the OSPF AS to which it is directly connected, and any networks outside the OSPF AS that provide routing information to any area in the OSPF AS.
- A stub area has routing information about the OSPF AS. It does not have any routing information about any networks outside the OSPF AS, including networks to which it is directly connected. It relies on a default route to send information outside the OSPF AS.
- A Not So Stubby Area (NSSA, RFC 1587) has routing information about the OSPF AS and networks outside the OSPF AS to which the NSSA is directly connected. It does not have any routing information about other networks outside the OSPF AS.

Each type of area is illustrated in the following figure.

**Figure 186** OSPF: Types of Areas




This OSPF AS consists of four areas, areas 0-3. Area 0 is always the backbone. In this example, areas 1, 2, and 3 are all connected to it. Area 1 is a normal area. It has routing information about the OSPF AS and networks X and Y. Area 2 is a stub area. It has routing information about the OSPF AS, but it depends on a default route to send information to networks X and Y. Area 3 is a NSSA. It has routing information about the OSPF AS and network Y but not about network X.

### OSPF Routers

Every router in the same area has the same routing information. They do this by exchanging Hello messages to confirm which neighbor (layer-3) devices exist, and then they exchange database descriptions (DDs) to create a synchronized link-state database. The link-state database contains records of router IDs, their associated links and path costs. The link-state database is then constantly updated through Link State Advertisements (LSA). Each router uses the link state database and the Dijkstra algorithm to compute the least cost paths to network destinations.

Like areas, each router has a unique 32-bit ID in the OSPF AS, and there are several types of routers. Each type is really just a different role, and it is possible for one router to play multiple roles at one time.

- An internal router (IR) only exchanges routing information with other routers in the same area.
- An Area Border Router (ABR) connects two or more areas. It is a member of all the areas to which it is connected, and it filters, summarizes, and exchanges routing information between them.

- An Autonomous System Boundary Router (ASBR) exchanges routing information with routers in networks outside the OSPF AS. This is called redistribution in OSPF.

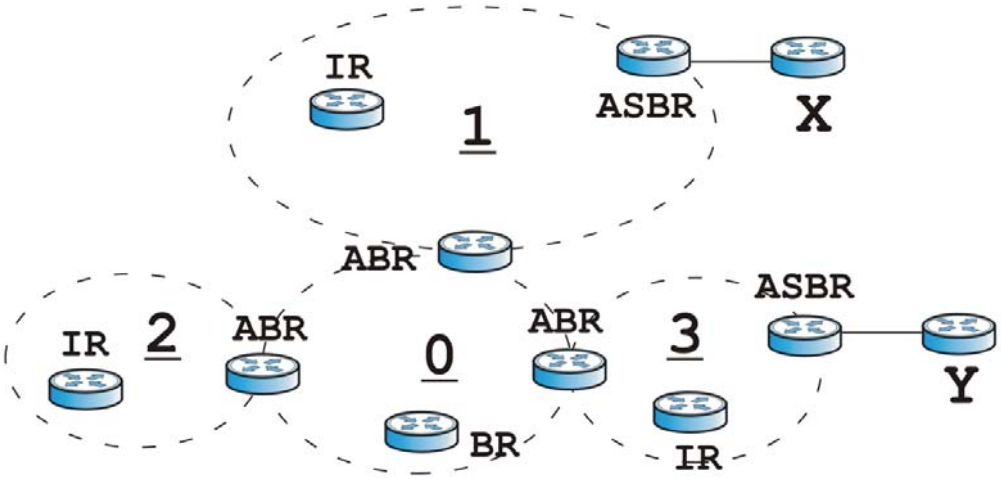
**Table 93** OSPF: Redistribution from Other Sources to Each Type of Area

| SOURCE \ TYPE OF AREA | NORMAL | NSSA | STUB |
|---|---|---|---|
| Static routes | Yes | Yes | No |
| RIP | Yes | Yes | Yes |

- A backbone router (BR) has at least one interface with area 0. By default, every router in area 0 is a backbone router, and so is every ABR.

Each type of router is illustrated in the following example.

**Figure 187** OSPF: Types of Routers




In order to reduce the amount of traffic between routers, a group of routers that are directly connected to each other selects a designated router (DR) and a backup designated router (BDR). All of the routers only exchange information with the DR and the BDR, instead of exchanging information with all of the other routers in the group. The DR and BDR are selected by priority; if two routers have the same priority, the highest router ID is used.

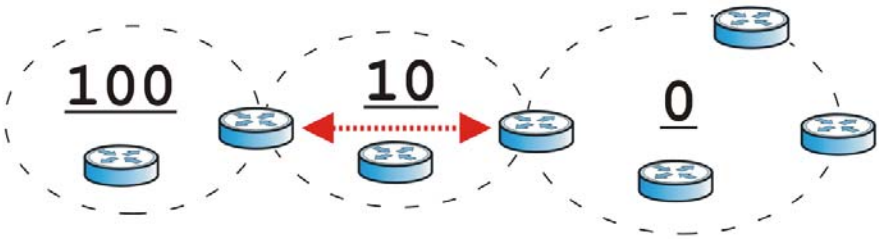
The DR and BDR are selected in each group of routers that are directly connected to each other. If a router is directly connected to several groups, it might be a DR in one group, a BDR in another group, and neither in a third group all at the same time.

### Virtual Links

In some OSPF AS, it is not possible for an area to be directly connected to the backbone. In this case, you can create a virtual link through an intermediate area

to logically connect the area to the backbone. This is illustrated in the following example.

**Figure 188** OSPF: Virtual Link




In this example, area 100 does not have a direct connection to the backbone. As a result, you should set up a virtual link on both ABR in area 10. The virtual link becomes the connection between area 100 and the backbone.

You cannot create a virtual link to a router in a different area.

### OSPF Configuration

Follow these steps when you configure OSPF on the ZyWALL.

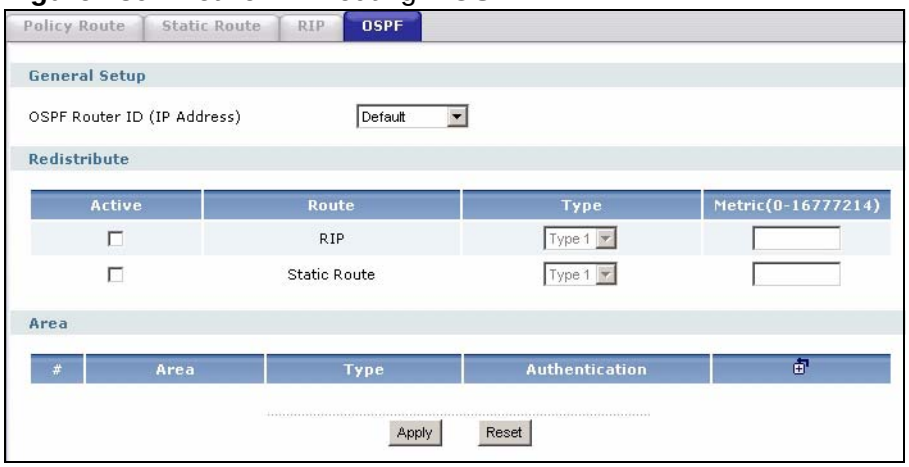
1. Enable OSPF.
2. Set up the OSPF areas.
3. Configure the appropriate interfaces. See Section 10.4.1 on page 191.
4. Set up virtual links, as needed.

## 13.3.1 Configuring the OSPF Screen

Use the first OSPF screen to specify the OSPF router the ZyWALL uses in the OSPF AS and maintain the policies for redistribution. In addition, it provides a summary of OSPF areas, allows you to remove them, and opens the **OSPF Add / Edit** screen to add or edit them.

Click **Network** > **Routing > OSPF** to open the following screen.

**Figure 189** Network > Routing > OSPF




The following table describes the labels in this screen. See Section 13.3.2 on page 293 for more information as well.

**Table 94** Network > Routing Protocol > OSPF

| LABEL | DESCRIPTION |
|---|---|
| OSPF Router ID | Select the 32-bit ID the ZyWALL uses in the OSPF AS.<br>**Default** - the highest available IP address assigned to the interfaces is the ZyWALL's ID.<br>**User Define** - enter the ID (in IP address format) in the field that appears when you select **User Define**. |
| Redistribute | |
| Active | Select this check box to advertise routes that were learned from the indicated source.<br>• If you select this for RIP, the ZyWALL advertises routes learned from RIP to **Normal** and **NSSA** areas but not to **Stub** areas.<br>• If you select this for static routes, the ZyWALL advertises routes learned from static routes to all types of areas. |
| Route | This field displays other sources of routing information that the ZyWALL can advertise in the OSPF AS. |
| Type | Select how OSPF calculates the cost associated with routing information from the indicated source. Choices are: **Type 1** and **Type 2**.<br>**Type 1** - cost = OSPF AS cost + external cost (**Metric**)<br>**Type 2** - cost = external cost (**Metric**); the OSPF AS cost is ignored. |
| Metric | Type the external cost for routes provided by the indicated source. The metric represents the "cost" of transmission for routing purposes. The way this is used depends on the **Type** field. This value is usually the average cost in the OSPF AS, and it can be between 1 and 16777214. |
| Area | This section displays information about OSPF areas in the ZyWALL. |

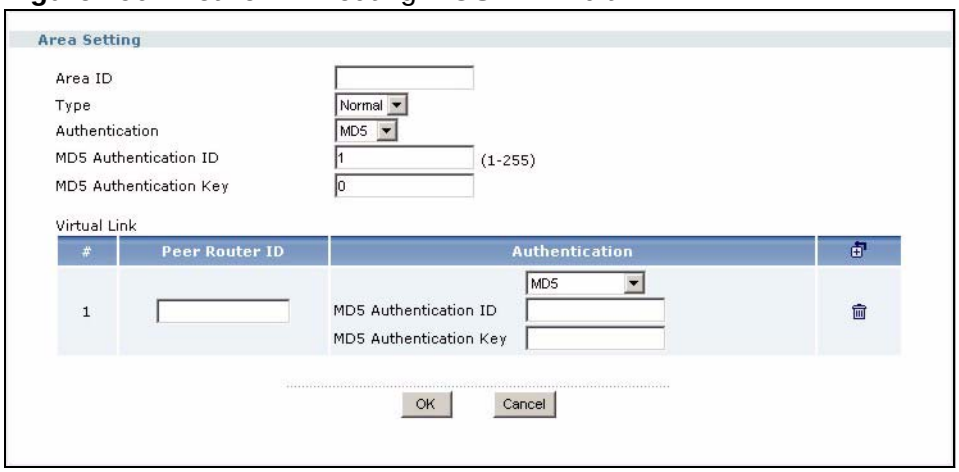
**Table 94** Network > Routing Protocol > OSPF (continued)

| LABEL | DESCRIPTION |
|---|---|
| # | This field is a sequential value, and it is not associated with a specific area. |
| Area | This field displays the 32-bit ID for each area in IP address format. |
| Type | This field displays the type of area. This type is different from the **Type** field above. |
| Authentication | This field displays the default authentication method in the area. |
| Add icon | This column provides icons to add, edit, and remove areas.<br><br>To add an area, click the **Add** icon at the top of the column. The **OSPF Area Add / Edit** screen appears.<br><br>To edit an area, click the **Edit** icon next to the area. The **Area Add / Edit** screen appears.<br><br>To delete an area, click on the **Remove** icon next to the area. The Web Configurator confirms that you want to delete the area before doing so. |
| Apply | Click this button to save your changes to the ZyWALL. |
| Reset | Click this button to return the screen to its last-saved settings. |

## 13.3.2 OSPF Area Add/Edit Screen

The **OSPF Area Add / Edit** screen allows you to create a new area or edit an existing one. To access this screen, go to the **OSPF** summary screen (see Section 13.3 on page 287), and click either the **Add** icon or an **Edit** icon.

**Figure 190** Network > Routing > OSPF > Edit



The following table describes the labels in this screen.

**Table 95** Network > Routing > OSPF > Edit

| LABEL | DESCRIPTION |
|---|---|
| Area ID | Type the unique, 32-bit identifier for the area in IP address format. |
| Type | Select the type of area.<br><br>**Normal** - This area is a normal area. It has routing information about the OSPF AS and about networks outside the OSPF AS.<br><br>**Stub** - This area is an stub area. It has routing information about the OSPF AS but not about networks outside the OSPF AS. It depends on a default route to send information outside the OSPF AS.<br><br>**NSSA** - This area is a Not So Stubby Area (NSSA), per RFC 1587. It has routing information about the OSPF AS and networks that are outside the OSPF AS and are directly connected to the NSSA. It does not have information about other networks outside the OSPF AS. |
| Authentication | Select the default authentication method used in the area. This authentication protects the integrity, but not the confidentiality, of routing updates.<br><br>**None** uses no authentication.<br><br>**Text** uses a plain text password that is sent over the network (not very secure).<br><br>**MD5** uses an MD5 password and authentication ID (most secure). |
| Text Authentication Key | This field is available if the **Authentication** is **Text**. Type the password for text authentication. The key can consist of alphanumeric characters and the underscore, and it can be up to 8 characters long. |
| MD5 Authentication ID | This field is available if the **Authentication** is **MD5**. Type the default ID for MD5 authentication in the area. The ID can be between 1 and 255. |
| MD5 Authentication Key | This field is available if the **Authentication** is **MD5**. Type the default password for MD5 authentication in the area. The password can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long. |
| Virtual Link | This section is displayed if the **Type** is **Normal**. Create a virtual link if you want to connect a different area (that does not have a direct connection to the backbone) to the backbone. You should set up the virtual link on the ABR that is connected to the other area and on the ABR that is connected to the backbone. |
| # | This field is a sequential value, and it is not associated with a specific area. |
| Peer Router ID | Type the 32-bit ID (in IP address format) of the other ABR in the virtual link. |

**Table 95** Network > Routing > OSPF > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Authentication | Select which authentication method to use in the virtual link. This authentication protects the integrity, but not the confidentiality, of routing updates.<br><br>**None** uses no authentication.<br><br>**Text** uses a plain text password that is sent over the network (not very secure).<br><br>**MD5** uses an MD5 password and authentication ID (most secure).<br><br>**Same as Area** has the virtual link also use the **Authentication** settings above. |
| Text Authentication Key | This field is available if the **Authentication** is **Text**. Type the password for text authentication. The key can consist of alphanumeric characters and the underscore, and it can be up to 8 characters long. |
| MD5 Authentication ID | This field is available if the **Authentication** is **MD5**. Type the default ID for MD5 authentication in the area. The ID can be between 1 and 255. |
| MD5 Authentication Key | This field is available if the **Authentication** is **MD5**. Type the default password for MD5 authentication in the area. The password can consist of alphanumeric characters and the underscore, and it can be up to 16 characters long. |
| Add icon | This column provides icons to add and remove virtual links.<br><br>To add a virtual link, click the **Add** icon at the top of the column. A new record appears in the virtual link list.<br><br>To delete a virtual link, click on the **Remove** icon next to the virtual link. The Web Configurator confirms that you want to delete the virtual link. |
| OK | Click **OK** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# 13.4 Routing Protocol Technical Reference

Here is more detailed information about RIP and OSPF.

### Authentication Types

Authentication is used to guarantee the integrity, but not the confidentiality, of routing updates. The transmitting router uses its key to encrypt the original message into a smaller message, and the smaller message is transmitted with the original message. The receiving router uses its key to encrypt the received message and then verifies that it matches the smaller message sent with it. If the received message is verified, then the receiving router accepts the updated

routing information. The transmitting and receiving routers must have the same key.

The ZyWALL supports three types of authentication for RIP and OSPF routing protocols:

- **None** - no authentication is used.
- **Text** – authentication using a plain text password, and the (unencrypted) password is sent over the network. This method is usually used temporarily to prevent network problems.
- **MD5** – authentication using an MD5 password and authentication ID.

MD5 is an authentication method that produces a 128-bit checksum, called a message-digest, for each packet. It also includes an authentication ID, which can be set to any value between 1 and 255. The ZyWALL only accepts packets if these conditions are satisfied.

- The packet's authentication ID is the same as the authentication ID of the interface that received it.
- The packet's message-digest is the same as the one the ZyWALL calculates using the MD5 password.

For RIP, authentication is not available in RIP version 1. In RIP version 2, you can only select one authentication type for all interfaces. For OSPF, the ZyWALL supports a default authentication type by area. If you want to use this default in an interface or virtual link, you set the associated **Authentication Type** field to **Same as Area**. As a result, you only have to update the authentication information for the area to update the authentication type used by these interfaces and virtual links. Alternatively, you can override the default in any interface or virtual link by selecting a specific authentication method. Please see the respective interface sections for more information.

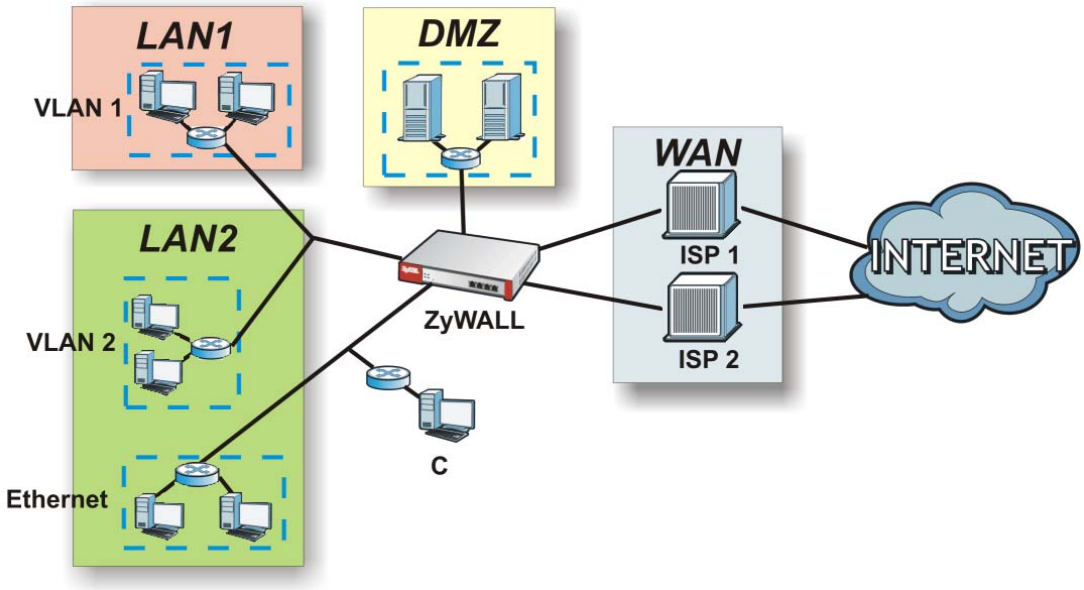
# 14 Zones

## 14.1 Zones Overview

Set up zones to configure network security and network policies in the ZyWALL. A zone is a group of interfaces or VPN tunnels. The ZyWALL uses zones instead of interfaces in many security and policy settings, such as firewall rules and remote management.

Zones cannot overlap. Each Ethernet interface, VLAN interface, bridge interface, PPPoE/PPTP interface, auxiliary interface, and VPN tunnel can be assigned to at most one zone. Virtual interfaces are automatically assigned to the same zone as the interface on which they run.

**Figure 191** Example: Zones




### 14.1.1 What You Can Do in the Zones Screens

Use the **Zone** screens (see Section 14.2 on page 299) to view and edit the ZyWALL's zones.

## 14.1.2 What You Need to Know About Zones

### Effects of Zones on Different Types of Traffic

Zones effectively divide traffic into three types--intra-zone traffic, inter-zone traffic, and extra-zone traffic--which are affected differently by zone-based security and policy settings.

### Intra-zone Traffic

- Intra-zone traffic is traffic between interfaces or VPN tunnels in the same zone. For example, in Figure 191 on page 297, traffic between VLAN 2 and the Ethernet is intra-zone traffic.
- In each zone, you can either allow or prohibit all intra-zone traffic. For example, in Figure 191 on page 297, you might allow intra-zone traffic in the LAN zone but prohibit it in the WAN zone.
- You can also set up firewall rules to control intra-zone traffic (for example, DMZ-to-DMZ), but many other types of zone-based security and policy settings do not affect intra-zone traffic.

### Inter-zone Traffic

Inter-zone traffic is traffic between interfaces or VPN tunnels in different zones. For example, in Figure 191 on page 297, traffic between VLAN 1 and the Internet is inter-zone traffic. This is the normal case when zone-based security and policy settings apply.

### Extra-zone Traffic

- Extra-zone traffic is traffic to or from any interface or VPN tunnel that is not assigned to a zone. For example, in Figure 191 on page 297, traffic to or from computer **C** is extra-zone traffic.
- Some zone-based security and policy settings may apply to extra-zone traffic, especially if you can set the zone attribute in them to **Any** or **All**. See the specific feature for more information.

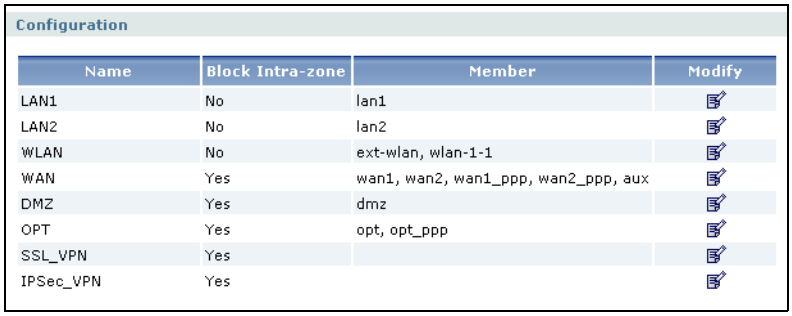
### Finding Out More

See Section 5.4.7 on page 89 for related information on these screens.

# 14.2 The Zone Screen

The **Zone** screen provides a summary of all zones. In addition, this screen allows you to edit zones. To access this screen, click **Network** > **Zone**.

**Figure 192** Network > Zone




The following table describes the labels in this screen.

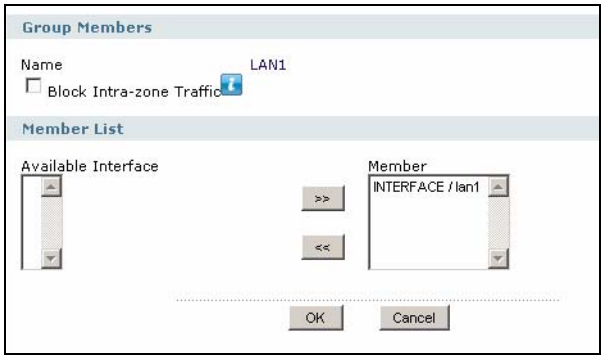
**Table 96** Network > Zone

| LABEL | DESCRIPTION |
|---|---|
| Name | This field displays the name of the zone. |
| Block Intra-zone | This field indicates whether or not the ZyWALL blocks network traffic between members in the zone. |
| Member | This field displays the names of the interfaces that belong to each zone. |
| Add icon | This column provides icons to edit zones.<br><br>To edit a zone, click the **Edit** icon next to the zone. The **Zone Edit** screen appears. |

# 14.3 Zone Edit

The **Zone Edit** screen allows you to edit a zone. To access this screen, go to the **Zone** screen (see Section 14.2 on page 299), and click an **Edit** icon.

**Figure 193** Network > Zone > Edit




The following table describes the labels in this screen.

**Table 97** Network > Zone > Edit

| LABEL | DESCRIPTION |
|---|---|
| Name | This is the name of the zone. |
| Block Intra-zone Traffic | Select this check box to block network traffic between members in the zone. |
| Member List | **Available** lists the interfaces and VPN tunnels that do not belong to any zone. The word in front of the name indicates whether this member is an interface or a VPN tunnel.<br><br>**INTERFACE** - this member is an interface.<br><br>**IPSEC** - this member is a VPN tunnel.<br><br>Select the interfaces and VPN tunnels that you want to add to the zone you are editing, and click the right arrow button to add them.<br><br>**Member** lists the interfaces and VPN tunnels that belong to the zone. Select any interfaces that you want to remove from the zone, and click the left arrow button to remove them. |

# 15

# DDNS

## 15.1 DDNS Overview

Dynamic DNS (DDNS) services let you use a domain name with a dynamic IP address.

### 15.1.1 What You Can Do in the DDNS Screens

- Use the **DDNS** screen (see Section 15.2 on page 302) to view a list of the configured DDNS domain names and their details.
- Use the **DDNS Add/Edit** screen (see Section 15.2.1 on page 304) to add a domain name to the ZyWALL or to edit the configuration of an existing domain name.
- Use the **DDNS Status** screen (see Section 15.3 on page 306) to view the status of the ZyWALL's DDNS domain names.

### 15.1.2 What You Need to Know About DDNS

DNS maps a domain name to a corresponding IP address and vice versa. Similarly, dynamic DNS maps a domain name to a dynamic IP address. As a result, anyone can use the domain name to contact you (in NetMeeting, CU-SeeMe, etc.) or to access your FTP server or Web site, regardless of the current IP address.

Note: You must have a public WAN IP address to use Dynamic DNS.

You must set up a dynamic DNS account with a supported DNS service provider before you can use Dynamic DNS services with the ZyWALL. When registration is complete, the DNS service provider gives you a password or key. At the time of writing, the ZyWALL supports the following DNS service providers. See the listed websites for details about the DNS services offered by each.

**Table 98** DDNS Service Providers

| PROVIDER | SERVICE TYPES SUPPORTED | WEBSITE |
|---|---|---|
| DynDNS | Dynamic DNS, Static DNS, and Custom DNS | www.dyndns.com |
| Dynu | Basic, Premium | www.dynu.com |

**Table 98** DDNS Service Providers (continued)

| PROVIDER | SERVICE TYPES SUPPORTED | WEBSITE |
|---|---|---|
| No-IP | No-IP | www.no-ip.com |
| Peanut Hull | Peanut Hull | www.oray.cn |
| 3322 | 3322 Dynamic DNS, 3322 Static DNS | www.3322.org |

Note: Record your DDNS account's user name, password, and domain name to use to configure the ZyWALL.

After, you configure the ZyWALL, it automatically sends updated IP addresses to the DDNS service provider, which helps redirect traffic accordingly.

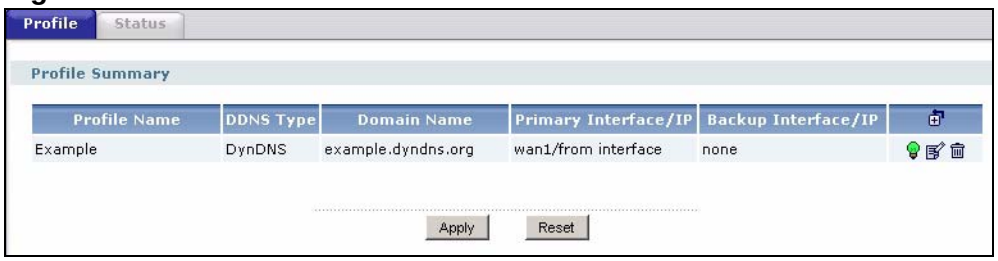
### Finding Out More

See Section 5.4.9 on page 89 for related information on these screens.

## 15.2 The DDNS Screen

The **DDNS** screen provides a summary of all DDNS domain names and their configuration. In addition, this screen allows you to add new domain names, edit the configuration for existing domain names, and delete domain names. Click **Network** > **DDNS** to open the following screen.

**Figure 194** Network > DDNS




The following table describes the labels in this screen.

**Table 99** Network > DDNS

| LABEL | DESCRIPTION |
|---|---|
| Profile Name | This field displays the descriptive profile name for this entry. |
| DDNS Type | This field displays which DDNS service you are using. |
| Domain Name | This field displays each domain name the ZyWALL can route. |

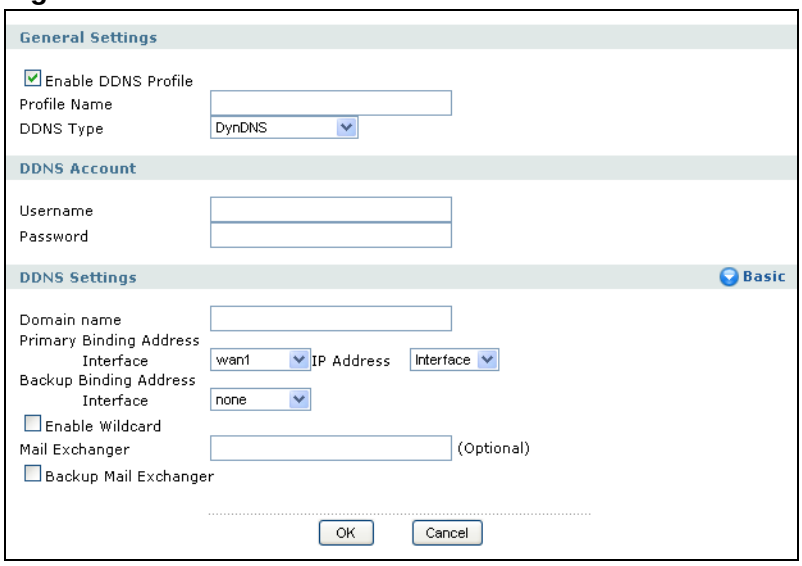
**Table 99** Network > DDNS (continued)

| LABEL | DESCRIPTION |
|---|---|
| Primary Interface/IP | This field displays the interface to use for updating the IP address mapped to the domain name followed by how the ZyWALL determines the IP address for the domain name.<br><br>**from interface** - The IP address comes from the specified interface.<br><br>**auto detected** -The DDNS server checks the source IP address of the packets from the ZyWALL for the IP address to use for the domain name.<br><br>**custom** - The IP address is static. |
| Backup Interface/IP | This field displays the alternate interface to use for updating the IP address mapped to the domain name followed by how the ZyWALL determines the IP address for the domain name. The ZyWALL uses the backup interface and IP address when the primary interface is disabled, its link is down or its connectivity check fails.<br><br>**from interface** - The IP address comes from the specified interface.<br><br>**auto detected** -The DDNS server checks the source IP address of the packets from the ZyWALL for the IP address to use for the domain name.<br><br>**custom** - The IP address is static. |
| Add icon | This column provides icons to add, edit, and remove domain names.<br><br>To add a domain name, click the **Add** icon at the top of the column. The **DDNS Add/Edit** screen appears.<br><br>To activate or deactivate a domain name entry, click the entry's **Active** icon. Make sure you click **Apply** to save and apply the change.<br><br>To edit a domain name, click the **Edit** icon next to the domain name. The **DDNS Add/Edit** screen appears.<br><br>To delete a domain name, click on the **Remove** icon next to the ISP account. The Web Configurator confirms that you want to delete the account before doing so. |
| Apply | Click this button to save your changes to the ZyWALL. |
| Reset | Click this button to return the screen to its last-saved settings. |

## 15.2.1 The Dynamic DNS Add/Edit Screen

The **DDNS Add/Edit** screen allows you to add a domain name to the ZyWALL or to edit the configuration of an existing domain name. Click **Network** > **DDNS** and then an **Add** or **Edit** icon to open this screen.

**Figure 195** Network > DDNS > Add




The following table describes the labels in this screen.

**Table 100** Network > DDNS > Add

| LABEL | DESCRIPTION |
|---|---|
| Enable DDNS Profile | Select this check box to use this DDNS entry. |
| Profile Name | When you are adding a DDNS entry, type a descriptive name for this DDNS entry in the ZyWALL. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.<br><br>This field is read-only when you are editing an entry. |
| DDNS Type | Select the type of DDNS service you are using. |
| Username | Type the user name used when you registered your domain name. You can use up to 31 alphanumeric characters and the underscore. Spaces are not allowed.<br><br>For a Dynu DDNS entry, this user name is the one you use for logging into the service, not the name recorded in your personal information in the Dynu website. |
| Password | Type the password provided by the DDNS provider. You can use up to 64 alphanumeric characters and the underscore. Spaces are not allowed. |
| DDNS Settings | Click **Advanced** to display more settings. Click **Basic** to display fewer settings. |
| Domain name | Type the domain name you registered. You can use up to 255 characters. |

**Table 100** Network > DDNS > Add (continued)

| LABEL | DESCRIPTION |
|---|---|
| Primary Binding Address | Use these fields to set how the ZyWALL determines the IP address that is mapped to your domain name in the DDNS server. The ZyWALL uses the **Backup Binding Address** if the interface specified by these settings is not available. |
| Interface | Select the interface to use for updating the IP address mapped to the domain name. Select **Any** to let the domain name be used with any interface. |
| IP Address | The options available in this field vary by DDNS provider.<br><br>**Interface** -The ZyWALL uses the IP address of the specified interface. This option appears when you select a specific interface in the **Primary Binding Address Interface** field.<br><br>**Auto** - If the interface has a dynamic IP address, the DDNS server checks the source IP address of the packets from the ZyWALL for the IP address to use for the domain name. You may want to use this if there are one or more NAT routers between the ZyWALL and the DDNS server.<br><br>Note: The ZyWALL may not determine the proper IP address if there is an HTTP proxy server between the ZyWALL and the DDNS server.<br><br>**Custom** - If you have a static IP address, you can select this to use it for the domain name. The ZyWALL still sends the static IP address to the DDNS server. |
| Custom IP | This field is only available when the **IP Address** is **Custom**. Type the IP address to use for the domain name. |
| Backup Binding Address | Use these fields to set an alternate interface to map the domain name to when the interface specified by the **Primary Binding Interface** settings is not available. |
| Interface | Select the interface to use for updating the IP address mapped to the domain name. Select **Any** to let the domain name be used with any interface. Select **None** to not use a backup address. |
| IP Address | The options available in this field vary by DDNS provider.<br><br>**Interface** -The ZyWALL uses the IP address of the specified interface. This option appears when you select a specific interface in the **Backup Binding Address Interface** field.<br><br>**Auto** -The DDNS server checks the source IP address of the packets from the ZyWALL for the IP address to use for the domain name. You may want to use this if there are one or more NAT routers between the ZyWALL and the DDNS server.<br><br>Note: The ZyWALL may not determine the proper IP address if there is an HTTP proxy server between the ZyWALL and the DDNS server.<br><br>**Custom** - If you have a static IP address, you can select this to use it for the domain name. The ZyWALL still sends the static IP address to the DDNS server. |

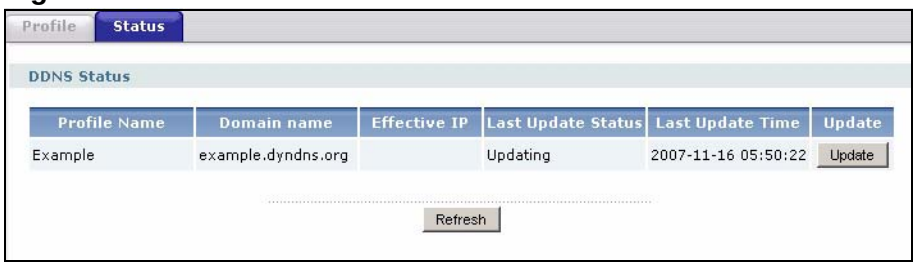
**Table 100** Network > DDNS > Add (continued)

| LABEL | DESCRIPTION |
|---|---|
| Custom IP | This field is only available when the **IP Address** is **Custom**. Type the IP address to use for the domain name. |
| Enable Wildcard | This option is only available with a DynDNS account.<br>Enable the wildcard feature to alias subdomains to be aliased to the same IP address as your (dynamic) domain name. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname. |
| Mail Exchanger | This option is only available with a DynDNS account.<br>DynDNS can route e-mail for your domain name to a mail server (called a mail exchanger). For example, DynDNS routes e-mail for john-doe@yourhost.dyndns.org to the host record specified as the mail exchanger.<br>If you are using this service, type the host record of your mail server here. Otherwise leave the field blank.<br>See www.dyndns.org for more information about mail exchangers. |
| Backup Mail Exchanger | This option is only available with a DynDNS account.<br>Select this check box if you are using DynDNS's backup service for e-mail. With this service, DynDNS holds onto your e-mail if your mail server is not available. Once your mail server is available again, the DynDNS server delivers the mail to you. See www.dyndns.org for more information about this service. |
| OK | Click **OK** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# 15.3 The DDNS Status Screen

The **DDNS Status** screen shows the status of the ZyWALL's DDNS domain names. Click **Network** > **DDNS > Status** to open the following screen.

**Figure 196** Network > DDNS > Status



The following table describes the labels in this screen.

**Table 101** Network > DDNS > Status

| LABEL | DESCRIPTION |
|---|---|
| Profile Name | This field displays the descriptive profile name for this entry. |
| Domain Name | This field displays each domain name the ZyWALL can route. |
| Effective IP | This is the (resolved) IP address of the domain name. |
| Last Update Status | This shows whether the last attempt to resolve the IP address for the domain name was successful or not. **Updating** means the ZyWALL is currently attempting to resolve the IP address for the domain name. |
| Last Update Time | This shows when the last attempt to resolve the IP address for the domain name occurred (in year-month-day hour:minute:second format). |
| Update | Click this to have the ZyWALL update the profile to the DDNS server. The ZyWALL attempts to resolve the IP address for the domain name. |
| Refresh | Click this to update the information displayed in the screen. |

# 16

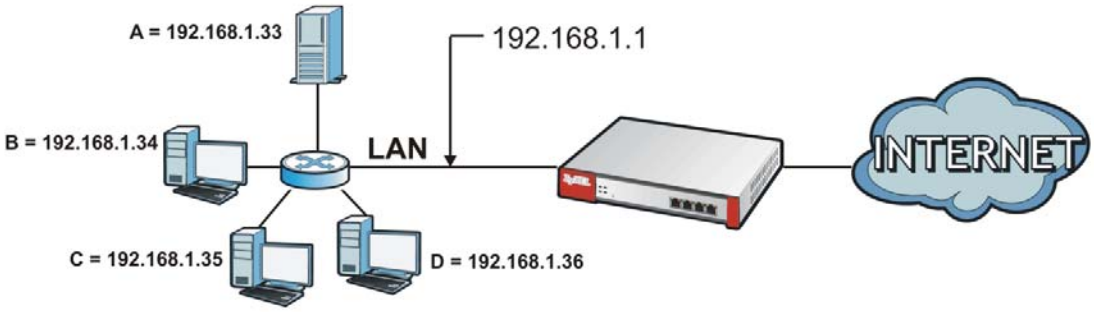
# Virtual Servers

## 16.1 Virtual Servers Overview

Virtual servers are computers on a private network behind the ZyWALL that you make available outside the private network. If the ZyWALL has only one public IP address, you can make the computers in the private network available by using ports to forward packets to the appropriate private IP address.

Suppose you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a third (**C** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

**Figure 197** Multiple Servers Behind NAT Example




### 16.1.1 What You Can Do in the Virtual Server Screens

Use the **Virtual Server** screens (see Section 16.2 on page 310) to view and manage the list of virtual servers and see their configuration details. You can also create new virtual servers and edit or delete existing ones.

### 16.1.2 What You Need to Know About Virtual Servers

Virtual server is also known as port forwarding or port translation.

Note: The virtual server changes the destination address of packets. This is also known as Destination NAT (DNAT).

### Finding Out More

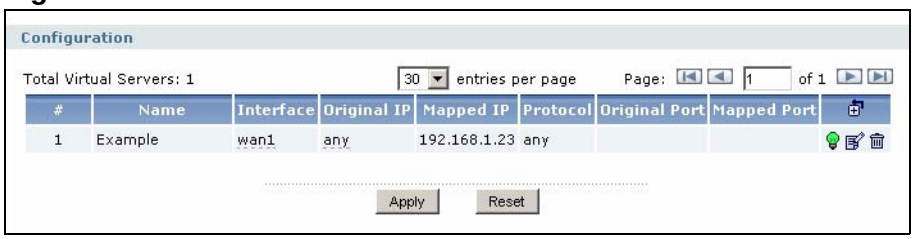
- See Section 5.4.19 on page 94 for related information on these screens.
- See Section 6.8.2 on page 138 for an example of how to configure a virtual server to allow H.323 traffic from the WAN to the LAN.
- See Section 16.3 on page 314 for examples of manually configuring NAT 1:1 mapping and manually configuring a policy route rule for NAT loopback. (Although you can have the ZyWALL automatically configure these for you instead.)

## 16.2 The Virtual Server Screen

The **Virtual Server** summary screen provides a summary of all virtual servers and their configuration. In addition, this screen allows you to create new virtual servers and edit and delete existing virtual servers. To access this screen, login to the Web Configurator and click **Network** > **Virtual Server**. The following screen appears, providing a summary of the existing virtual servers.

Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

**Figure 198** Network > Virtual Server




The following table describes the labels in this screen.

**Table 102** Network > Virtual Server

| LABEL | DESCRIPTION |
|---|---|
| Total Virtual Servers | This is how many virtual server entries are configured in the ZyWALL. |
| entries per page | Select how many virtual server entries to display per page in the screen. |
| Page x of x | This is the number of the page of entries currently displayed and the total number of pages of entries. Type a page number to go to or use the arrows to navigate the pages of entries. |
| # | This field is a sequential value, and it is not associated with a specific virtual server. |
| Name | This field displays the name of the virtual server. |
| Interface | This field displays the interface on which packets for the virtual server were received. |

**Table 102** Network > Virtual Server (continued)

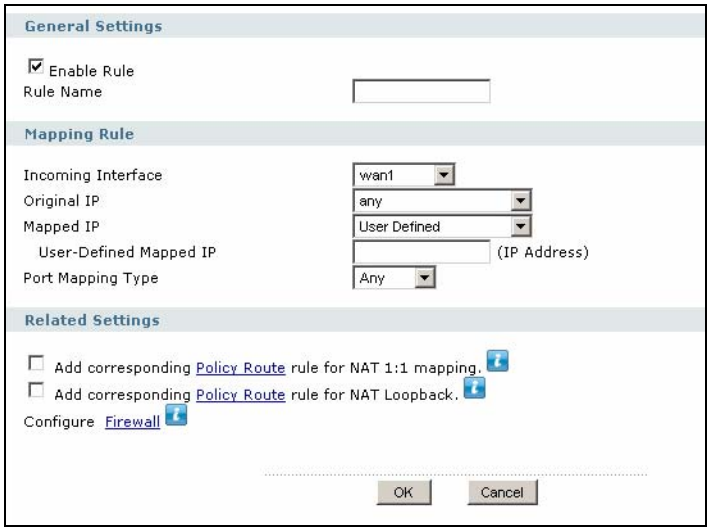
| LABEL | DESCRIPTION |
|---|---|
| Original IP | This field displays the original destination IP address (or address object) of packets for the virtual server. It displays **any** if there is no restriction on the original destination IP address. |
| Mapped IP | This field displays the new destination IP address for the packet. |
| Protocol | This field displays the service used by the packets for this virtual server. It displays **any** if there is no restriction on the services. |
| Original Port | This field displays the original destination port(s) of packets for the virtual server. This field is blank if there is no restriction on the original destination port. |
| Mapped Port | This field displays the new destination port(s) for the packet. This field is blank if there is no restriction on the original destination port. |
| Add icon | This column provides icons to add, edit, and remove virtual servers. In addition, you can activate and deactivate virtual servers.<br><br>To add a virtual server, click the **Add** icon at the top of the column. The **Virtual Server Add/Edit** screen appears.<br><br>To activate / deactivate a virtual server, click the **Active** icon next to the virtual server.<br><br>To edit a virtual server, click the **Edit** icon next to the virtual server. The **Virtual Server Add/Edit** screen appears.<br><br>To delete a virtual server, click on the **Remove** icon next to the virtual server. The Web Configurator confirms that you want to delete it before doing so. |
| Apply | Click this button to save your changes to the ZyWALL. |
| Reset | Click this button to return the screen to its last-saved settings. |

## 16.2.1 The Virtual Server Add/Edit Screen

The **Virtual Server Add/Edit** screen lets you create new virtual servers and edit existing ones. To open this window, open the **Virtual Server** summary screen.

(See Section 16.2 on page 310.) Then, click on an **Add** icon or **Edit** icon to open the following screen.

**Figure 199** Network > Virtual Server > Edit




The following table describes the labels in this screen.

**Table 103** Network > Virtual Server > Edit

| LABEL | DESCRIPTION |
|---|---|
| Enable | Use this option to turn the virtual server on or off. |
| Rule Name | Type in the name of the virtual server. The name is used to refer to the virtual server. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| Incoming Interface | Select the interface on which packets for the virtual server must be received. It can be an Ethernet, VLAN, bridge, or PPPoE/PPTP interface. |
| Original IP | Use the drop-down list box to indicate which destination IP address this virtual server supports. Choices are:<br><br>**Any** - this virtual server supports the IP address of the selected interface.<br><br>**User Defined** - this virtual server supports a specific IP address, specified in the **User Defined** field.<br><br>HOST address - the drop-down box lists all the HOST address objects in the ZyWALL. If you select one of them, this virtual server supports the IP address specified by the address object.<br><br>Select **Create Object** to configure a new IP address object. |
| User Defined Original IP | This field is available if **Original IP** is **User Defined**. Type the destination IP address that this virtual server supports. |

**Table 103** Network > Virtual Server > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Mapped IP | Use the drop-down list box to indicate to which translated destination IP address this virtual server forwards the packet. Choices are:<br><br>**User Defined** - this virtual server supports a specific IP address, specified in the **User Defined** field.<br><br>HOST address - the drop-down box lists all the HOST address objects in the ZyWALL. If you select one of them, this virtual server supports the IP address specified by the address object.<br><br>Select **Create Object** to configure a new IP address object. |
| User Defined Original IP | This field is available if **Mapped IP** is **User Defined**. Type the translated destination IP address that this virtual server supports. |
| Port Mapping Type | Use the drop-down list box to select how many original destination ports this virtual server supports for the selected destination IP address (**Original IP**). Choices are:<br><br>**Any** - this virtual server supports all the destination ports.<br><br>**Port** - this virtual server supports one destination port.<br><br>**Ports** - this virtual server supports a range of destination ports. You might use a range of destination ports for unknown services or when one server supports more than one service.<br><br>See Appendix B on page 905 for some common port numbers. |
| Protocol Type | This field is available if **Mapping Type** is **Port** or **Ports**. Select the protocol (**TCP**, **UDP**, or **Any**) used by the service requesting the connection. |
| Original Port | This field is available if **Mapping Type** is **Port**. Enter the original destination port this virtual server supports. |
| Mapped Port | This field is available if **Mapping Type** is **Port**. Enter the translated destination port if this virtual server forwards the packet. |
| Original Start Port | This field is available if **Mapping Type** is **Ports**. Enter the beginning of the range of original destination ports this virtual server supports. |
| Original End Port | This field is available if **Mapping Type** is **Ports**. Enter the end of the range of original destination ports this virtual server supports. |
| Mapped Start Port | This field is available if **Mapping Type** is **Ports**. Enter the beginning of the range of translated destination ports if this virtual server forwards the packet. |
| Mapped End Port | This field is available if **Mapping Type** is **Ports**. Enter the end of the range of translated destination ports if this virtual server forwards the packet. The original port range and the mapped port range must be the same size. |
| Add corresponding Policy Route rule for NAT 1:1 mapping. | If the server will initiate sessions to the clients, select this check box to create a corresponding policy route so the ZyWALL uses the same public IP address as the traffic's source address. This is called NAT 1:1.<br><br>Or you can click **Policy Route** to go to the screens where you can manually configure a NAT 1:1 policy route for this virtual server.<br><br>See page 314 for an example of NAT 1:1. |

**Table 103** Network > Virtual Server > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Add corresponding Policy Route rule for NAT Loopback. | Select this to allow local users to use a domain name to access this virtual server. By default this virtual server entry only applies this address mapping to packets coming in from the WAN.<br><br>Or you can click **Policy Route** to go to the screens where you can manually configure a NAT loopback policy route for this virtual server.<br><br>See page 318 for an example of NAT loopback. |
| Firewall | By default the firewall blocks incoming connections from external addresses. After you configure your virtual server rule settings, click the **Firewall** link to configure a firewall rule to allow the virtual server's traffic to come in.<br><br>The ZyWALL checks virtual servers before it applies To-ZyWALL firewall rules, so To-ZyWALL firewall rules do not apply to traffic that is forwarded by virtual servers. The ZyWALL still checks other firewall rules according to the source IP address and mapped IP address. |
| OK | Click **OK** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to return to the **Virtual Server** summary screen without creating the virtual server (if it is new) or saving any changes (if it already exists). |

# 16.3 NAT 1:1 and NAT Loopback Examples

The following sections provide examples of manually configuring NAT 1:1 mapping and a policy route rule for NAT loopback. These are provided for your reference, you can select options in the **Virtual Server Add/Edit** screen to have the ZyWALL automatically configure these for you instead of configuring them manually.

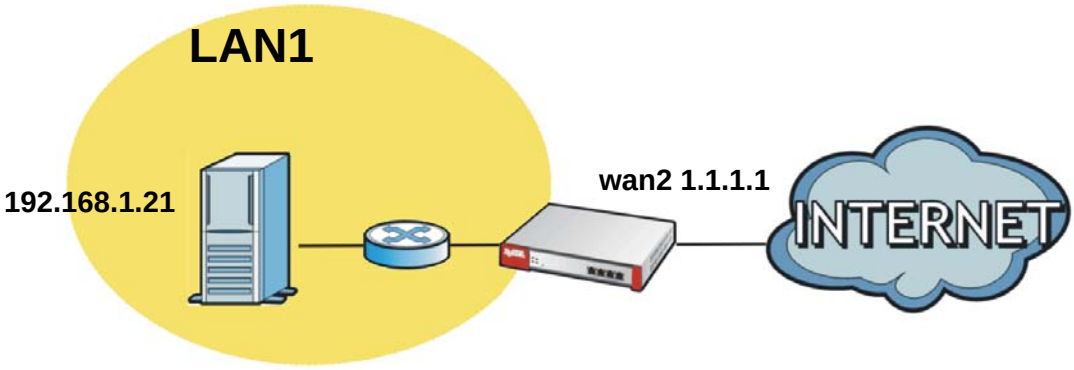
## NAT 1:1 Example

In this example, there is an SMTP mail server in the LAN zone. It has a private IP address of 192.168.1.21. The public IP address for the server is 1.1.1.1 and is on the **wan2** interface.

In order for the server to be accessible to people from the Internet (WAN zone), you need to create a 1:1 NAT mapping from the public IP address to the server's private one.

The firewall is enabled, so you also need to create a rule to allow traffic in from the WAN zone.

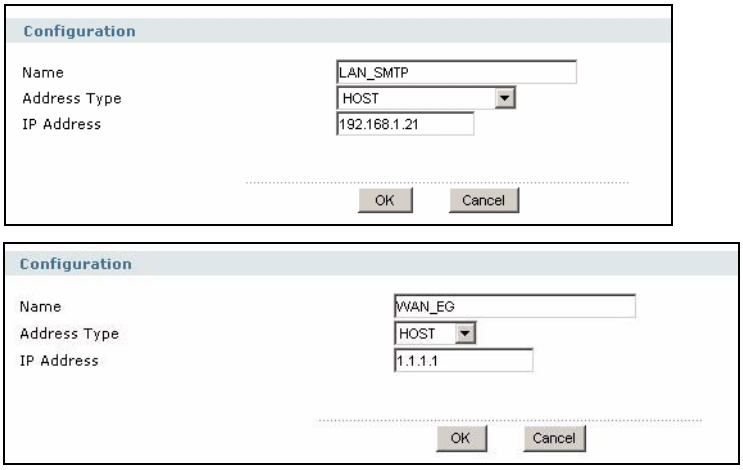
**Figure 200** NAT 1:1 Example Network Topology




## NAT 1:1 Address Objects

Use **Object > Address > Add** to create address objects for the private and public IP addresses (LAN_SMTP and WAN_EG) as shown next.

**Figure 201** Create Address Objects

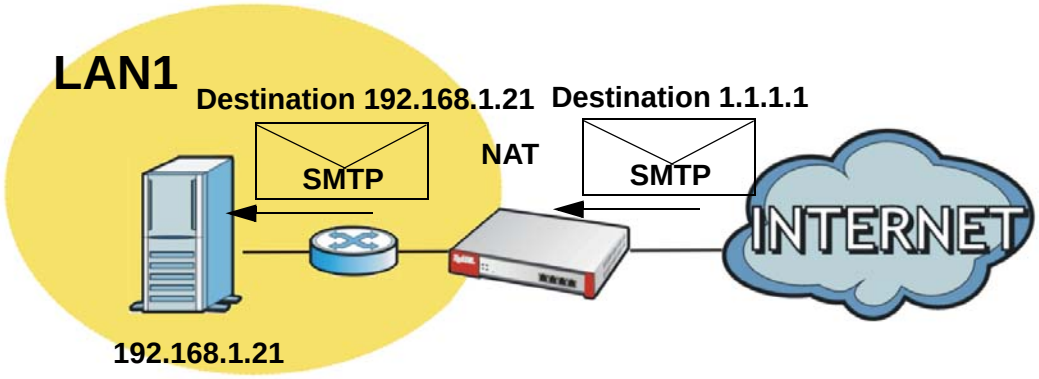



## NAT 1:1 Virtual Server

This section sets up a virtual server rule that changes the destination of SMTP traffic coming to IP address 1.1.1.1 at the ZyWALL's **wan2** interface, to the LAN

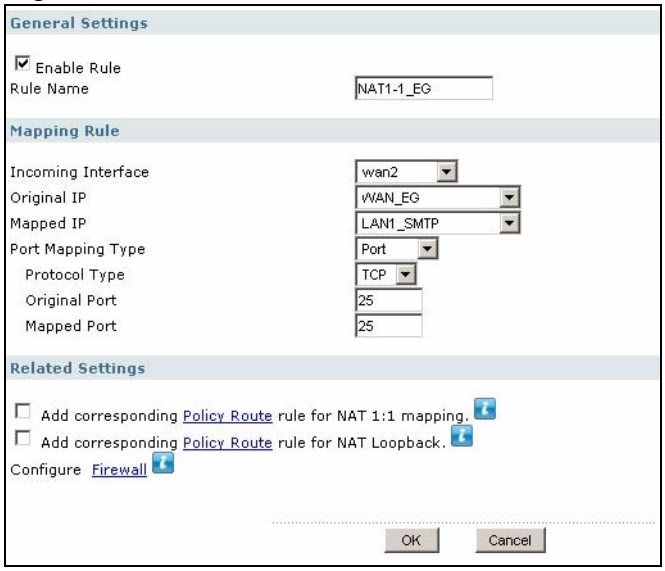
SMTP server's IP address (192.168.1.21). This is also called Destination NAT (DNAT)

**Figure 202** NAT 1:1 Example Virtual Server




The **wan2** interface has a different IP address than 1.1.1.1, so in order for the ZyWALL gateway to be able to do ARP resolution correctly, you need to create a **wan2** virtual server entry. In the **Network > Virtual Server** screen, click the + symbol and create a new virtual server entry as shown next. This entry maps TCP port 25 (SMTP) traffic coming to IP address 1.1.1.1 on **wan2** to the IP address of the SMTP server (192.168.1.21 defined in the **LAN_SMTP** object). In this example the SMTP server also uses port 25, so the **Mapped Port** is set to 25. The following sections describe how to manually configure corresponding policy routes for NAT 1:1 mapping and loopback so the options to have the ZyWALL automatically create them are not selected here.

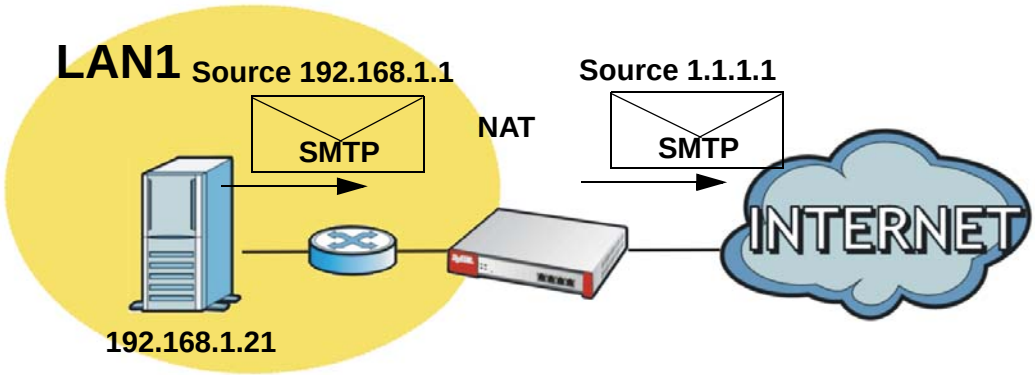
**Figure 203** Create a Virtual Server



## NAT 1:1 Policy Route

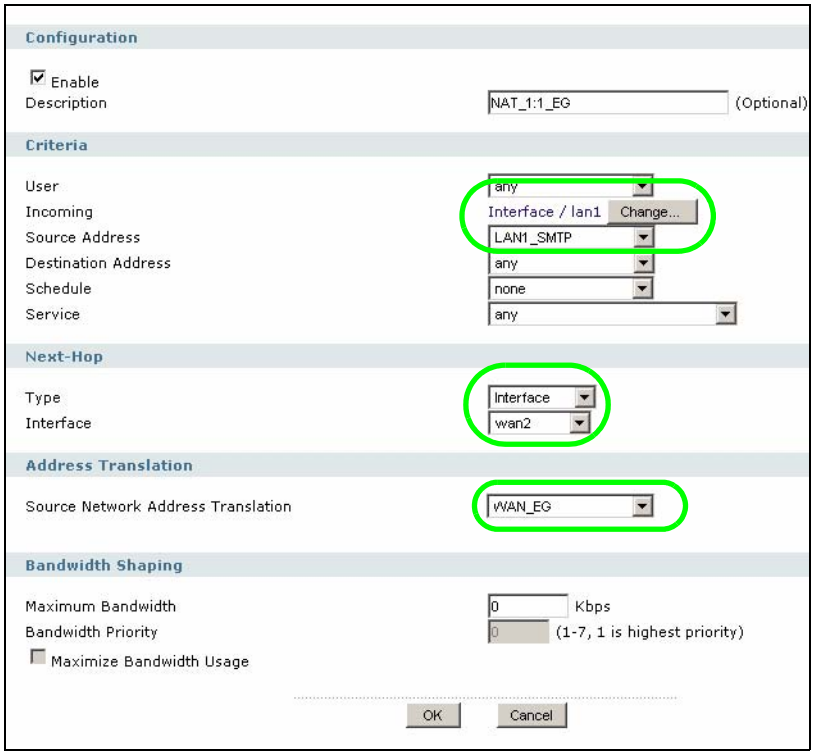
This section sets up a policy route for the traffic coming from the LAN SMTP server to the ZyWALL's **lan1** interface. It changes the source address from 192.168.1.21 to 1.1.1.1. This is also called Source NAT (SNAT). It sends the traffic out through the **wan2** interface.

**Figure 204** NAT 1:1 Example Policy Route




Click **Network > Routing > Policy Route > Add** and configure the screen as shown next. Be careful of where you create the route as routes are ordered in descending priority.

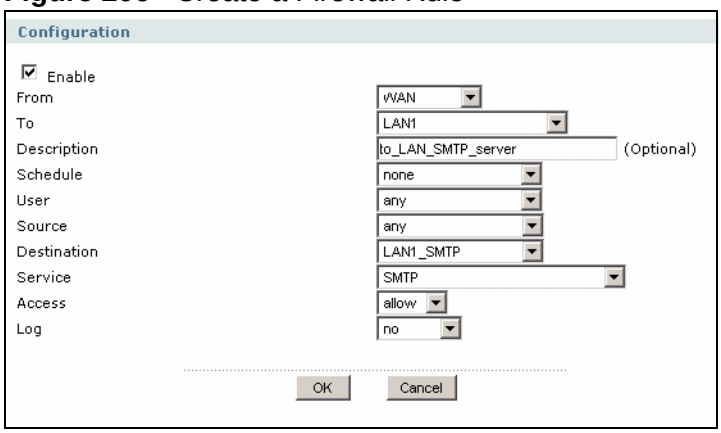
**Figure 205** Create a Policy Route



### NAT 1:1 Firewall Rule

Create a firewall rule to allow access from the WAN zone to the mail server in the LAN1 zone. Be careful of where you create the rule as firewall rules are ordered in descending priority.

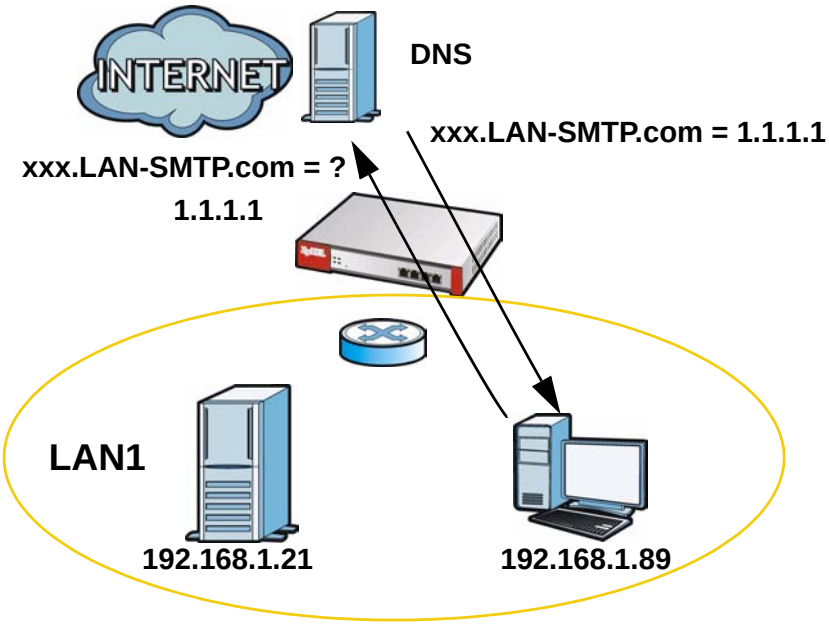
**Figure 206** Create a Firewall Rule




## NAT Loopback Example

The NAT 1:1 Example on page 314 maps a public IP address to the private IP address of a LAN1 SMTP mail server to allow users to access the SMTP mail server from the WAN. LAN1 users can also use an IP address to access the mail server. However, you need to configure NAT loopback for LAN1 users to use a domain name to access the server.

**Figure 207** LAN Computer Queries the DNS Server

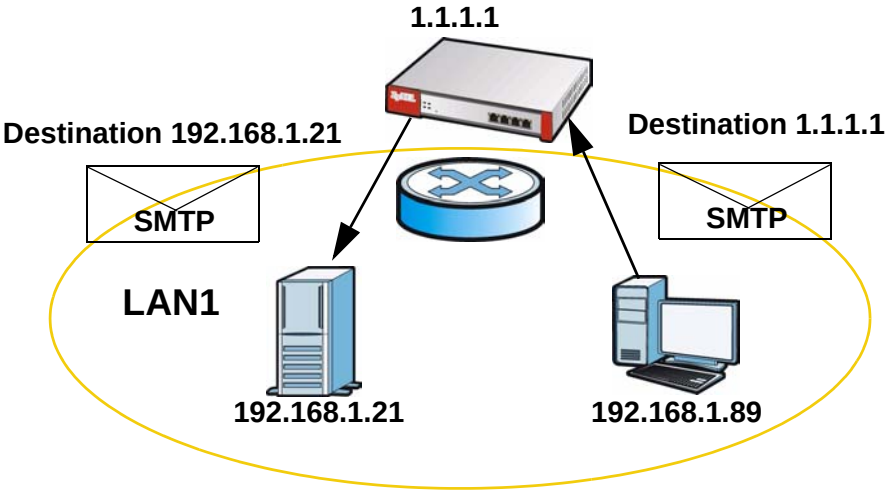


A LAN1 user computer at IP address 192.168.1.89 queries the domain name (xxx.LAN-SMTP.com in this example) from a public DNS server and gets the SMTP server's 1-1 NAT mapped public IP address of 1.1.1.1.

## NAT Loopback Virtual Server

When a LAN1 user sends SMTP traffic to IP address 1.1.1.1, the traffic comes into the ZyWALL through the LAN interface, thus it does not match the NAT 1:1 mapping's virtual server rule for SMTP traffic coming to IP 1.1.1.1 from **wan2**. So you must configure a similar virtual server rule for **wan2**.

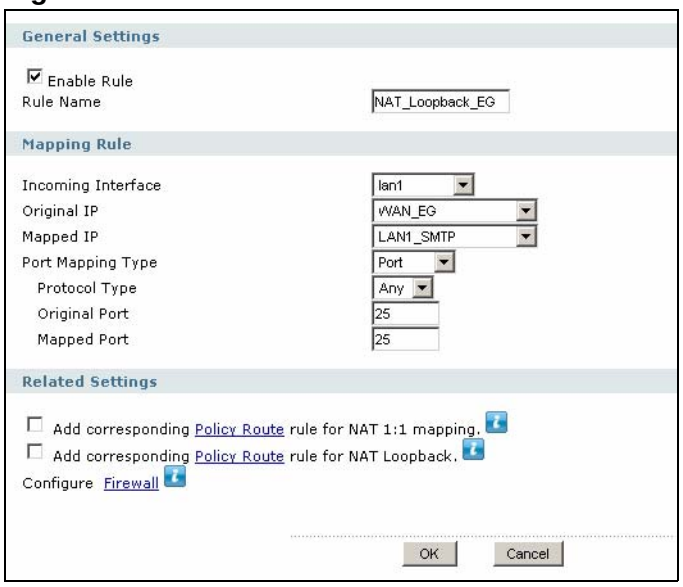
**Figure 208** NAT Loopback Virtual Server




Click **Network > Virtual Server** and the + symbol and create the virtual server rule as shown next. This virtual server rule is the same as in NAT 1:1 Virtual Server on page 315, except you use the **lan1** interface instead of the **wan2** interface. This rule maps TCP port 25 (SMTP) traffic destined for IP address

1.1.1.1 and coming in on **wan2** to the SMTP server (IP address 192.168.1.21). In this example the SMTP server also uses port 25, so the **Mapped Port** is set to 25.

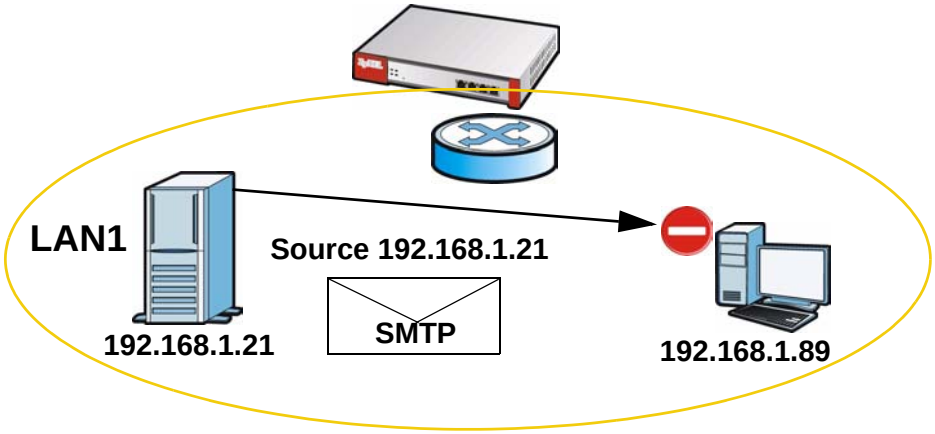
**Figure 209** Create a Virtual Server




## NAT Loopback Policy Route

Without a NAT loopback policy route, the LAN1 user SMTP traffic goes to the LAN1 SMTP server with the LAN1 computer's IP address as the source. The source address is in the same subnet, so the LAN1 SMTP server replies directly. The return traffic uses the SMTP server's LAN1 IP address as the source address[3]. This creates a triangle route since the source does not match the original destination address (1.1.1.1). The user's computer shuts down the session.

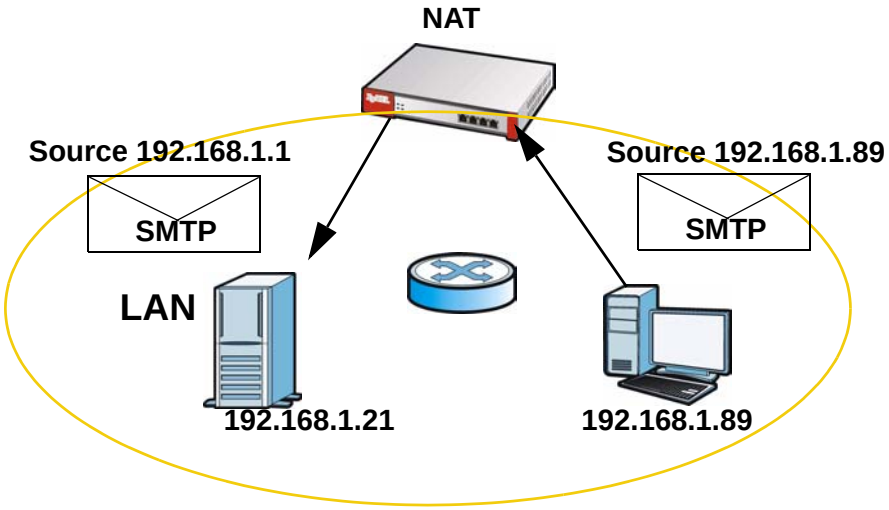
**Figure 210** Triangle Route




3. Even if the packets go through the ZyWALL, they only undergo layer 2 switching, not NAT.

Configure a policy route to use the IP address of the ZyWALL's **lan1** interface (192.168.1.1) as the source address of the traffic going to the LAN1 SMTP server from the LAN1 users. This way the LAN SMTP server replies to the ZyWALL and the ZyWALL applies NAT.

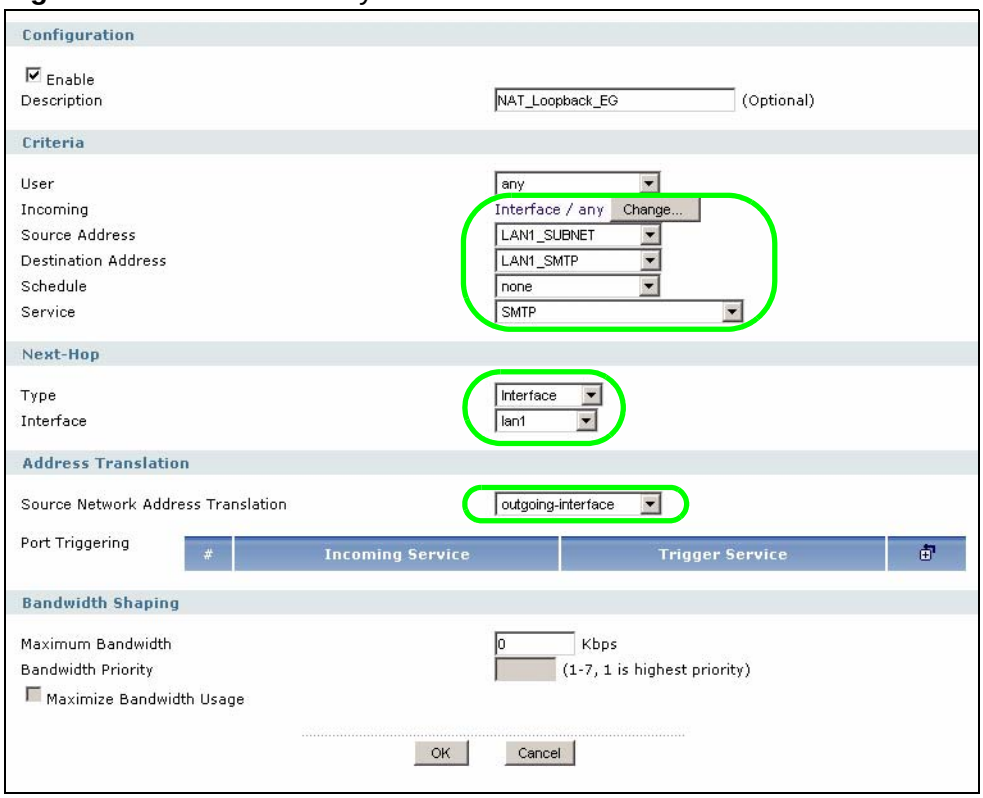
**Figure 211** NAT Loopback Policy Route




Click **Network > Routing > Policy Route > Add** and create the policy route as shown next. Be careful of where you create the route as routes are ordered in

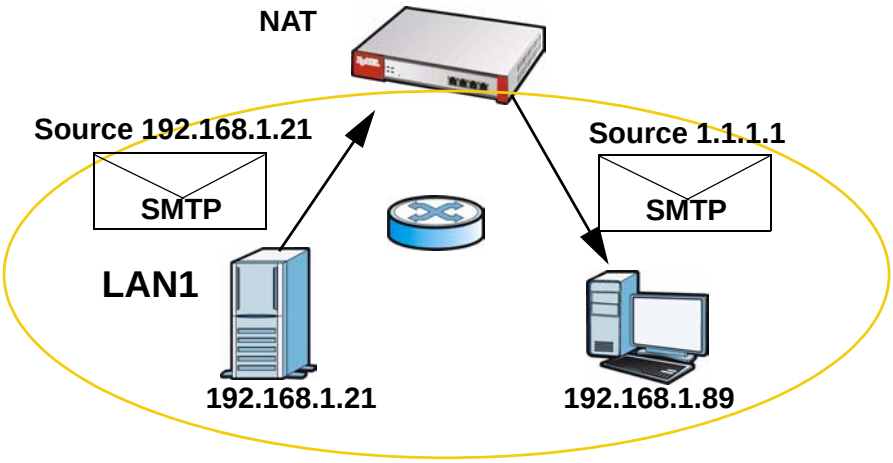
descending priority. This policy route applies source NAT to traffic sent from LAN1 to the SMTP server.

**Figure 212** Create a Policy Route




Now the LAN1 SMTP server replies to the ZyWALL's LAN1 IP address and the ZyWALL changes the source address to 1.1.1.1 before sending it to the LAN1 user's computer. The source in the return traffic matches the original destination address (1.1.1.1) and the LAN1 user can use the LAN1 SMTP server.

**Figure 213** NAT Loopback Successful

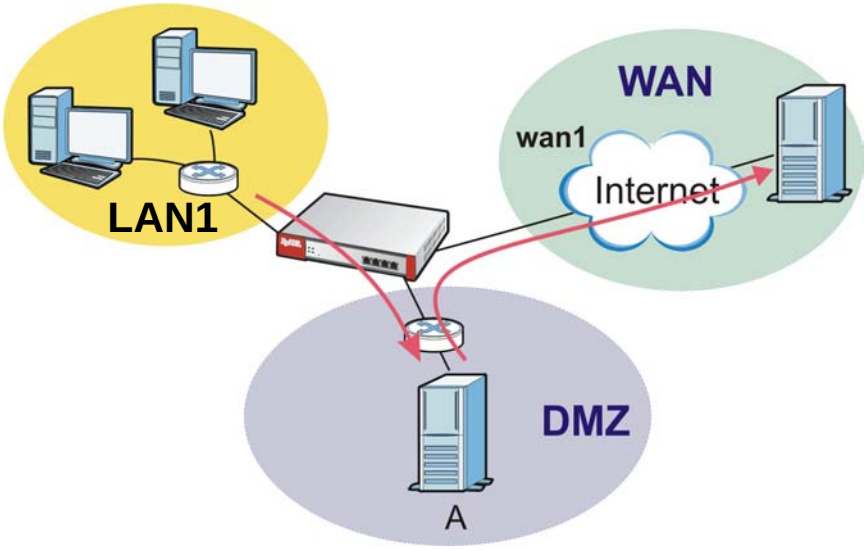


# 17 HTTP Redirect

## 17.1 Overview

HTTP redirect forwards the client's HTTP request (except HTTP traffic destined for the ZyWALL) to a web proxy server. In the following example, proxy server **A** is connected to the **DMZ** interface. When a client connected to the **LAN1** zone wants to open a web page, its HTTP request is redirected to proxy server **A** first. If proxy server **A** cannot find the web page in its cache, a policy route allows it to access the Internet to get them from a server. Proxy server **A** then forwards the response to the client.

**Figure 214** HTTP Redirect Example




### 17.1.1 What You Can Do in the HTTP Redirect Screens

Use the **HTTP Redirect** screens (see Section 17.2 on page 325) to display and edit the HTTP redirect rules.

## 17.1.2 What You Need to Know About HTTP Redirect

### Web Proxy Server

A proxy server helps client devices make indirect requests to access the Internet or outside network resources/services. A proxy server can act as a firewall or an ALG (application layer gateway) between the private network and the Internet or other networks. It also keeps hackers from knowing internal IP addresses.

A client connects to a web proxy server each time he/she wants to access the Internet. The web proxy provides caching service to allow quick access and reduce network usage. The proxy checks its local cache for the requested web resource first. If it is not found, the proxy gets it from the specified server and forwards the response to the client.

### HTTP Redirect, Firewall and Policy Route

With HTTP redirect, the relevant packet flow for HTTP traffic is:

1. Firewall
2. Application Patrol
3. HTTP Redirect
4. Policy Route

Even if you set a policy route to the same incoming interface and service as a HTTP redirect rule, the ZyWALL checks the HTTP redirect rules first and forwards HTTP traffic to a proxy server if matched. You need to make sure there is no firewall rule(s) blocking the HTTP requests from the client to the proxy server.

You also need to manually configure a policy route to forward the HTTP traffic from the proxy server to the Internet. To make the example in Figure 214 on page 323 work, make sure you have the following settings.

For HTTP traffic between **lan1** and **dmz**:

- a from LAN1 to WAN firewall rule (default) to allow HTTP requests from **lan1** to **dmz**. Responses to this request are allowed automatically.
- a application patrol rule to allow HTTP traffic between **lan1** and **dmz**.
- a HTTP redirect rule to forward HTTP traffic from **lan1** to proxy server **A**.

For HTTP traffic between **dmz** and **wan1**:

- a from DMZ to WAN firewall rule (default) to allow HTTP requests from **dmz** to **wan1**. Responses to these requests are allowed automatically.

- a application patrol rule to allow HTTP traffic between **dmz** and **wan1**.
- a policy route to forward HTTP traffic from proxy server **A** to the Internet.

### Finding Out More

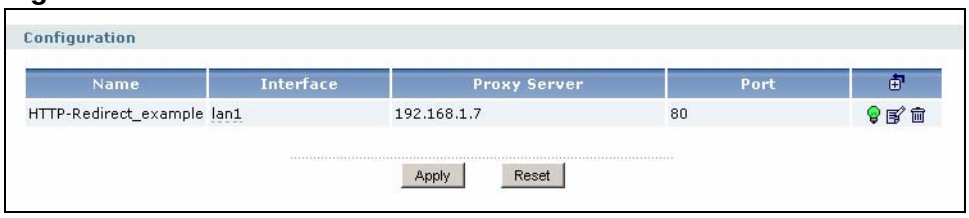
See Section 5.4.20 on page 95 for related information on these screens.

## 17.2 The HTTP Redirect Screen

To configure redirection of a HTTP request to a proxy server, click **Network > HTTP Redirect**. This screen displays the summary of the HTTP redirect rules.

Note: You can configure up to one HTTP redirect rule for each (incoming) interface.

**Figure 215** Network > HTTP Redirect




The following table describes the labels in this screen.

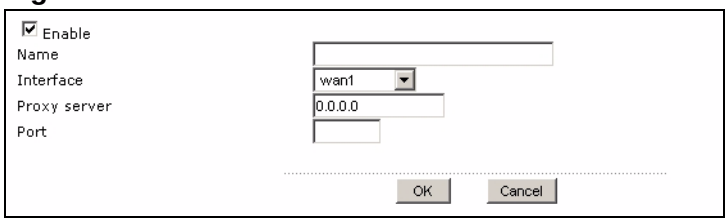
**Table 104** Network > HTTP Redirect

| LABEL | DESCRIPTION |
|---|---|
| Name | This is the descriptive name of a rule. |
| Interface | This is the interface on which the request must be received. |
| Proxy Server | This is the IP address of the proxy server. |
| Port | This is the service port number used by the proxy server. |
| Add icon | Click the **Add** icon in the heading row to add a new entry.<br>The **Active** icon displays whether the rule is enabled or not. Click the **Active** icon to activate or deactivate the rule. Make sure you click **Apply** to save and apply the change.<br>Click the **Edit** icon to go to the screen where you can edit the rule on the ZyWALL.<br>Click the **Remove** icon to delete an existing rule from the ZyWALL. A window displays asking you to confirm that you want to delete the rule. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 17.2.1 The HTTP Redirect Edit Screen

Click **Network > HTTP Redirect** to open the **HTTP Redirect** screen. Then click the **Add** or **Edit** icon to open the **HTTP Redirect Edit** screen where you can configure the rule.

**Figure 216** Network > HTTP Redirect > Edit




The following table describes the labels in this screen.

**Table 105** Network > HTTP Redirect > Edit

| LABEL | DESCRIPTION |
|---|---|
| Enable | Use this option to turn the HTTP redirect rule on or off. |
| Name | Enter a name to identify this rule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| Interface | Select the interface on which the HTTP request must be received for the ZyWALL to forward it to the specified proxy server. |
| Proxy Server | Enter the IP address of the proxy server. |
| Port | Enter the port number that the proxy server uses. |
| OK | Click **OK** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# 18 ALG

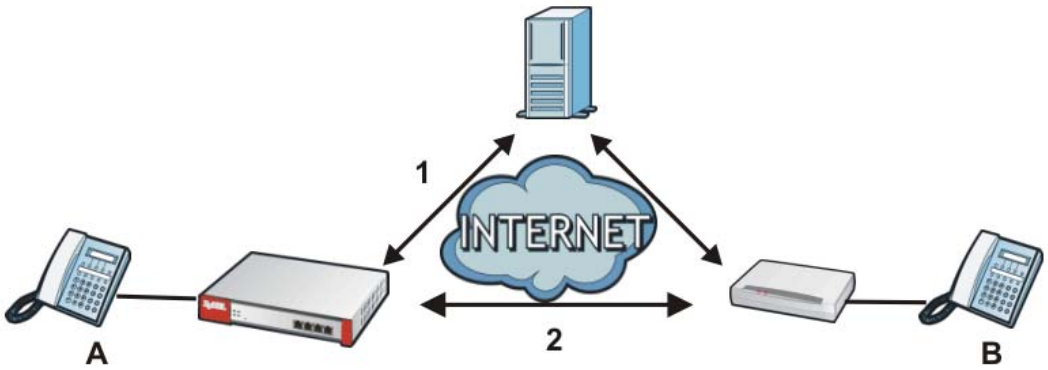
## 18.1 ALG Overview

Application Layer Gateway (ALG) allows the following applications to operate properly through the ZyWALL's NAT.

- FTP - File Transfer Protocol (FTP) is an Internet file transfer service.
- SIP - Session Initiation Protocol (SIP) is an application-layer protocol that can be used to create voice and multimedia sessions over Internet.
- H.323 - This is a teleconferencing protocol suite that provides audio, data and video conferencing.

The following example shows SIP signaling (**1**) and audio (**2**) sessions between SIP clients **A** and **B** and the SIP server.

**Figure 217** SIP ALG Example




The ZyWALL only needs to use the ALG feature for traffic that goes through the ZyWALL's NAT.

### 18.1.1 What You Can Do in the ALG Screen

Use the **ALG** screen (Section 18.2 on page 331) to set up SIP, H.323, and FTP ALG settings.

## 18.1.2 What You Need to Know About ALG

### Application Layer Gateway (ALG), NAT and Firewall

The ZyWALL can function as an Application Layer Gateway (ALG) to allow certain NAT un-friendly applications (such as SIP) to operate properly through the ZyWALL's NAT and firewall. The ZyWALL dynamically creates an implicit NAT session and firewall session for the application's traffic from the WAN to the LAN. The ALG on the ZyWALL supports all of the ZyWALL's NAT mapping types.

### FTP ALG

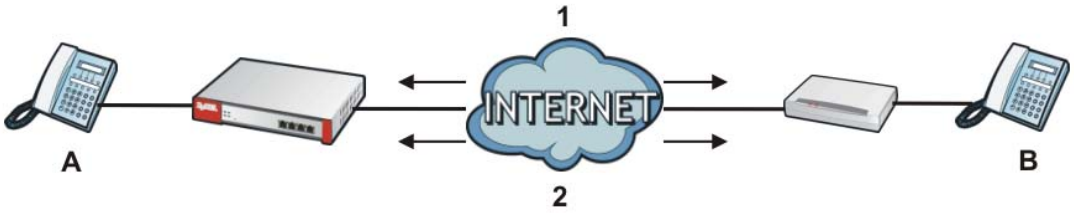
The FTP ALG allows TCP packets with a specified port destination to pass through. If the FTP server is located on the LAN, you must also configure virtual server (NAT port forwarding) and firewall rules if you want to allow access to the server from the WAN.

### H.323 ALG

- The H.323 ALG supports peer-to-peer H.323 calls.
- The H.323 ALG handles H.323 calls that go through NAT or that the ZyWALL routes. You can also make other H.323 calls that do not go through NAT or routing. Examples would be calls between LAN IP addresses that are on the same subnet.
- The H.323 ALG allows calls to go out through NAT. For example, you could make a call from a private IP address on the LAN to a peer device on the WAN.
- The H.323 ALG operates on TCP packets with a specified port destination.
- The ZyWALL allows H.323 audio connections.
- The ZyWALL can also apply bandwidth management to traffic that goes through the H.323 ALG.

The following example shows H.323 signaling (1) and audio (2) sessions between H.323 devices A and B.

**Figure 218** H.323 ALG Example




### SIP ALG

- SIP clients can be connected to the LAN or DMZ. A SIP server must be on the WAN.

- Using the SIP ALG allows you to use bandwidth management on SIP traffic.
- The SIP ALG handles SIP calls that go through NAT or that the ZyWALL routes. You can also make other SIP calls that do not go through NAT or routing. Examples would be calls between LAN IP addresses that are on the same subnet.
- The SIP ALG supports peer-to-peer SIP calls. The firewall (by default) allows peer to peer calls from the LAN zone to go to the WAN zone and blocks peer to peer calls from the WAN zone to the LAN zone.
- The SIP ALG allows UDP packets with a specified port destination to pass through.
- The ZyWALL allows SIP audio connections.
- You do not need to use STUN (Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators) for VoIP devices behind the ZyWALL when you enable the SIP ALG.
- Configuring the SIP ALG to use custom port numbers for SIP traffic also configures the application patrol (see Chapter 29 on page 477) to use the same port numbers for SIP traffic. Likewise, configuring the application patrol to use custom port numbers for SIP traffic also configures SIP ALG to use the same port numbers for SIP traffic.

### Peer-to-Peer Calls and the ZyWALL

The ZyWALL ALG can allow peer-to-peer VoIP calls for both H.323 and SIP. You must configure the firewall and virtual server (port forwarding) to allow incoming (peer-to-peer) calls from the WAN to a private IP address on the LAN (or DMZ).

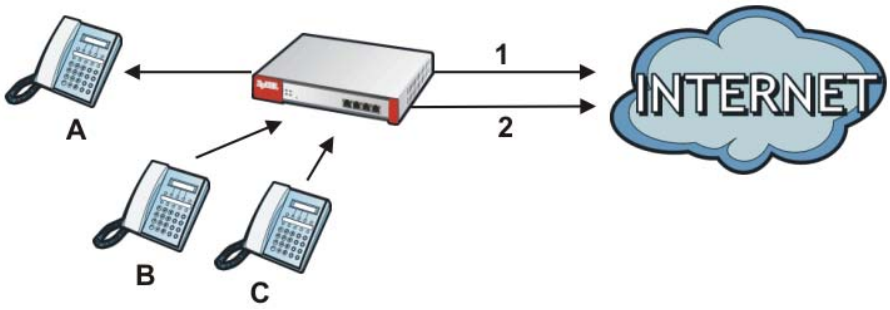
### VoIP Calls from the WAN with Multiple Outgoing Calls

When you configure the firewall and virtual server (port forwarding) to allow calls from the WAN to a specific IP address on the LAN, you can also use policy routing to have H.323 (or SIP) calls from other LAN or DMZ IP addresses go out through a different WAN IP address. The policy routing lets the ZyWALL correctly forward the return traffic for the calls initiated from the LAN IP addresses.

For example, you configure the firewall and virtual server to allow LAN IP address **A** to receive calls from the Internet through WAN IP address **1**. You also use a policy route to have LAN IP address **A** make calls out through WAN IP address **1**. Configure another policy route to have H.323 (or SIP) calls from LAN IP addresses **B** and **C** go out through WAN IP address **2**. Even though only LAN IP address **A**

can receive incoming calls from the Internet, LAN IP addresses **B** and **C** can still make calls out to the Internet.

**Figure 219** VoIP Calls from the WAN with Multiple Outgoing Calls

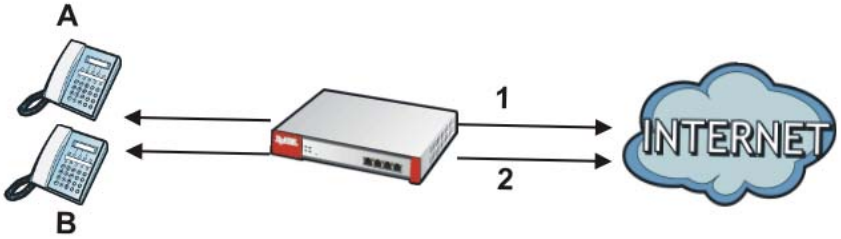



## VoIP with Multiple WAN IP Addresses

With multiple WAN IP addresses on the ZyWALL, you can configure different firewall and virtual server (port forwarding) rules to allow incoming calls from each WAN IP address to go to a specific IP address on the LAN (or DMZ). Use policy routing to have the H.323 (or SIP) calls from each of those LAN or DMZ IP addresses go out through the same WAN IP address that calls come in on. The policy routing lets the ZyWALL correctly forward the return traffic for the calls initiated from the LAN IP addresses.

For example, you configure firewall and virtual server rules to allow LAN IP address **A** to receive calls through public WAN IP address **1**. You configure different firewall and port forwarding rules to allow LAN IP address **B** to receive calls through public WAN IP address **2**. You configure corresponding policy routes to have calls from LAN IP address **A** go out through WAN IP address **1** and calls from LAN IP address **B** go out through WAN IP address **2**.

**Figure 220** VoIP with Multiple WAN IP Addresses




## Finding Out More

- See Section 5.4.21 on page 96 for related information on these screens.
- See Section 6.8 on page 137 for a tutorial showing how to use the ALG for peer-to-peer H.323 traffic.
- See Section 18.3 on page 333 for ALG background/technical information.

### 18.1.3 Before You Begin

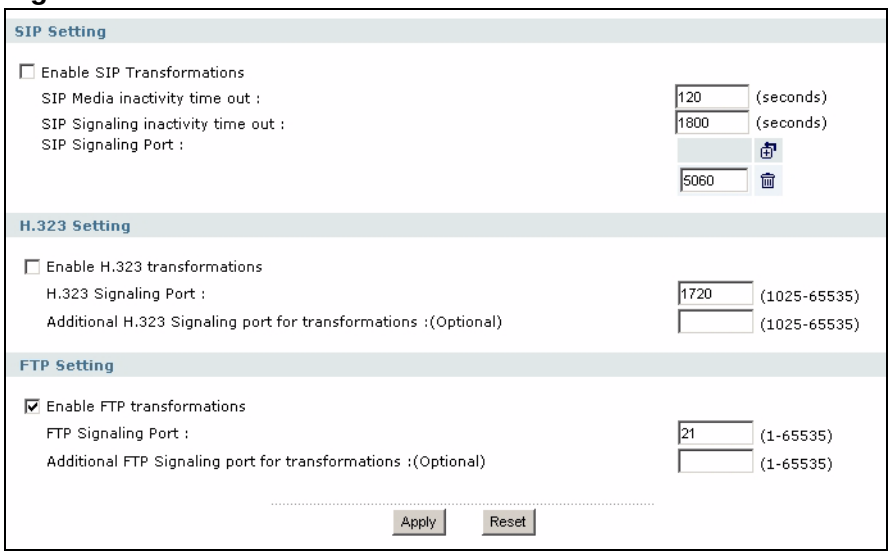
You must also configure the firewall and enable virtual server in the ZyWALL to allow sessions initiate from the WAN.

## 18.2 The ALG Screen

Click **Network > ALG** to open the **ALG** screen. Use this screen to turn ALGs off or on, configure the port numbers to which they apply, and configure SIP ALG time outs.

Note: If the ZyWALL provides an ALG for a service, you must enable the ALG in order to use the application patrol on that service's traffic.

**Figure 221** Network > ALG




The following table describes the labels in this screen.

**Table 106** Network > ALG

| LABEL | DESCRIPTION |
|---|---|
| SIP Setting | |
| Enable SIP Transformations | Turn on the SIP ALG to detect SIP traffic and help build SIP sessions through the ZyWALL's NAT. The ZyWALL modifies IP addresses and port numbers embedded in the SIP data payload. Enabling the SIP ALG also allows you to use the application patrol to detect SIP traffic and manage the SIP traffic's bandwidth (see Chapter 29 on page 477 for the application partol). |

**Table 106** Network > ALG (continued)

| LABEL | DESCRIPTION |
|---|---|
| SIP Media inactivity time out | Use this field to set how many seconds (1~86400) the ZyWALL will allow a SIP session to remain idle (without voice traffic) before dropping it.<br><br>If no voice packets go through the SIP ALG before the timeout period expires, the ZyWALL deletes the audio session. You cannot hear anything and you will need to make a new call to continue your conversation. |
| SIP Signaling inactivity time out | Most SIP clients have an “expire” mechanism indicating the lifetime of signaling sessions. The SIP user agent sends registration packets to the SIP server periodically and keeps the session alive in the ZyWALL.<br><br>If the SIP client does not have this mechanism and makes no calls during the ZyWALL SIP timeout, the ZyWALL deletes the signaling session after the timeout period. Enter the SIP signaling session timeout value (1~86400). |
| SIP Signaling Port | If you are using a custom UDP port number (not 5060) for SIP traffic, enter it here.<br><br>Configuring port numbers for SIP traffic here also configures the application patrol feature to use the same port numbers for SIP traffic.<br><br>Click the **Add** icon to add another custom UDP port number for SIP traffic. You can have a total of up to eight.<br><br>Click the **Remove** icon to delete a custom UDP port number for SIP traffic. |
| H.323 Setting | |
| Enable H.323 transformations | Turn on the H.323 ALG to detect H.323 traffic and help build H.323 sessions through the ZyWALL’s NAT. The ZyWALL modifies IP addresses and port numbers embedded in the H.323 data payload. Enabling the H.323 ALG also allows you to use the application patrol to detect H.323 traffic and manage the H.323 traffic’s bandwidth (see Chapter 29 on page 477 for the application partol). |
| H.323 Signaling Port | If you are using a custom TCP port number (not 1720) for H.323 traffic, enter it here. |
| Additional H.323 Signaling port for transformations | If you are also using H.323 on an additional TCP port number, enter it here. |
| FTP Setting | |
| Enable FTP Transformations | Turn on the FTP ALG to detect FTP traffic and help build FTPsessions through the ZyWALL’s NAT. The ZyWALL modifies IP addresses and port numbers embedded in the FTP data payload. Enabling the FTP ALG also allows you to use the application patrol to detect FTP traffic and manage the FTP traffic’s bandwidth (see Chapter 29 on page 477 for the application partol). |
| FTP Signaling Port | If you are using a custom TCP port number (not 21) for FTP traffic, enter it here. |

**Table 106** Network > ALG (continued)

| LABEL | DESCRIPTION |
|---|---|
| Additional FTP Signaling port for transformations | If you are also using FTP on an additional TCP port number, enter it here. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# 18.3 ALG Technical Reference

Here is more detailed information about the Application Layer Gateway.

### ALG

Some applications cannot operate through NAT (are NAT un-friendly) because they embed IP addresses and port numbers in their packets' data payload. The ZyWALL examines and uses IP address and port number information embedded in the VoIP traffic's data stream. When a device behind the ZyWALL uses an application for which the ZyWALL has VoIP pass through enabled, the ZyWALL translates the device's private IP address inside the data stream to a public IP address. It also records session port numbers and allows the related sessions to go through the firewall so the application's traffic can come in from the WAN to the LAN.

### ALG and Trunks

If you send your ALG-managed traffic through an interface trunk and all of the interfaces are set to active, you can configure routing policies to specify which interface the ALG-managed traffic uses.

You could also have a trunk with one interface set to active and a second interface set to passive. The ZyWALL does not automatically change ALG-managed connections to the second (passive) interface when the active interface's connection goes down. When the active interface's connection fails, the client needs to re-initialize the connection through the second interface (that was set to passive) in order to have the connection go through the second interface. VoIP clients usually re-register automatically at set intervals or the users can manually force them to re-register.

### FTP

File Transfer Protocol (FTP) is an Internet file transfer service that operates on the Internet and over TCP/IP networks. A system running the FTP server accepts

commands from a system running an FTP client. The service allows users to send commands to the server for uploading and downloading files.

### H.323

H.323 is a standard teleconferencing protocol suite that provides audio, data and video conferencing. It allows for real-time point-to-point and multipoint communication between client computers over a packet-based network that does not provide a guaranteed quality of service. NetMeeting uses H.323.

### SIP

The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet. SIP is used in VoIP (Voice over IP), the sending of voice signals over the Internet Protocol.

SIP signaling is separate from the media for which it handles sessions. The media that is exchanged during the session can use a different path from that of the signaling. SIP handles telephone calls and can interface with traditional circuit-switched telephone networks.

### RTP

When you make a VoIP call using H.323 or SIP, the RTP (Real time Transport Protocol) is used to handle voice data transfer. See RFC 1889 for details on RTP.

# 19

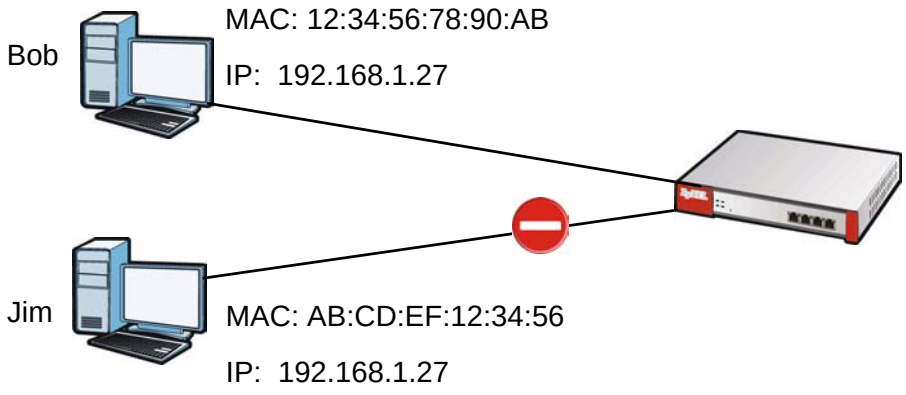
# IP/MAC Binding

## 19.1 IP/MAC Binding Overview

IP address to MAC address binding helps ensure that only the intended devices get to use privileged IP addresses. The ZyWALL uses DHCP to assign IP addresses and records to MAC address it assigned each IP address. The ZyWALL then checks incoming connection attempts against this list. A user cannot manually assign another IP to his computer and use it to connect to the ZyWALL.

Suppose you configure access privileges for IP address 192.168.1.27 and use static DHCP to assign it to Tim's computer's MAC address of 12:34:56:78:90:AB. IP/MAC binding drops traffic from any computer trying to use IP address 192.168.1.27 with another MAC address.

**Figure 222** IP/MAC Binding Example




### 19.1.1 What You Can Do in the IP/MAC Binding Screens

- Use the **Summary** and **Edit** screens (Section 19.2 on page 336) to bind IP addresses to MAC addresses.
- Use the **Exempt List** screen (Section 19.3 on page 339) to configure ranges of IP addresses to which the ZyWALL does not apply IP/MAC binding.
- The **Monitor** screen (Section 19.4 on page 339) lists the devices that have received an IP address from ZyWALL interfaces with IP/MAC binding enabled.

### 19.1.2 What You Need to Know About IP/MAC Binding

#### DHCP

IP/MAC address bindings are based on the ZyWALL's dynamic and static DHCP entries.

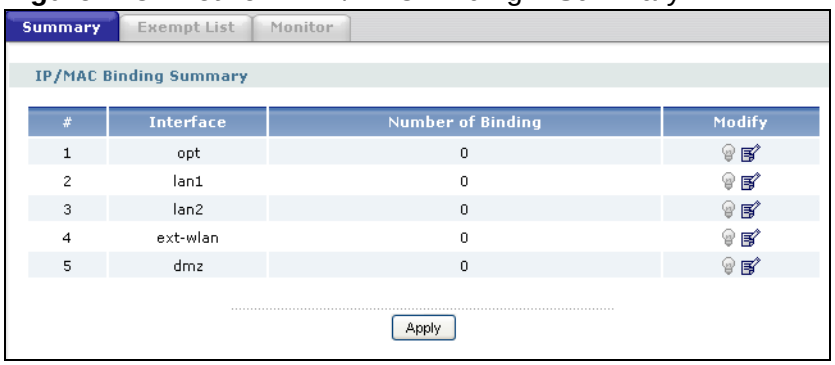
#### Interfaces Used With IP/MAC Binding

IP/MAC address bindings are grouped by interface. You can use IP/MAC binding with Ethernet, bridge, VLAN, and WLAN interfaces. You can also enable or disable IP/MAC binding and logging in an interface's configuration screen.

## 19.2 IP/MAC Binding Summary

Click **Network > IP/MAC Binding** to open the **IP/MAC Binding Summary** screen. This screen lists the total number of IP to MAC address bindings for devices connected to each supported interface.

**Figure 223** Network > IP/MAC Binding > Summary




The following table describes the labels in this screen.

**Table 107** Network > IP/MAC Binding > Summary

| LABEL | DESCRIPTION |
|---|---|
| # | This is the index number of the interface. |
| Interface | This is the name of an interface that supports IP/MAC binding. |
| Number of Binding | This field displays the interface's total number of IP/MAC bindings and IP addresses that the interface has assigned by DHCP. |

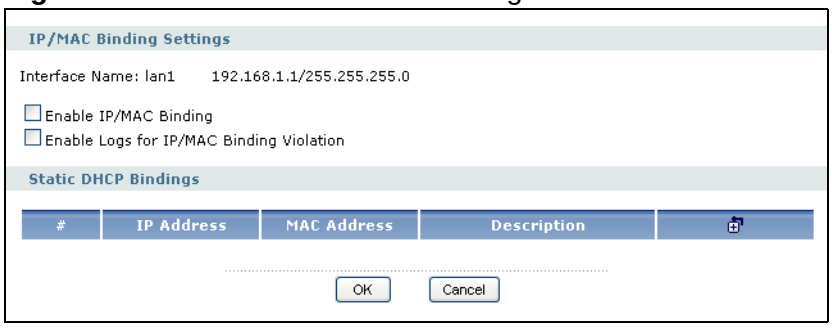
**Table 107** Network > IP/MAC Binding > Summary (continued)

| LABEL | DESCRIPTION |
|---|---|
| Modify | The **Active** icon displays whether or not IP/MAC binding is enabled for an interface. Click it to activate or deactivate IP/MAC binding on an interface. Make sure you click **Apply** to save and apply the change.<br><br>Click the **Edit** icon to go to the screen where you can edit an interface's IP/MAC binding settings. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |

## 19.2.1 IP/MAC Binding Edit

Click **Network > IP/MAC Binding > Edit** to open the **IP/MAC Binding Edit** screen. Use this screen to configure an interface's IP to MAC address binding settings.

**Figure 224** Network > IP/MAC Binding > Edit




The following table describes the labels in this screen.

**Table 108** Network > IP/MAC Binding > Edit

| LABEL | DESCRIPTION |
|---|---|
| IP/MAC Binding Settings | |
| Interface Name | This field displays the name of the interface within the ZyWALL and the interface's IP address and subnet mask. |
| Enable IP/MAC Binding | Select this option to have this interface enforce links between specific IP addresses and specific MAC addresses. This stops anyone else from manually using a bound IP address on another device connected to this interface. Use this to make use only the intended users get to use specific IP addresses. |
| Enable Logs for IP/MAC Binding Violation | Select this option to have the ZyWALL generate a log if a device connected to this interface attempts to use an IP address not assigned by the ZyWALL. |
| Static DHCP Bindings | This table lists the bound IP and MAC addresses. The ZyWALL checks this table when it assigns IP addresses. If the computer's MAC address is in the table, the ZyWALL assigns the corresponding IP address. You can also access this table from the interface's edit screen. |

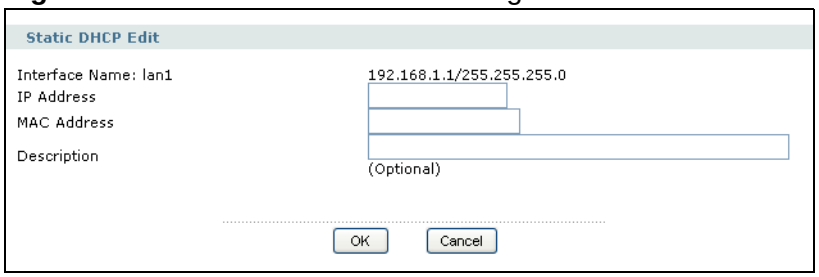
**Table 108** Network > IP/MAC Binding > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| # | This is the index number of the static DHCP entry. |
| IP Address | This is the IP address that the ZyWALL assigns to a device with the entry's MAC address. |
| MAC Address | This is the MAC address of the device to which the ZyWALL assigns the entry's IP address. |
| Description | This helps identify the entry. |
| Add icon | Click the **Add** icon to add a new entry.<br>Click the **Edit** icon to go to the screen where you can edit the entry.<br>Click the **Remove** icon to delete an entry. A window displays asking you to confirm that you want to delete it. |
| OK | Click **OK** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving. |

## 19.2.2 Static DHCP Edit

Click **Network > IP/MAC Binding > Edit** to open the **IP/MAC Binding Edit** screen. Click the **Add** or **Edit** icon to open the following screen. Use this screen to configure an interface's IP to MAC address binding settings.

**Figure 225** Network > IP/MAC Binding > Edit > Add




The following table describes the labels in this screen.

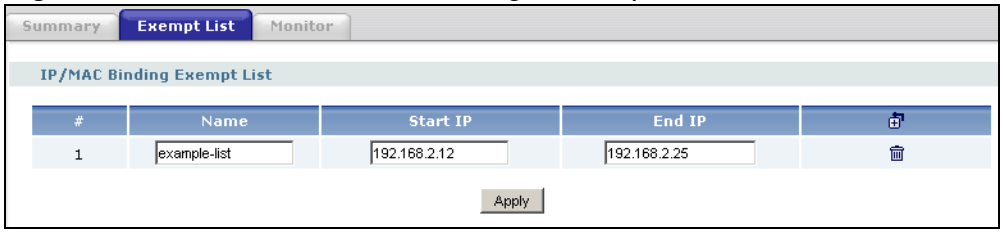
**Table 109** Network > IP/MAC Binding > Edit > Add

| LABEL | DESCRIPTION |
|---|---|
| Interface Name | This field displays the name of the interface within the ZyWALL and the interface's IP address and subnet mask. |
| IP Address | Enter the IP address that the ZyWALL is to assign to a device with the entry's MAC address. |
| MAC Address | Enter the MAC address of the device to which the ZyWALL assigns the entry's IP address. |
| Description | Enter up to 64 printable ASCII characters to help identify the entry. For example, you may want to list the computer's owner. |
| OK | Click **OK** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# 19.3 IP/MAC Binding Exempt List

Click **Network > IP/MAC Binding > Exempt List** to open the **IP/MAC Binding Exempt List** screen. Use this screen to configure ranges of IP addresses to which the ZyWALL does not apply IP/MAC binding.

**Figure 226** Network > IP/MAC Binding > Exempt List




The following table describes the labels in this screen.

**Table 110** Network > IP/MAC Binding > Exempt List

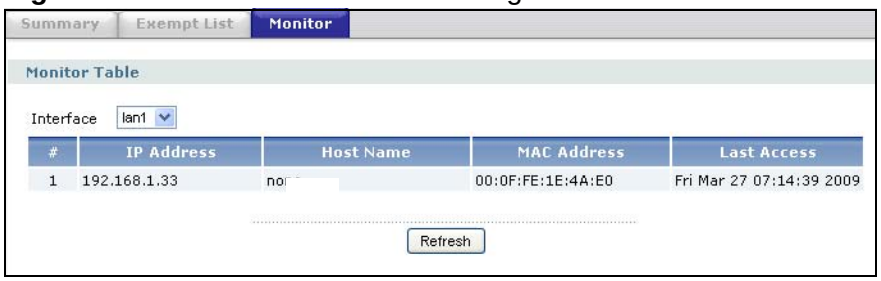
| LABEL | DESCRIPTION |
|---|---|
| # | This is the index number of the IP/MAC binding list entry. |
| Name | Enter a name to help identify this entry. |
| Start IP | Enter the first IP address in a range of IP addresses for which the ZyWALL does not apply IP/MAC binding. |
| End IP | Enter the last IP address in a range of IP addresses for which the ZyWALL does not apply IP/MAC binding. |
| Add icon | Click the **Add** icon to add a new entry.<br>Click the **Remove** icon to delete an entry. A window displays asking you to confirm that you want to delete it. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |

# 19.4 IP/MAC Binding Monitor

Click **Network > IP/MAC Binding > Monitor** to open the **IP/MAC Binding Monitor** screen. This screen lists the devices that have received an IP address from ZyWALL interfaces with IP/MAC binding enabled and have ever established a

session with the ZyWALL. Devices that have never established a session with the ZyWALL do not display in the list.

**Figure 227** Network > IP/MAC Binding > Monitor




The following table describes the labels in this screen.

**Table 111** Network > IP/MAC Binding > Monitor

| LABEL | DESCRIPTION |
|---|---|
| Interface | Select a ZyWALL interface that has IP/MAC binding enabled to show to which devices it has assigned an IP address. |
| # | This is the index number of an IP/MAC binding entry. |
| IP Address | This is the IP address that the ZyWALL assigned to a device. |
| Host Name | This field displays the name used to identify this device on the network (the computer name). The ZyWALL learns these from the DHCP client requests. |
| MAC Address | This field displays the MAC address to which the IP address is currently assigned. |
| Last Access | This is when the device last established a session with the ZyWALL through this interface. |
| Refresh | Click this button to update the information in the screen. |

# PART III
# Firewall

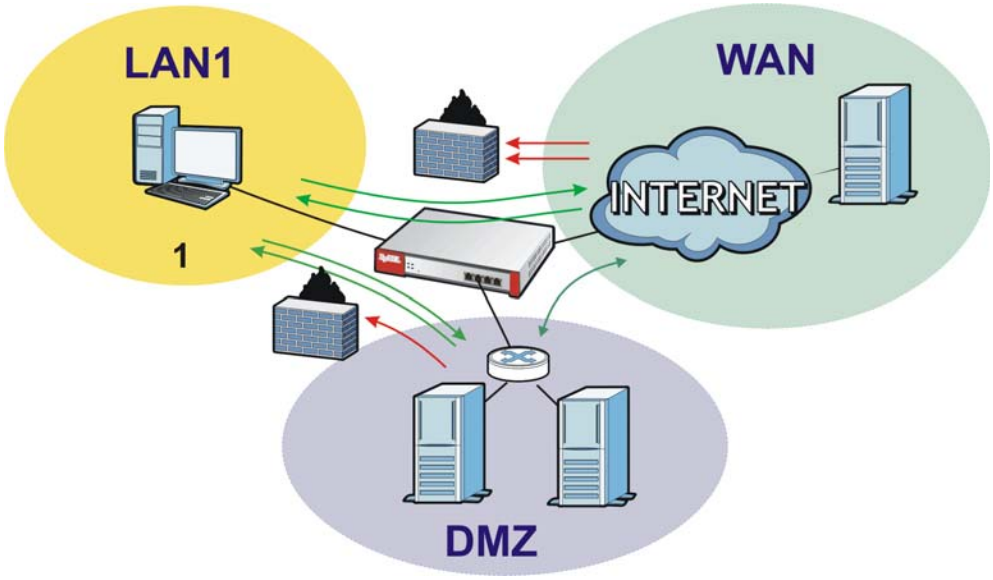
# 20 Firewall

## 20.1 Overview

Use the firewall to block or allow services that use static port numbers. Use application patrol (see Chapter 29 on page 477) to control services using flexible/dynamic port numbers. The firewall can also limit the number of user sessions.

This figure shows the ZyWALL's default firewall rules in action and demonstrates how stateful inspection works. User **1** can initiate a Telnet session from within the LAN1 zone and responses to this request are allowed. However, other Telnet traffic initiated from the WAN or DMZ zone and destined for the LAN1 zone is blocked. Communications between the WAN and the DMZ zones are allowed. The firewall allows VPN traffic between any of the networks.

**Figure 228** Default Firewall Action




### 20.1.1 What You Can Do in the Firewall Screens

- Use the **Firewall** screens (Section 20.2 on page 351) to enable or disable the firewall and asymmetrical routes, and manage and configure firewall rules.
- Use the **Session Limit** screens (see Section 20.3 on page 357) to limit the number of concurrent NAT/firewall sessions a client can use.

## 20.1.2 What You Need to Know About the Firewall

### Stateful Inspection

The ZyWALL has a stateful inspection firewall. The ZyWALL restricts access by screening data packets against defined access rules. It also inspects sessions. For example, traffic from one zone is not allowed unless it is initiated by a computer in another zone first.

### Zones

A zone is a group of interfaces or VPN tunnels. Group the ZyWALL's interfaces into different zones based on your needs. You can configure firewall rules for data passing between zones or even between interfaces and/or VPN tunnels in a zone.

### Default Firewall Behavior

Firewall rules are grouped based on the direction of travel of packets to which they apply. Here is the default firewall behavior for traffic going through the ZyWALL in various directions.

**Table 112** Default Firewall Rules

| FROM ZONE TO ZONE | STATEFUL PACKET INSPECTION |
|---|---|
| From ANY to ANY | Traffic that does not match any firewall rule is allowed. This includes traffic to or from interfaces or VPN tunnels that are not assigned to a zone (extra-zone traffic). |
| From WAN to LAN | Traffic from the WAN to the LAN is dropped. |
| From WAN to WLAN | Traffic from the WAN to the WLAN is dropped. |
| From WAN to ZyWALL (Default services) | Traffic from the WAN to the ZyWALL (default services) is allowed. Default services are traffic types described in To-ZyWALL Rules on page 345. |
| From WAN to ZyWALL | Traffic from the WAN to the ZyWALL itself is dropped except for the traffic types described in To-ZyWALL Rules on page 345. |
| From DMZ to LAN | Traffic from the DMZ to the LAN is dropped. |
| From DMZ to WLAN | Traffic from the DMZ to the WLAN is dropped. |
| From DMZ to ZyWALL (Default services) | Traffic from the DMZ to the ZyWALL (default services) is allowed. Default services are traffic types described in To-ZyWALL Rules on page 345. |
| From DMZ to ZyWALL | Traffic from the DMZ to the ZyWALL itself is dropped except for the traffic types described in To-ZyWALL Rules on page 345. |
| From WLAN to LAN | Traffic from the WLAN to the LAN is dropped. |
| From WLAN to WAN (guest) | Traffic from the WLAN to the WAN (guest) is allowed. |
| From WLAN to WAN (DNS) | Traffic from the WLAN to the WAN (DNS) is allowed. |

**Table 112** Default Firewall Rules

| FROM ZONE TO ZONE | STATEFUL PACKET INSPECTION |
|---|---|
| From WLAN to WAN | Traffic from WLAN to WAN is dropped. |
| From WLAN to DMZ | Traffic from WLAN to DMZ is dropped. |
| From WLAN to ZyWALL | Traffic from the DMZ to the ZyWALL is allowed. |

### To-ZyWALL Rules

Rules with **ZyWALL** as the **To Zone** apply to traffic going to the ZyWALL itself. By default:

- The firewall allows only LAN, WLAN, or WAN computers to access or manage the ZyWALL.
- The ZyWALL drops most packets from the WAN zone to the ZyWALL itself, except for VRRP traffic for Device HA and ESP/AH/IKE/NATT/HTTPS services for VPN tunnels, and generates a log.
- The ZyWALL drops most packets from the DMZ zone to the ZyWALL itself, except for DNS and NetBIOS traffic, and generates a log.

When you configure a firewall rule for packets destined for the ZyWALL itself, make sure it does not conflict with your service control rule. See Chapter 45 on page 731 for more information about service control (remote management). The ZyWALL checks the firewall rules before the service control rules for traffic destined for the ZyWALL.

You can configure a To-ZyWALL firewall rule (with **From Any To ZyWALL** direction) for traffic from an interface which is not in a zone.

### Global Firewall Rules

Firewall rules with **from any** and/or **to any** as the packet direction are called global firewall rules. The global firewall rules are the only firewall rules that apply to an interface or VPN tunnel that is not included in a zone. The **from any** rules apply to traffic coming from the interface and the **to any** rules apply to traffic going to the interface.

### Firewall Rule Criteria

The ZyWALL checks the schedule, user name (user's login name on the ZyWALL), source IP address, destination IP address and IP protocol type of network traffic against the firewall rules (in the order you list them). When the traffic matches a rule, the ZyWALL takes the action specified in the rule.

### User Specific Firewall Rules

You can specify users or user groups in firewall rules. For example, to allow a specific user from any computer to access a zone by logging in to the ZyWALL, you can set up a rule based on the user name only. If you also apply a schedule to the firewall rule, the user can only access the network at the scheduled time. A user-aware firewall rule is activated whenever the user logs in to the ZyWALL and will be disabled after the user logs out of the ZyWALL.

### Firewall and Application Patrol

To use a service, make sure both the firewall and application patrol allow the service's packets to go through the ZyWALL. The ZyWALL checks the firewall rules before the application patrol rules for traffic going through the ZyWALL.

### Firewall and VPN Traffic

After you create a VPN tunnel and add it to a zone, you can set the firewall rules applied to VPN traffic. If you add a VPN tunnel to an existing zone (the LAN1 zone for example), you can configure a new LAN1 to LAN1 firewall rule or use intra-zone traffic blocking to allow or block VPN traffic transmitting between the VPN tunnel and other interfaces in the LAN zone. If you add the VPN tunnel to a new zone (the VPN zone for example), you can configure rules for VPN traffic between the VPN zone and other zones or **From VPN To-ZyWALL** rules for VPN traffic destined for the ZyWALL.

### Session Limits

Accessing the ZyWALL or network resources through the ZyWALL requires a NAT session and corresponding firewall session. Peer to peer applications, such as file sharing applications, may use a large number of NAT sessions. A single client could use all of the available NAT sessions and prevent others from connecting to or through the ZyWALL. The ZyWALL lets you limit the number of concurrent NAT/firewall sessions a client can use.

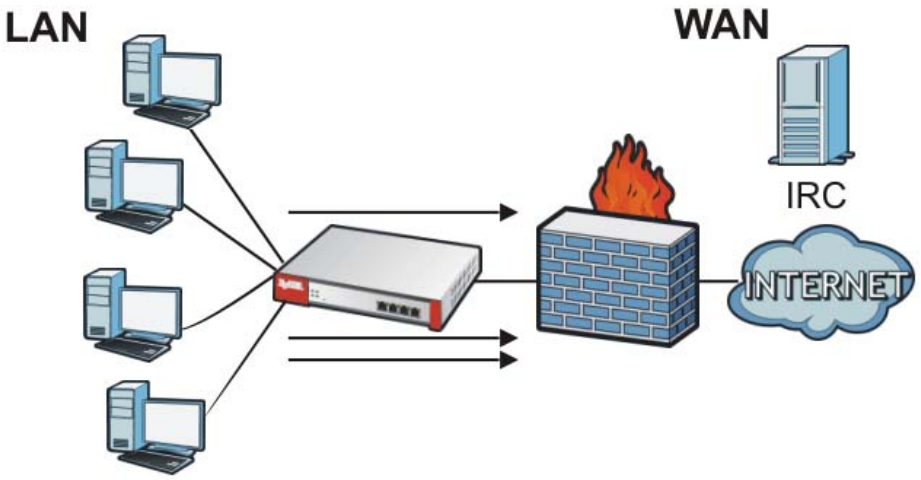
### Finding Out More

- See Section 5.4.12 on page 91 for related information on the **Firewall** screens.
- See Section 6.6.6 on page 133 for an example of creating firewall rules as part of configuring user-aware access control (Section 6.6 on page 127).
- See Section 6.8.3 on page 139 for an example of creating a firewall rule to allow H.323 traffic from the WAN to the LAN.

## 20.1.3 Firewall Rule Example Applications

Suppose that your company decides to block all of the LAN users from using IRC (Internet Relay Chat) through the Internet. To do this, you would configure a LAN to WAN firewall rule that blocks IRC traffic from any source IP address from going to any destination address. You do not need to specify a schedule since you need the firewall rule to always be in effect. The following figure shows the results of this rule.

**Figure 229** Blocking All LAN to WAN IRC Traffic Example




Your firewall would have the following rules.

**Table 113** Blocking All LAN to WAN IRC Traffic Example

| # | USER | SOURCE | DESTINATION | SCHEDULE | SERVICE | ACTION |
|---|---|---|---|---|---|---|
| 1 | Any | Any | Any | Any | IRC | Deny |
| 2 | Any | Any | Any | Any | Any | Allow |

- The first row blocks LAN access to the IRC service on the WAN.
- The second row is the firewall's default policy that allows all LAN1 to WAN traffic.

The ZyWALL applies the firewall rules in order. So for this example, when the ZyWALL receives traffic from the LAN, it checks it against the first rule. If the traffic matches (if it is IRC traffic) the firewall takes the action in the rule (drop) and stops checking the firewall rules. Any traffic that does not match the first firewall rule will match the second rule and the ZyWALL forwards it.

Now suppose that your company wants to let the CEO use IRC. You can configure a LAN1 to WAN firewall rule that allows IRC traffic from the IP address of the CEO's computer. You can also configure a LAN to WAN rule that allows IRC traffic from any computer through which the CEO logs into the ZyWALL with his/her user

name. In order to make sure that the CEO's computer always uses the same IP address, make sure it either:

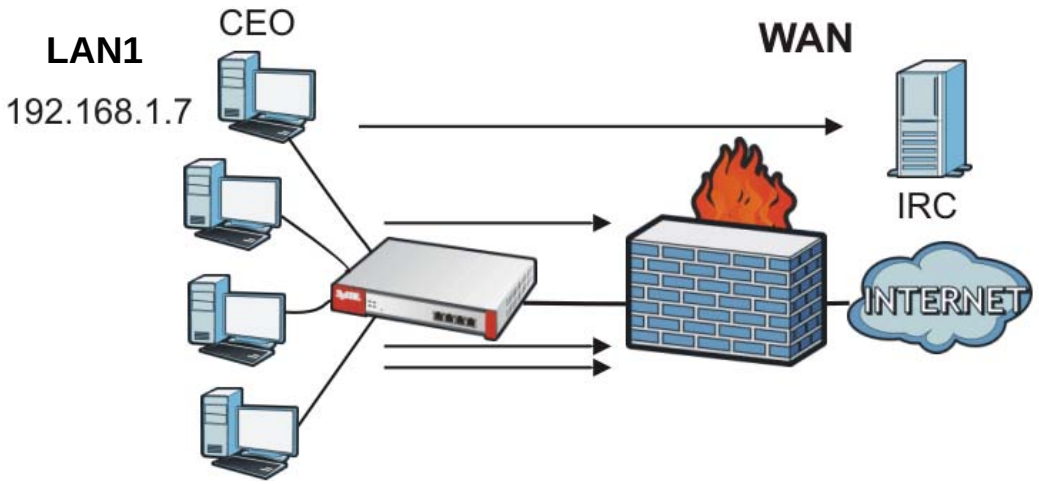
- Has a static IP address,

  or

- You configure a static DHCP entry for it so the ZyWALL always assigns it the same IP address (see DHCP Settings on page 259 for information on DHCP).

Now you configure a LAN1 to WAN firewall rule that allows IRC traffic from the IP address of the CEO's computer (192.168.1.7 for example) to go to any destination address. You do not need to specify a schedule since you want the firewall rule to always be in effect. The following figure shows the results of your two custom rules.

**Figure 230** Limited LAN to WAN IRC Traffic Example




Your firewall would have the following configuration.

**Table 114** Limited LAN1 to WAN IRC Traffic Example 1

| # | USER | SOURCE | DESTINATION | SCHEDULE | SERVICE | ACTION |
|---|---|---|---|---|---|---|
| 1 | Any | 192.168.1.7 | Any | Any | IRC | Allow |
| 2 | Any | Any | Any | Any | IRC | Deny |
| 3 | Any | Any | Any | Any | Any | Allow |

- The first row allows the LAN1 computer at IP address 192.168.1.7 to access the IRC service on the WAN.
- The second row blocks LAN1 access to the IRC service on the WAN.
- The third row is the firewall's default policy of allowing all traffic from the LAN1 to go to the WAN.

Alternatively, you configure a LAN1 to WAN rule with the CEO's user name (say CEO) to allow IRC traffic from any source IP address to go to any destination address.

Your firewall would have the following configuration.

**Table 115** Limited LAN1 to WAN IRC Traffic Example 2

| # | USER | SOURCE | DESTINATION | SCHEDULE | SERVICE | ACTION |
|---|---|---|---|---|---|---|
| 1 | CEO | Any | Any | Any | IRC | Allow |
| 2 | Any | Any | Any | Any | IRC | Deny |
| 3 | Any | Any | Any | Any | Any | Allow |

- The first row allows any LAN1 computer to access the IRC service on the WAN by logging into the ZyWALL with the CEO's user name.
- The second row blocks LAN1 access to the IRC service on the WAN.
- The third row is the firewall's default policy of allowing all traffic from the LAN1 to go to the WAN.

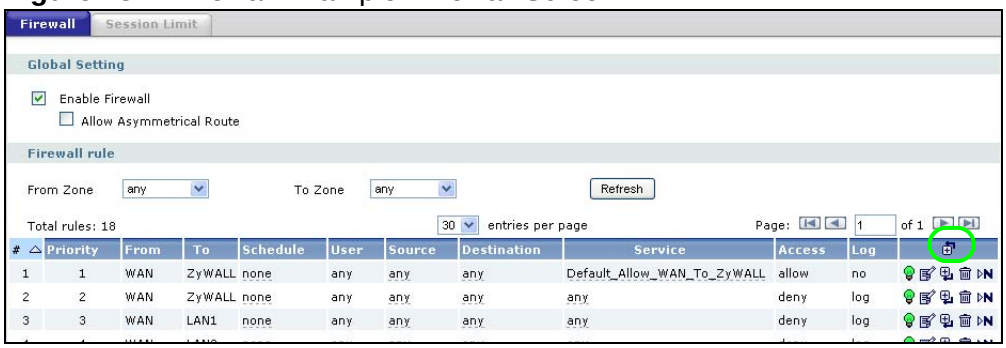
The rule for the CEO must come before the rule that blocks all LAN1 to WAN IRC traffic. If the rule that blocks all LAN1 to WAN IRC traffic came first, the CEO's IRC traffic would match that rule and the ZyWALL would drop it and not check any other firewall rules.

## 20.1.4 Firewall Rule Configuration Example

The following Internet firewall rule example allows a hypothetical MyService from the WAN to IP addresses 192.168.1.10 through 192.168.1.15 (Dest_1) on the LAN1.

1 Click **Firewall**. Click the **Add** icon ( ) in the heading row to configure a new first entry. Remember the sequence (priority) of the rules is important since they are applied in order.

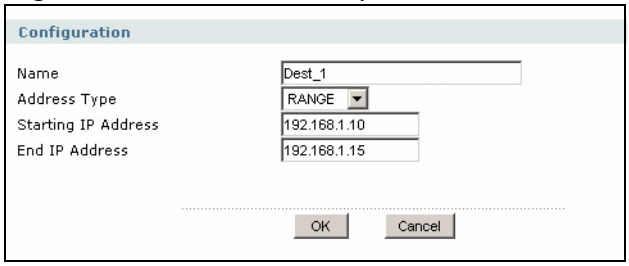
**Figure 231** Firewall Example: Firewall Screen




2 Select **Create Object** in the **Destination** drop-down list box.

3 The screen for configuring an address object opens. Configure it as follows and click **OK**.

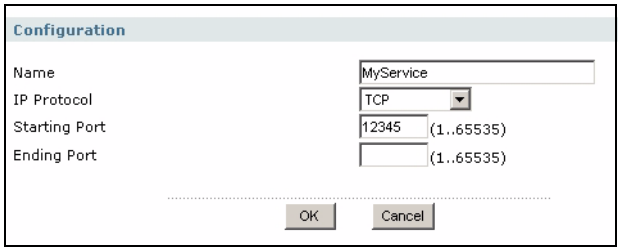
**Figure 232** Firewall Example: Create an Address Object




4 Select **Create Object** in the **Service** drop-down list box.

5 The screen for configuring a service object opens. Configure it as follows and click **OK**.

**Figure 233** Firewall Example: Create a Service Object

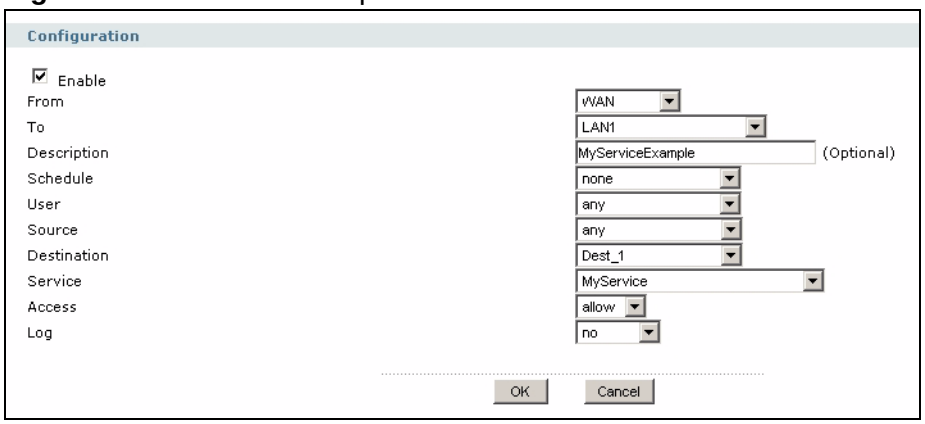



6 Select **From WAN** and **To LAN1**.

7 Enter the name of the firewall rule.

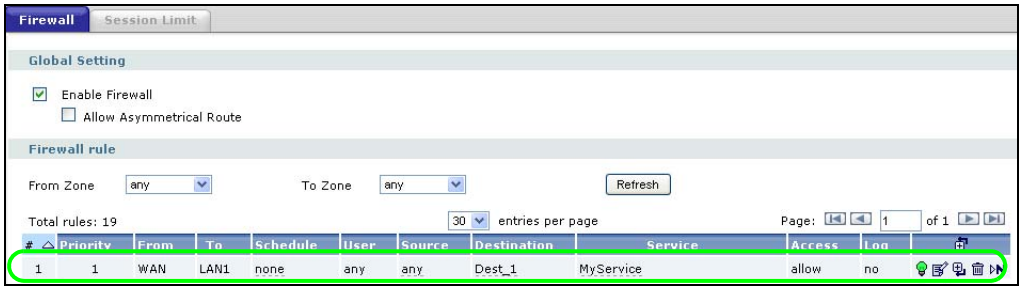
8 Make sure **Dest_1** is selected for the **Destination** and **MyService** is selected as the **Service**. Enter a description and configure the rest of the screen as follows. Click **OK** when you are done.

**Figure 234** Firewall Example: Edit a Firewall Rule



9 The firewall rule appears in the firewall rule summary.

**Figure 235** Firewall Example: MyService Example Rule in Summary




# 20.2 The Firewall Screen

### Asymmetrical Routes

If an alternate gateway on the LAN has an IP address in the same subnet as the ZyWALL's LAN IP address, return traffic may not go through the ZyWALL. This is called an asymmetrical or "triangle" route. This causes the ZyWALL to reset the connection, as the connection has not been acknowledged.

You can have the ZyWALL permit the use of asymmetrical route topology on the network (not reset the connection). However, allowing asymmetrical routes may let traffic from the WAN go directly to the LAN without passing through the ZyWALL. A better solution is to use virtual interfaces to put the ZyWALL and the backup gateway on separate subnets. Virtual interfaces allow you to partition your network into logical sections over the same interface. See the chapter about interfaces for more information.

By putting LAN 1 and the alternate gateway (**A** in the figure) in different subnets, all returning network traffic must pass through the ZyWALL to the LAN. The following steps and figure describe such a scenario.

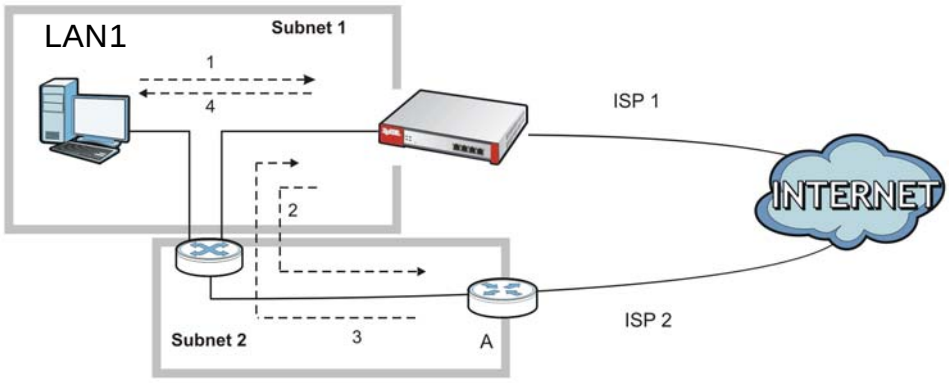
1 A computer on the LAN1 initiates a connection by sending a SYN packet to a receiving server on the WAN.

2 The ZyWALL reroutes the packet to gateway **A**, which is in **Subnet 2**.

3 The reply from the WAN goes to the ZyWALL.

4 The ZyWALL then sends it to the computer on the LAN1 in **Subnet 1**.

**Figure 236** Using Virtual Interfaces to Avoid Asymmetrical Routes



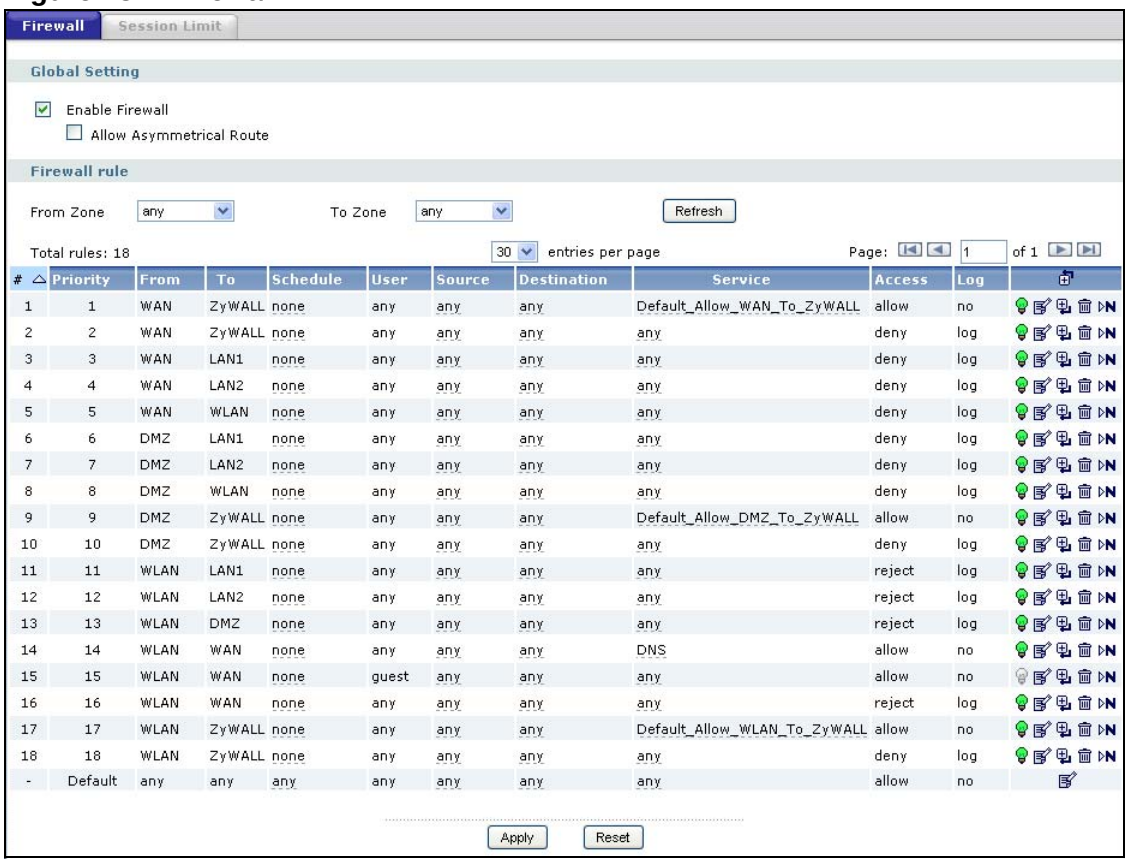

## 20.2.1 Configuring the Firewall Screen

Click **Firewall** to open the **Firewall** screen. Use this screen to enable or disable the firewall and asymmetrical routes, set a maximum number of sessions per host, and display the configured firewall rules. Specify from which zone packets come and to which zone packets travel to display only the rules specific to the selected direction. Note the following.

- If you enable intra-zone traffic blocking (see the chapter about zones), the firewall automatically creates (implicit) rules to deny packet passage between the interfaces in the specified zone.
- Besides configuring the firewall, you also need to configure virtual servers (NAT port forwarding) to allow computers on the WAN to access LAN devices. See Chapter 16 on page 309 for more information.
- The ZyWALL applies virtual server (Destination NAT) settings before applying the firewall rules. So for example, if you configure a virtual server that sends WAN traffic to a LAN IP address, when you configure a corresponding firewall rule to allow the traffic, you need to set the LAN IP address as the destination. See Section 6.8 on page 137 for an example.
- The ordering of your rules is very important as rules are applied in sequence.

- Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

**Figure 237** Firewall




The following table describes the labels in this screen.

**Table 116** Firewall

| LABEL | DESCRIPTION |
|---|---|
| Global Setting | |
| Enable Firewall | Select this check box to activate the firewall. The ZyWALL performs access control when the firewall is activated. |
| Allow Asymmetrical Route | If an alternate gateway on the LAN has an IP address in the same subnet as the ZyWALL's LAN IP address, return traffic may not go through the ZyWALL. This is called an asymmetrical or "triangle" route. This causes the ZyWALL to reset the connection, as the connection has not been acknowledged.<br><br>Select this check box to have the ZyWALL permit the use of asymmetrical route topology on the network (not reset the connection).<br><br>Note: Allowing asymmetrical routes may let traffic from the WAN go directly to the LAN without passing through the ZyWALL. A better solution is to use virtual interfaces to put the ZyWALL and the backup gateway on separate subnets. |

**Table 116** Firewall (continued)

| LABEL | DESCRIPTION |
|---|---|
| From Zone<br><br>To Zone | This is the direction of travel of packets. Select from which zone the packets come and to which zone they go.<br><br>Firewall rules are grouped based on the direction of travel of packets to which they apply. For example, from **LAN1** to **LAN1** means packets traveling from a computer or subnet on the LAN to either another computer or subnet on the LAN1.<br><br>From **any** displays all the firewall rules for traffic going to the selected **To Zone**.<br><br>To **any** displays all the firewall rules for traffic coming from the selected **From Zone**.<br><br>From **any** to **any** displays all of the firewall rules.<br><br>To **ZyWALL** rules are for traffic that is destined for the ZyWALL and control which computers can manage the ZyWALL. |
| The following read-only fields summarize the rules you have created that apply to traffic traveling in the selected packet direction. | |
| Total Rules | This field displays the total number of firewall rules. |
| entries per page | Select how many entries you want to display on each page. |
| Page x of x | This is the number of the page of entries currently displayed and the total number of pages of entries. Type a page number to go to or use the arrows to navigate the pages of entries. |
| # | This is the index number of your firewall rule. It is not associated with a specific rule.<br><br>The entry with a hyphen (-) instead of a number is the default firewall behavior that the ZyWALL performs on traffic that does not match any other traffic direction. Only the access right and log alert are configurable for the default firewall rule. To apply other behavior, configure a firewall rule that traffic will match so the ZyWALL will not have to use its default behavior. |
| Priority | This is the position of your firewall rule in the global rule list (including all through-ZyWALL and to-ZyWALL rules). The ordering of your rules is important as rules are applied in sequence. Default displays for the default firewall behavior that the ZyWALL performs on traffic that does not match any other traffic direction. The ZyWALL checks the traffic against any other applicable rules before applying this default behavior. |
| Schedule | This field tells you the schedule object that the rule uses. **none** means the rule is active at all times if enabled. |
| User | This is the user name or user group name to which this firewall rule applies. |
| Source | This displays the source address object to which this firewall rule applies. |
| Destination | This displays the destination address object to which this firewall rule applies. |
| Service | This displays the service object to which this firewall rule applies. |

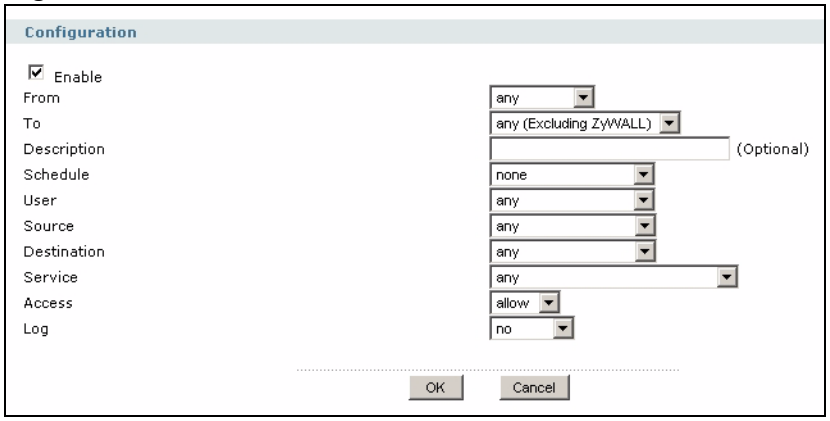
**Table 116** Firewall (continued)

| LABEL | DESCRIPTION |
|---|---|
| Access | This field displays whether the firewall silently discards packets (**deny**), discards packets and sends a TCP reset packet to the sender (**reject**) or permits the passage of packets (**allow**). |
| Log | This field shows you whether a log (and alert) is created when packets match this rule or not. |
| Add icon | Click the **Add** icon in the heading row to add a new first entry.<br><br>The **Active** icon displays whether the rule is enabled or not. Click it to activate or deactivate the rule. Make sure you click **Apply** to save and apply the change.<br><br>Click the **Edit** icon to go to the screen where you can edit the rule on the ZyWALL.<br><br>Click the **Add** icon in an entry to add a rule below the current entry.<br><br>Click the **Remove** icon to delete an existing rule from the ZyWALL. A window displays asking you to confirm that you want to delete the rule. Note that subsequent firewall rules move up by one when you take this action.<br><br>In a numbered list, click the **Move to N** icon to display a field to type an index number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed. For example, if you type 6, the rule you are moving becomes number 6 and the previous rule 6 (if there is one) gets pushed up (or down) one.<br><br>The ordering of your rules is important as they are applied in order of their numbering. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 20.2.2 The Firewall Edit Screen

In the **Firewall** screen, click the **Edit** or **Add** icon to display the **Firewall Rule Edit** screen. Refer to the following table for information on the labels.

**Figure 238** Firewall > Edit



The following table describes the labels in this screen.

**Table 117** Firewall > Edit

| LABEL | DESCRIPTION |
|---|---|
| Enable | Select this check box to activate the firewall rule. |
| From<br><br>To | For through-ZyWALL rules, select the direction of travel of packets to which the rule applies.<br><br>**any** means all interfaces or VPN tunnels.<br><br>**ZyWALL** means packets destined for the ZyWALL itself. |
| Description | Enter a descriptive name of up to 60 printable ASCII characters for the firewall rule. Spaces are allowed. |
| Schedule | Select a schedule that defines when the rule applies or select **Create Object** to configure a new one (see Chapter 40 on page 677 for details). Otherwise, select **none** and the rule is always effective. |
| User | This field is not available when you are configuring a to-ZyWALL rule.<br><br>Select a user name or user group to which to apply the rule. Select **Create Object** to configure a new user account (see Section 37.2.1 on page 652 for details). The firewall rule is activated only when the specified user logs into the system and the rule will be disabled when the user logs out.<br><br>Otherwise, select **any** and there is no need for user logging.<br><br>Note: If you specified a source IP address (group) instead of **any** in the field below, the user's IP address should be within the IP address range. |
| Source | Select a source address or address group for whom this rule applies. Select **Create Object** to configure a new one. Select **any** if the policy is effective for every source. |
| Destination | Select a destination address or address group for whom this rule applies. Select **Create Object** to configure a new one. Select **any** if the policy is effective for every destination. |
| Service | Select a service or service group from the drop-down list box. Select **Create Object** to add a new service. See Chapter 39 on page 671 for more information. |
| Access | Use the drop-down list box to select what the firewall is to do with packets that match this rule.<br><br>Select **deny** to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender.<br><br>Select **reject** to deny the packets and send a TCP reset packet to the sender. Any UDP packets are dropped without sending a response packet.<br><br>Select **allow** to permit the passage of the packets. |
| Log | Select whether to have the ZyWALL generate a log (**log**), log and alert (**log alert**) or not (**no**) when the rule is matched. See Chapter 47 on page 793 for more on logs. |

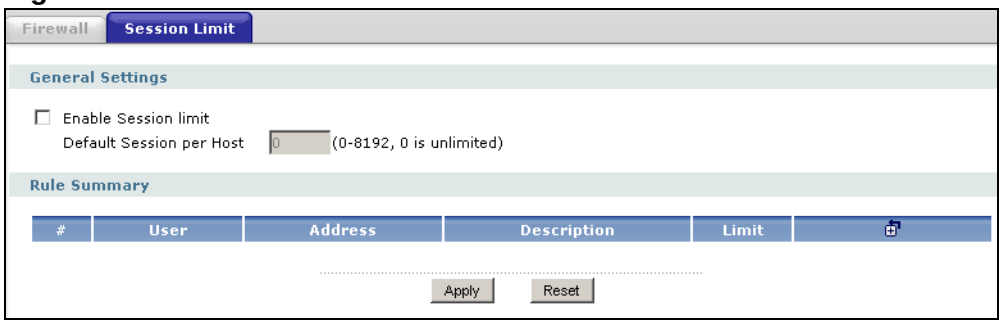
**Table 117** Firewall > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| OK | Click **OK** to save your customized settings and exit this screen. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# 20.3 The Session Limit Screen

Click **Firewall > Session Limit** to display the **Firewall Session Limit** screen. Use this screen to limit the number of concurrent NAT/firewall sessions a client can use. You can apply a default limit for all users and individual limits for specific users, addresses, or both. The individual limit takes priority if you apply both.

**Figure 239** Firewall > Session Limit




The following table describes the labels in this screen.

**Table 118** Firewall > Session Limit

| LABEL | DESCRIPTION |
|---|---|
| General Settings | |
| Enable Session limit | Select this check box to control the number of concurrent sessions hosts can have. |
| Default Session per Host | Use this field to set a common limit to the number of concurrent NAT/ firewall sessions each client computer can have.<br><br>If only a few clients use peer to peer applications, you can raise this number to improve their performance. With heavy peer to peer application use, lower this number to ensure no single client uses too many of the available NAT sessions.<br><br>Create rules below to apply other limits for specific users or addresses. |
| Rule Summary | This table lists the rules for limiting the number of concurrent sessions hosts can have. |
| # | This is the index number of a session limit rule. It is not associated with a specific rule. |
| User | This is the user name or user group name to which this session limit rule applies. |

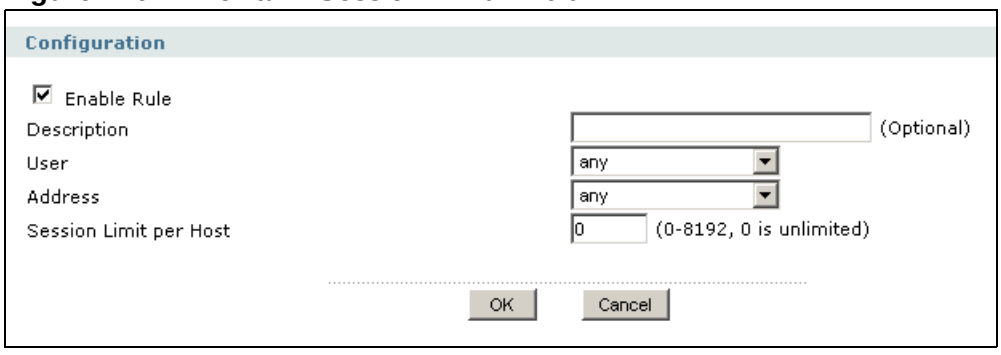
**Table 118** Firewall > Session Limit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Address | This is the address object to which this session limit rule applies. |
| Limit | This is how many concurrent sessions this user or address is allowed to have. |
| Add icon | Click the **Add** icon in the heading row to add a new first entry.<br>The **Active** icon displays whether the rule is enabled or not. Click it to activate or deactivate the rule. Make sure you click **Apply** to save and apply the change.<br>Click the **Edit** icon to go to the screen where you can edit the rule on the ZyWALL.<br>Click the **Add** icon in an entry to add a rule below the current entry.<br>Click the **Remove** icon to delete an existing rule from the ZyWALL. A window displays asking you to confirm that you want to delete the rule. Note that subsequent rules move up by one when you take this action.<br>In a numbered list, click the **Move to N** icon to display a field to type an index number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed. For example, if you type 6, the rule you are moving becomes number 6 and the previous rule 6 (if there is one) gets pushed up (or down) one.<br>The ordering of your rules is important as they are applied in order of their numbering. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 20.3.1 The Session Limit Edit Screen

Click **Firewall > Session Limit** and the **Add** or **Edit** icon to display the **Firewall Session Limit Edit** screen. Use this screen to configure rules that define a session limit for specific users or addresses.

**Figure 240** Firewall > Session Limit > Edit



The following table describes the labels in this screen.

**Table 119** Firewall > Session Limit > Edit

| LABEL | DESCRIPTION |
|---|---|
| Enable Rule | Select this check box to turn on this session limit rule. |
| Description | Enter information to help you identify this rule. Use up to 64 printable ASCII characters. Spaces are allowed. |
| User | Select a user name or user group to which to apply the rule. Select **Create Object** to configure a new user account (see Section 37.2.1 on page 652 for details). The rule is activated only when the specified user logs into the system and the rule will be disabled when the user logs out.<br><br>Otherwise, select **any** and there is no need for user logging.<br><br>Note: If you specified an IP address (or address group) instead of **any** in the field below, the user's IP address should be within the IP address range. |
| Address | Select a source address or address group for whom this rule applies. Select **Create Object** to configure a new one. Select **any** if the policy is effective for every source address. |
| Session Limit per Host | Use this field to set a limit to the number of concurrent NAT/firewall sessions this rule's users or addresses can have.<br><br>For this rule's users and addresses, this setting overrides the **Default Session per Host** setting in the general **Firewall Session Limit** screen. |
| OK | Click **OK** to save your customized settings and exit this screen. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# PART IV
# VPN

# 21

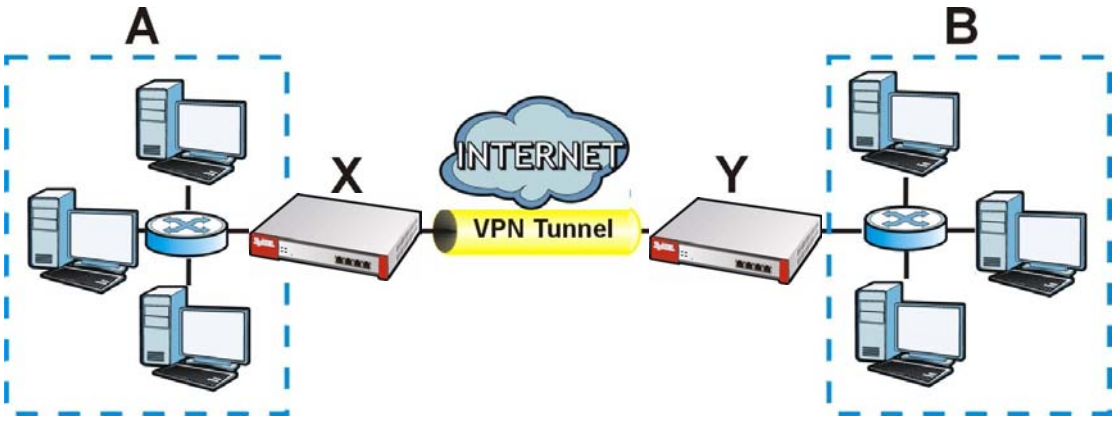
# IPSec VPN

## 21.1 IPSec VPN Overview

A virtual private network (VPN) provides secure communications between sites without the expense of leased site-to-site lines. A secure VPN is a combination of tunneling, encryption, authentication, access control and auditing. It is used to transport traffic over the Internet or any insecure network that uses TCP/IP for communication.

Internet Protocol Security (IPSec) is a standards-based VPN that offers flexible solutions for secure data communications across a public network like the Internet. IPSec is built around a number of standardized cryptographic techniques to provide confidentiality, data integrity and authentication at the IP layer. The following figure is an example of an IPSec VPN tunnel.

**Figure 241** IPSec VPN Example




The VPN tunnel connects the ZyWALL (**X**) and the remote (peer) IPSec router (**Y**). These routers then connect the local network (**A**) and remote network (**B**).

### 21.1.1 What You Can Do in the IPSec VPN Screens

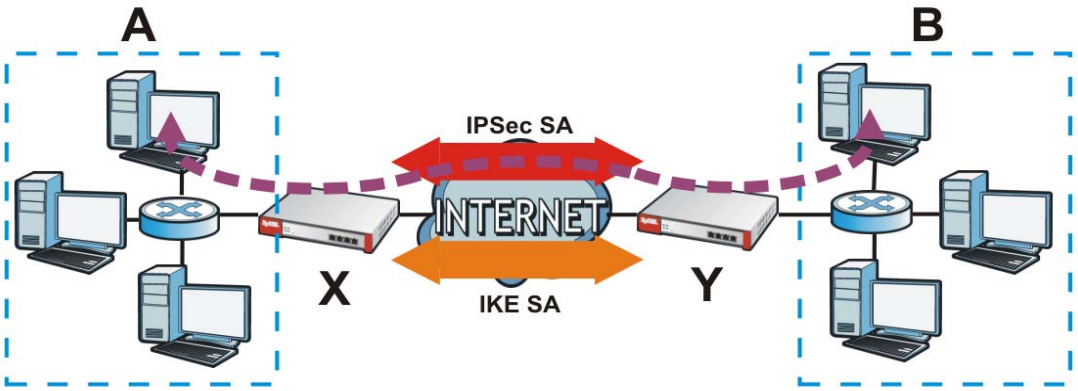
- Use the **VPN Connection** screens (see Section 21.2 on page 366) to specify which VPN gateway a VPN connection policy uses and which devices (behind the IPSec routers) can use the VPN tunnel and the IPSec SA settings (phase 2 settings). You can also activate / deactivate and connect / disconnect each VPN connection (each IPSec SA).

- Use the **VPN Gateway** screens (see Section 21.2.1 on page 368) to manage the ZyWALL's VPN gateways. A VPN gateway specifies the IPSec routers at either end of a VPN tunnel and the IKE SA settings (phase 1 settings). You can also activate and deactivate each VPN gateway.
- Use the **VPN Concentrator** screens (see Section 21.4 on page 388) to combine several IPSec VPN connections into a single secure network.
- Use the **SA Monitor** screen (see Section 21.5 on page 391) to display and manage the active IPSec SAs.

## 21.1.2 What You Need to Know About IPSec VPN

An IPSec VPN tunnel is usually established in two phases. Each phase establishes a security association (SA), a contract indicating what security parameters the ZyWALL and the remote IPSec router will use. The first phase establishes an Internet Key Exchange (IKE) SA between the ZyWALL and remote IPSec router. The second phase uses the IKE SA to securely establish an IPSec SA through which the ZyWALL and remote IPSec router can send data between computers on the local network and remote network. This is illustrated in the following figure.

**Figure 242** VPN: IKE SA and IPSec SA

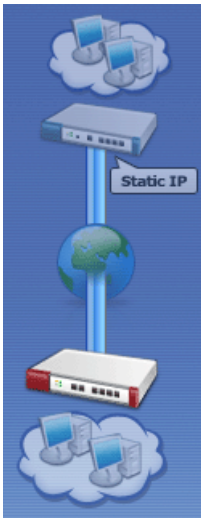
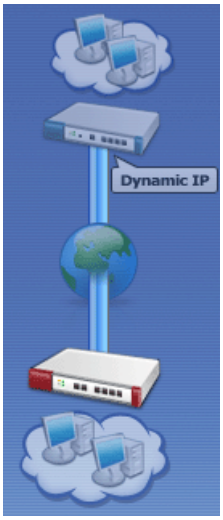



In this example, a computer in network **A** is exchanging data with a computer in network **B**. Inside networks **A** and **B**, the data is transmitted the same way data is normally transmitted in the networks. Between routers **X** and **Y**, the data is protected by tunneling, encryption, authentication, and other security features of the IPSec SA. The IPSec SA is secure because routers **X** and **Y** established the IKE SA first.

## Application Scenarios

The ZyWALL's application scenarios make it easier to configure your VPN connection settings.

**Table 120** IPSec VPN Application Scenarios

| SITE-TO-SITE | SITE-TO-SITE WITH DYNAMIC PEER | REMOTE ACCESS (SERVER ROLE) | REMOTE ACCESS (CLIENT ROLE) |
|---|---|---|---|
|  |  |  |  |
| Choose this if the remote IPSec router has a static IP address or a domain name.<br><br>This ZyWALL can initiate the VPN tunnel.<br><br>The remote IPSec router can also initiate the VPN tunnel if this ZyWALL has a static IP address or a domain name. | Choose this if the remote IPSec router has a dynamic IP address.<br><br>You don't specify the remote IPSec router's address, but you specify the remote policy (the addresses of the devices behind the remote IPSec router).<br><br>This ZyWALL must have a static IP address or a domain name.<br><br>Only the remote IPSec router can initiate the VPN tunnel. | Choose this to allow incoming connections from IPSec VPN clients.<br><br>The clients have dynamic IP addresses and are also known as dial-in users.<br><br>You don't specify the addresses of the client IPSec routers or the remote policy.<br><br>This creates a dynamic IPSec VPN rule that can let multiple clients connect.<br><br>Only the clients can initiate the VPN tunnel. | Choose this to connect to an IPSec server.<br><br>This ZyWALL is the client (dial-in user).<br><br>Client role ZyWALLs initiate IPSec VPN connections to a server role ZyWALL.<br><br>This ZyWALL can have a dynamic IP address.<br><br>The IPSec server doesn't configure this ZyWALL's IP address or the addresses of the devices behind it.<br><br>Only this ZyWALL can initiate the VPN tunnel. |

## Finding Out More

- See Section 5.4.4 on page 88 for related information on these screens.

- See Section 21.6 on page 392 for IPSec VPN background information.
- See Section 6.5 on page 123 for an example of configuring IPSec VPN.

### 21.1.3 Before You Begin

This section briefly explains the relationship between VPN tunnels and other features. It also gives some basic suggestions for troubleshooting.

You should set up the following features before you set up the VPN tunnel.

- In any VPN connection, you have to select address objects to specify the local policy and remote policy. You should set up the address objects first.
- In a VPN gateway, you can select an Ethernet interface, virtual Ethernet interface, VLAN interface, or virtual VLAN interface to specify what address the ZyWALL uses as its IP address when it establishes the IKE SA. You should set up the interface first. See Chapter 10 on page 181.
- In a VPN gateway, you can enable extended authentication. If the ZyWALL is in server mode, you should set up the authentication method (AAA server) first. The authentication method specifies how the ZyWALL authenticates the remote IPSec router. See Chapter 41 on page 683.
- In a VPN gateway, the ZyWALL and remote IPSec router can use certificates to authenticate each other. Make sure the ZyWALL and the remote IPSec router will trust each other's certificates. See Chapter 43 on page 699.

## 21.2 The VPN Connection Screen

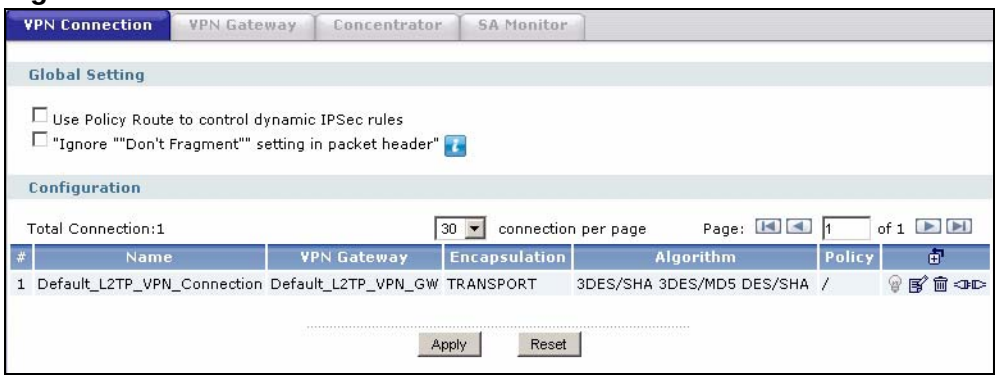
Click **VPN** > **IPSec VPN** to open the **VPN Connection** screen. The **VPN Connection** screen lists the VPN connection policies and their associated VPN gateway(s), and various settings. In addition, it also lets you activate / deactivate and connect / disconnect each VPN connection (each IPSec SA). Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

Note: Except for dynamic IPSec VPN rules, each VPN connection requires a corresponding policy route.

Dynamic IPSec VPN rules only require a corresponding policy route if you select **Use Policy Route to control dynamic IPSec rules**.

The VPN wizard automatically creates a corresponding policy route. If you create the VPN connection in the **VPN > IPSec VPN** screens, you need to manually create a corresponding policy route.

**Figure 243** VPN > IPSec VPN > VPN Connection




Each field is discussed in the following table. See Section 21.2.2 on page 375 and Section 21.2.1 on page 368 for more information.

**Table 121** VPN > IPSec VPN > VPN Connection

| LABEL | DESCRIPTION |
|---|---|
| Use Policy Route to control dynamic IPSec rules | Leave this cleared to have the ZyWALL automatically obtain source and destination addresses for dynamic IPSec rules. When you leave this option's check box cleared, you do not need to configure policy routes for the dynamic IPSec tunnels.<br><br>Only select this if you want to use policy routes to manually specify the destination addresses of dynamic IPSec rules. You must configure a policy route for each dynamic IPSec tunnel. |
| Ignore ""Don't Fragment"" setting in packet header | Select this to fragment packets larger than the MTU (Maximum Transmission Unit) that have the "don't" fragment" bit in the header turned on. When you clear this the ZyWALL drops packets larger than the MTU that have the "don't" fragment" bit in the header turned on. |
| Total Connection | This field displays the total number of VPN connection policies. |
| connection per page | Select how many entries you want to display on each page. |
| Page x of x | This is the number of the page of entries currently displayed and the total number of pages of entries. Type a page number to go to or use the arrows to navigate the pages of entries. |
| # | This field is a sequential value, and it is not associated with a specific connection. |
| Name | This field displays the name of the IPSec SA. |
| VPN Gateway | This field displays the associated VPN gateway(s). If there is no VPN gateway, this field displays "manual key". |
| Encapsulation | This field displays what encapsulation the IPSec SA uses. |
| Algorithm | This field displays what encryption and authentication methods, respectively, the IPSec SA uses. |

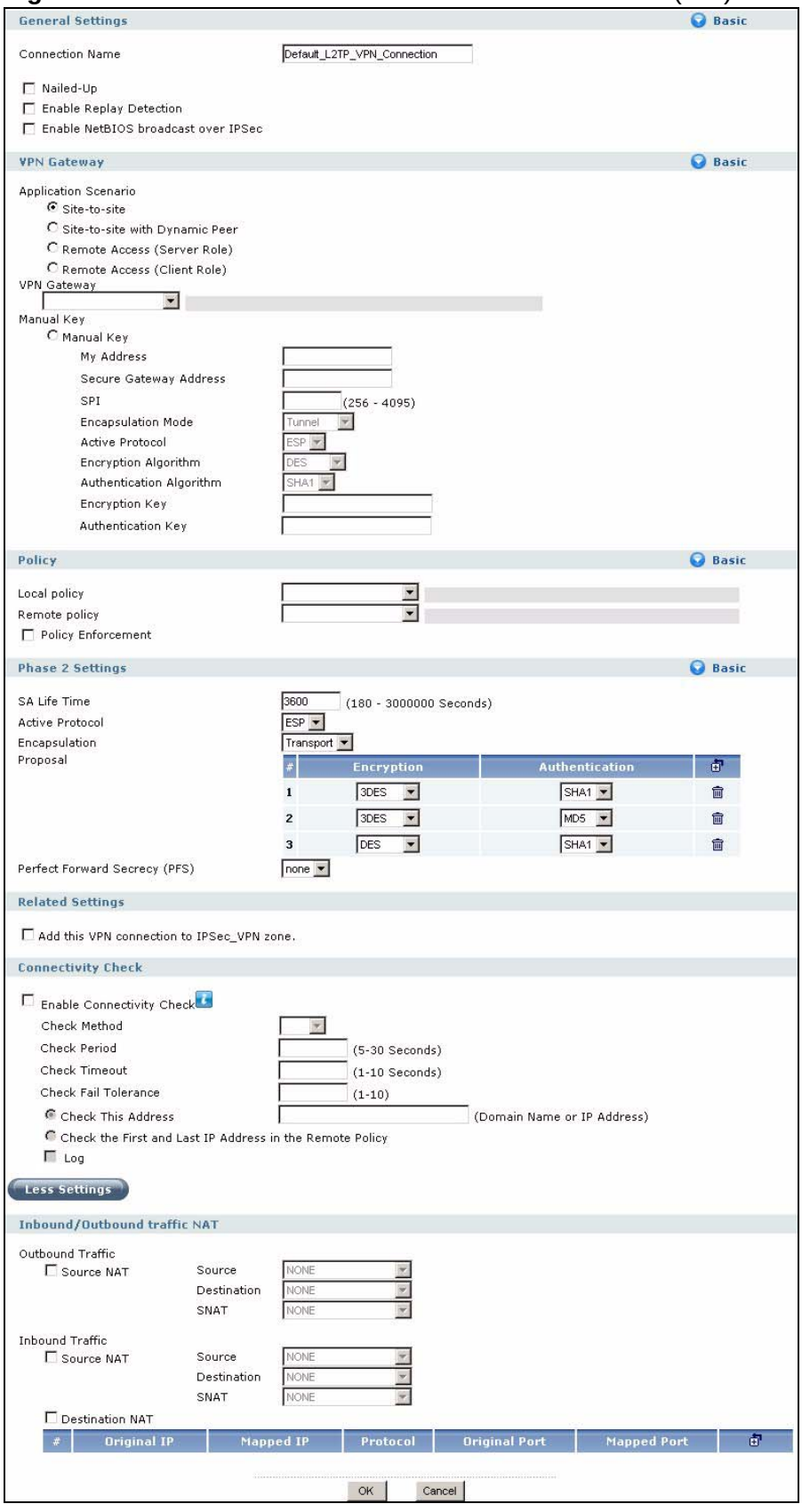
**Table 121** VPN > IPSec VPN > VPN Connection (continued)

| LABEL | DESCRIPTION |
|---|---|
| Policy | This field displays the local policy and the remote policy, respectively. |
| Add icon | This column provides icons to add, edit, and remove VPN connections, as well as to activate / deactivate and connect / disconnect VPN connections.<br><br>To add a VPN connection, click the **Add** icon at the top of the column. The **VPN Connection Add / Edit Manual** screen appears.<br><br>To edit a VPN connection, click the **Edit** icon next to the connection. The **VPN Connection Add / Edit Manual** or **VPN Connection Add / Edit Gateway** screen appears accordingly.<br><br>To delete a VPN connection, click the **Remove** icon next to the connection. The Web Configurator confirms that you want to delete the VPN connection.<br><br>To activate or deactivate an IPSec SA, click the **Active** icon next to the VPN connection. Make sure you click **Apply** to save and apply the change.<br><br>To connect or disconnect an IPSec SA, click the **Connect** icon next to the VPN connection. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 21.2.1 The VPN Connection Add/Edit (IKE) Screen

The **VPN Connection Add / Edit Gateway** screen allows you to create a new VPN connection policy or edit an existing one. To access this screen, go to the **VPN Connection** screen (see Section 21.2 on page 366), and click either the **Add** icon or an **Edit** icon. If you click the **Add** icon, you have to select a specific VPN gateway in the **VPN Gateway** field before the following screen appears.

**Figure 244** VPN > IPSec VPN > VPN Connection > Edit (IKE)



Each field is described in the following table.

**Table 122** VPN > IPSec VPN > VPN Connection > Edit

| LABEL | DESCRIPTION |
|---|---|
| General Settings | Click **Advanced** to display more settings. Click **Basic** to display fewer settings. |
| Connection Name | Type the name used to identify this IPSec SA. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| Nailed-Up | Select this if you want the ZyWALL to automatically renegotiate the IPSec SA when the SA life time expires. |
| Enable Replay Detection | Select this check box to detect and reject old or duplicate packets to protect against Denial-of-Service attacks. |
| Enable NetBIOS Broadcast over IPSec | Select this check box if you the ZyWALL to send NetBIOS (Network Basic Input/Output System) packets through the IPSec SA.<br><br>NetBIOS packets are TCP or UDP packets that enable a computer to connect to and communicate with a LAN. It may sometimes be necessary to allow NetBIOS packets to pass through IPSec SAs in order to allow local computers to find computers on the remote network and vice versa. |
| VPN Gateway | Click **Advanced** to display more settings. Click **Basic** to display fewer settings. |
| Application Scenario | Select the scenario that best describes your intended VPN connection.<br><br>**Site-to-site** - Choose this if the remote IPSec router has a static IP address or a domain name. This ZyWALL can initiate the VPN tunnel.<br><br>**Site-to-site with Dynamic Peer** - Choose this if the remote IPSec router has a dynamic IP address. Only the remote IPSec router can initiate the VPN tunnel.<br><br>**Remote Access (Server Role)** - Choose this to allow incoming connections from IPSec VPN clients. The clients have dynamic IP addresses and are also known as dial-in users. Only the clients can initiate the VPN tunnel.<br><br>**Remote Access (Client Role)** - Choose this to connect to an IPSec server. This ZyWALL is the client (dial-in user) and can initiate the VPN tunnel. |
| VPN Gateway | Select the VPN gateway this VPN connection is to use or select **Create Object** to add another VPN gateway for this VPN connection to use. |
| Manual Key | Select this option to configure a VPN connection policy that uses a manual key instead of IKE key management. This may be useful if you have problems with IKE key management. See Section 21.2.2 on page 375 for how to configure the manual key fields.<br><br>Note: Only use manual key as a temporary solution, because it is not as secure as a regular IPSec SA. |
| Policy | Click **Advanced** to display more settings. Click **Basic** to display fewer settings. |
| Local Policy | Select the address or address group corresponding to the local network. Select **Create Object** to configure a new one. |

**Table 122** VPN > IPSec VPN > VPN Connection > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Remote Policy | Select the address or address group corresponding to the remote network. Select **Create Object** to configure a new one. |
| Policy Enforcement | Clear this to allow traffic with source and destination IP addresses that do not match the local and remote policy to use the VPN tunnel. Leave this cleared for free access between the local and remote networks.<br><br>Note: Clear this to use the IPSec SA in a VPN concentrator.<br><br>Selecting this restricts who can use the VPN tunnel. The ZyWALL drops traffic with source and destination IP addresses that do not match the local and remote policy. |
| Phase 2 Settings | Click **Advanced** to display more settings. Click **Basic** to display fewer settings. |
| SA Life Time | Type the maximum number of seconds the IPSec SA can last. Shorter life times provide better security. The ZyWALL automatically negotiates a new IPSec SA before the current one expires, if there are users who are accessing remote resources. |
| Active Protocol | Select which protocol you want to use in the IPSec SA. Choices are:<br><br>**AH** (RFC 2402) - provides integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not encryption. If you select **AH**, you must select an **Authentication** algorithm.<br><br>**ESP** (RFC 2406) - provides encryption and the same services offered by **AH**, but its authentication is weaker. If you select **ESP**, you must select an **Encryption** algorithm and **Authentication** algorithm.<br><br>Both **AH** and **ESP** increase processing requirements and latency (delay).<br><br>The ZyWALL and remote IPSec router must use the same active protocol. |
| Encapsulation | Select which type of encapsulation the IPSec SA uses. Choices are<br><br>**Tunnel** - this mode encrypts the IP header information and the data.<br><br>**Transport** - this mode only encrypts the data.<br><br>The ZyWALL and remote IPSec router must use the same encapsulation. |
| Proposal | |
| # | This field is a sequential value, and it is not associated with a specific proposal. The sequence of proposals should not affect performance significantly. |

**Table 122** VPN > IPSec VPN > VPN Connection > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Encryption | This field is applicable when the **Active Protocol** is **ESP**. Select which key size and encryption algorithm to use in the IPSec SA. Choices are:<br><br>**NULL** - no encryption key or algorithm<br><br>**DES** - a 56-bit key with the DES encryption algorithm<br><br>**3DES** - a 168-bit key with the DES encryption algorithm<br><br>**AES128** - a 128-bit key with the AES encryption algorithm<br><br>**AES192** - a 192-bit key with the AES encryption algorithm<br><br>**AES256** - a 256-bit key with the AES encryption algorithm<br><br>The ZyWALL and the remote IPSec router must both have at least one proposal that uses use the same encryption and the same key.<br><br>Longer keys are more secure, but require more processing power, resulting in increased latency and decreased throughput. |
| Authentication | Select which hash algorithm to use to authenticate packet data in the IPSec SA. Choices are **SHA1** and **MD5**. **SHA1** is generally considered stronger than **MD5**, but it is also slower.<br><br>The ZyWALL and the remote IPSec router must both have a proposal that uses the same authentication algorithm. |
| Add icon | This column contains icons to add and remove proposals.<br><br>To add a proposal, click the **Add** icon at the top of the column.<br><br>To remove a proposal, click the **Remove** icon next to the proposal. The ZyWALL confirms that you want to delete it before doing so. |
| Perfect Forward Secrecy (PFS) | Select whether or not you want to enable Perfect Forward Secrecy (PFS) and, if you do, which Diffie-Hellman key group to use for encryption. Choices are:<br><br>**none** - disable PFS<br><br>**DH1** - enable PFS and use a 768-bit random number<br><br>**DH2** - enable PFS and use a 1024-bit random number<br><br>**DH5** - enable PFS and use a 1536-bit random number<br><br>PFS changes the root key that is used to generate encryption keys for each IPSec SA. The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. Both routers must use the same DH key group. |
| Related Settings | |
| Add this VPN connection to IPSec_VPN zone. | Select this check box to add the VPN connection policy to the IPSec_VPN security zone. Any security rules or settings configured for the IPSec_VPN security zone will also apply to this VPN connection policy. |
| Connectivity Check | The ZyWALL can regularly check the VPN connection to the gateway you specified to make sure it is still available. |

**Table 122** VPN > IPSec VPN > VPN Connection > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Enable Connectivity Check | Select this to turn on the VPN connection check. |
| Check Method | Select how the ZyWALL checks the connection. The peer must be configured to respond to the method you select.<br>Select **icmp** to have the ZyWALL regularly ping the address you specify to make sure traffic can still go through the connection. You may need to configure the peer to respond to pings.<br>Select **tcp** to have the ZyWALL regularly perform a TCP handshake with the address you specify to make sure traffic can still go through the connection. You may need to configure the peer to accept the TCP connection. |
| Check Port | This field displays when you set the **Check Method** to **tcp**. Specify the port number to use for a TCP connectivity check. |
| Check Period | Enter the number of seconds between connection check attempts. |
| Check Timeout | Enter the number of seconds to wait for a response before the attempt is a failure. |
| Check Fail Tolerance | Enter the number of consecutive failures allowed before the ZyWALL disconnects the VPN tunnel. The ZyWALL resumes using the first peer gateway address when the VPN connection passes the connectivity check. |
| Check this Address | Select this to specify a domain name or IP address for the connectivity check. Enter that domain name or IP address in the field next to it. |
| Check the First and Last IP Address in the Remote Policy | Select this to have the ZyWALL check the connection to the first and last IP addresses in the connection's remote policy. Make sure one of these is the peer gateway's LAN IP address. |
| Log | Select this to have the ZyWALL generate a log every time it checks this VPN connection. |
| More Settings/ Less Settings | Click this button to show or hide the **Inbound/Outbound traffic NAT** fields. |
| Inbound/ Outbound traffic NAT | |
| Outbound Traffic | |
| Source NAT | This translation hides the source address of computers in the local network. It may also be necessary if you want the ZyWALL to route packets from computers outside the local network through the IPSec SA. |
| Source | Select the address object that represents the original source address (or select **Create Object** to configure a new one). This is the address object for the computer or network outside the local network. The size of the original source address range (**Source**) must be equal to the size of the translated source address range (**SNAT**). |
| Destination | Select the address object that represents the original destination address (or select **Create Object** to configure a new one). This is the address object for the remote network. |

**Table 122** VPN > IPSec VPN > VPN Connection > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| SNAT | Select the address object that represents the translated source address (or select **Create Object** to configure a new one). This is the address object for the local network. The size of the original source address range (**Source**) must be equal to the size of the translated source address range (**SNAT**). |
| Inbound Traffic | |
| Source NAT | This translation hides the source address of computers in the remote network. |
| Source | Select the address object that represents the original source address (or select **Create Object** to configure a new one). This is the address object for the remote network. The size of the original source address range (**Source**) must be equal to the size of the translated source address range (**SNAT**). |
| Destination | Select the address object that represents the original destination address (or select **Create Object** to configure a new one). This is the address object for the local network. |
| SNAT | Select the address object that represents the translated source address (or select **Create Object** to configure a new one). This is the address that hides the original source address. The size of the original source address range (**Source**) must be equal to the size of the translated source address range (**SNAT**). |
| Destination NAT | This translation forwards packets (for example, mail) from the remote network to a specific computer (for example, the mail server) in the local network. |
| # | This field is a sequential value, and it is not associated with a specific NAT record. However, the order of records is the sequence in which conditions are checked and executed. |
| Original IP | Select the address object that represents the original destination address. This is the address object for the remote network. |
| Mapped IP | Select the address object that represents the desired destination address. For example, this is the address object for the mail server. |
| Protocol | Select the protocol required to use this translation. Choices are: **TCP**, **UDP**, or **All**. |
| Original Port | These fields are available if the protocol is **TCP** or **UDP**. Enter the original destination port or range of original destination ports. The size of the original port range must be the same size as the size of the mapped port range. |
| Mapped Port | These fields are available if the protocol is **TCP** or **UDP**. Enter the translated destination port or range of translated destination ports. The size of the original port range must be the same size as the size of the mapped port range. |

**Table 122** VPN > IPSec VPN > VPN Connection > Edit (continued)

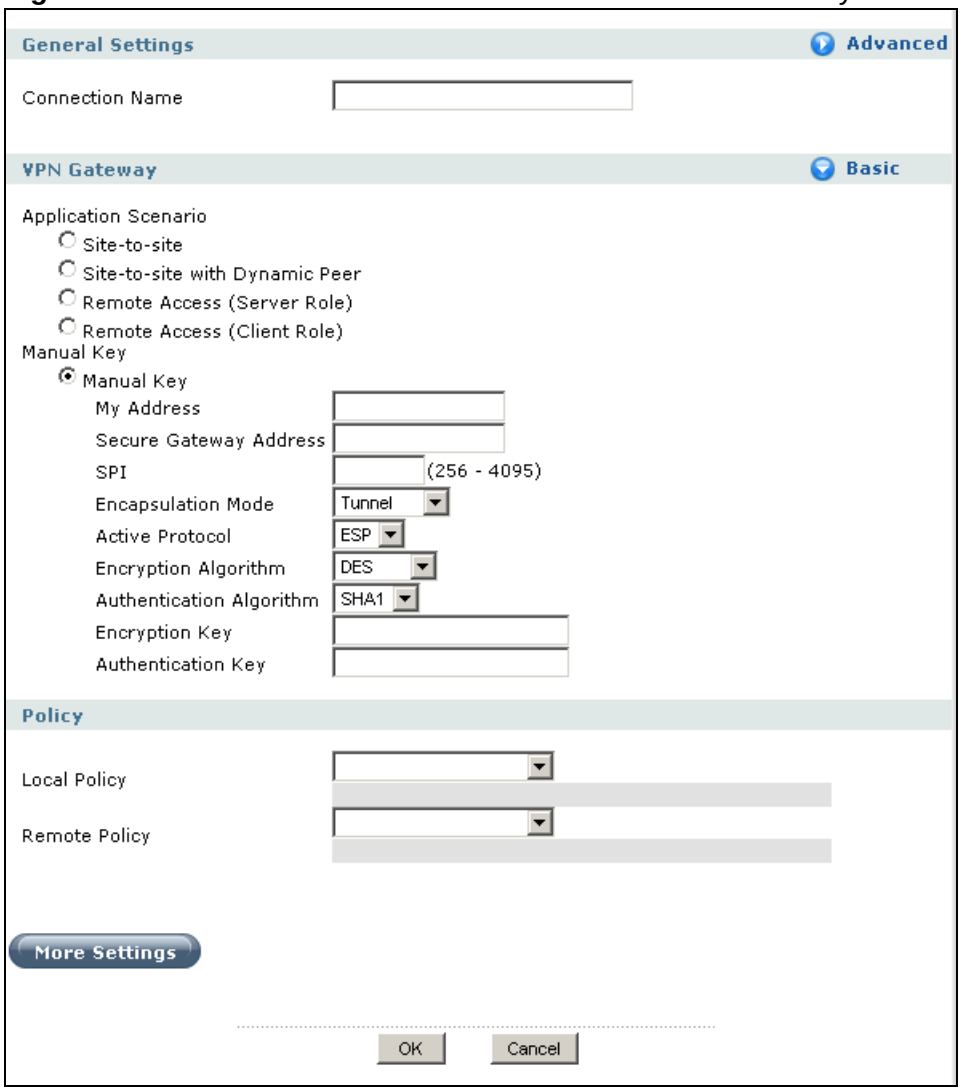
| LABEL | DESCRIPTION |
|---|---|
| Add icon | This column contains icons to add, move, and remove NAT records.<br>To add a NAT record, click the **Add** icon at the top of the column.<br>To move a NAT record, click the **Move to N** icon next to the record, and then type the row number to which you want to move it. The records are renumbered automatically.<br>To remove a NAT record, click the **Remove** icon next to the record. The ZyWALL confirms that you want to delete the NAT record before doing so. |
| OK | Click **OK** to save the changes. |
| Cancel | Click **Cancel** to discard all changes and return to the main VPN screen. |

## 21.2.2 The VPN Connection Add/Edit Manual Key Screen

The **VPN Connection Add/Edit Manual Key** screen allows you to create a new VPN connection or edit an existing one using a manual key. This is useful if you have problems with IKE key management. To access this screen, go to the **VPN Connection summary** screen (see Section 21.2 on page 366), and click either the **Add** icon or an existing manual key entry's **Edit** icon. In the VPN Gateway section of the screen, select **Manual Key**.

Note: Only use manual key as a temporary solution, because it is not as secure as a regular IPSec SA.

**Figure 245** VPN > IPSec VPN > VPN Connection > Manual Key > Edit




This table describes labels specific to manual key configuration. See Section 21.2 on page 366 for descriptions of the other fields.

**Table 123** VPN > IPSec VPN > VPN Connection > Manual Key > Edit

| LABEL | DESCRIPTION |
|---|---|
| Manual Key | |
| My Address | Type the IP address of the ZyWALL in the IPSec SA. 0.0.0.0 is invalid. |
| Secure Gateway Address | Type the IP address of the remote IPSec router in the IPSec SA. |
| SPI | Type a unique **SPI** (Security Parameter Index) between 256 and 4095. The SPI is used to identify the ZyWALL during authentication.<br><br>The ZyWALL and remote IPSec router must use the same SPI. |

**Table 123** VPN > IPSec VPN > VPN Connection > Manual Key > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Encapsulation Mode | Select which type of encapsulation the IPSec SA uses. Choices are<br>**Tunnel** - this mode encrypts the IP header information and the data<br>**Transport** - this mode only encrypts the data. You should only select this if the IPSec SA is used for communication between the ZyWALL and remote IPSec router.<br>If you select **Transport** mode, the ZyWALL automatically switches to **Tunnel** mode if the IPSec SA is not used for communication between the ZyWALL and remote IPSec router. In this case, the ZyWALL generates a log message for this change.<br>The ZyWALL and remote IPSec router must use the same encapsulation. |
| Active Protocol | Select which protocol you want to use in the IPSec SA. Choices are:<br>**AH** (RFC 2402) - provides integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not encryption. If you select **AH**, you must select an **Authentication Algorithm**.<br>**ESP** (RFC 2406) - provides encryption and the same services offered by **AH**, but its authentication is weaker. If you select **ESP**, you must select an **Encryption Algorithm** and **Authentication Algorithm**.<br>The ZyWALL and remote IPSec router must use the same protocol. |
| Encryption Algorithm | This field is applicable when the **Active Protocol** is **ESP**. Select which key size and encryption algorithm to use in the IPSec SA. Choices are:<br>**NULL** - no encryption key or algorithm<br>**DES** - a 56-bit key with the DES encryption algorithm<br>**3DES** - a 168-bit key with the DES encryption algorithm<br>**AES128** - a 128-bit key with the AES encryption algorithm<br>**AES192** - a 192-bit key with the AES encryption algorithm<br>**AES256** - a 256-bit key with the AES encryption algorithm<br>The ZyWALL and the remote IPSec router must use the same algorithm and key. Longer keys require more processing power, resulting in increased latency and decreased throughput. |
| Authentication Algorithm | Select which hash algorithm to use to authenticate packet data in the IPSec SA. Choices are **SHA1** and **MD5**. **SHA1** is generally considered stronger than **MD5**, but it is also slower.<br>The ZyWALL and remote IPSec router must use the same algorithm. |

**Table 123** VPN > IPSec VPN > VPN Connection > Manual Key > Edit (continued)

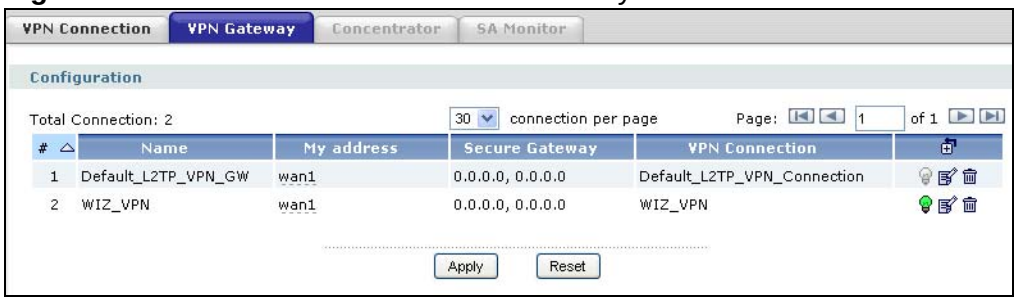
| LABEL | DESCRIPTION |
|---|---|
| Encryption Key | This field is applicable when you select an **Encryption Algorithm**. Enter the encryption key, which depends on the encryption algorithm.<br><br>**DES** - type a unique key 8-32 characters long<br><br>**3DES** - type a unique key 24-32 characters long<br><br>**AES128** - type a unique key 16-32 characters long<br><br>**AES192** - type a unique key 24-32 characters long<br><br>**AES256** - type a unique key 32 characters long<br><br>You can use any alphanumeric characters or ,;\|`~!@#$%^&*()_+\{}':./<>=-".<br><br>If you want to enter the key in hexadecimal, type “0x” at the beginning of the key. For example, "0x0123456789ABCDEF" is in hexadecimal format; in “0123456789ABCDEF” is in ASCII format. If you use hexadecimal, you must enter twice as many characters as listed above.<br><br>The remote IPSec router must have the same encryption key.<br><br>The ZyWALL ignores any characters above the minimum number of characters required by the algorithm. For example, if you enter 1234567890XYZ for a DES encryption key, the ZyWALL only uses 12345678. The ZyWALL still stores the longer key. |
| Authentication Key | Enter the authentication key, which depends on the authentication algorithm.<br><br>**MD5** - type a unique key 16-20 characters long<br><br>**SHA1** - type a unique key 20 characters long<br><br>You can use any alphanumeric characters or ,;\|`~!@#$%^&*()_+\{}':./<>=-". If you want to enter the key in hexadecimal, type “0x” at the beginning of the key. For example, "0x0123456789ABCDEF" is in hexadecimal format; in “0123456789ABCDEF” is in ASCII format. If you use hexadecimal, you must enter twice as many characters as listed above.<br><br>The remote IPSec router must have the same authentication key.<br><br>The ZyWALL ignores any characters above the minimum number of characters required by the algorithm. For example, if you enter 12345678901234567890 for a MD5 authentication key, the ZyWALL only uses 1234567890123456. The ZyWALL still stores the longer key. |
| OK | Click **OK** to save your settings and exit this screen. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# 21.3 The VPN Gateway Screen

The **VPN Gateway** summary screen displays the IPSec VPN gateway policies in the ZyWALL, as well as the ZyWALL's address, remote IPSec router's address, and associated VPN connections for each one. In addition, it also lets you activate and deactivate each VPN gateway.

To access this screen, click **VPN** > **Network** > **IPSec VPN** > **VPN Gateway**. The following screen appears.

**Figure 246** VPN > IPSec VPN > VPN Gateway




Each field is discussed in the following table. See Section 21.3.1 on page 380 for more information.

**Table 124** VPN > IPSec VPN > VPN Gateway

| LABEL | DESCRIPTION |
|---|---|
| Total Connection | This field displays the total number of VPN gateway policies. |
| connection per page | Select how many entries you want to display on each page. |
| Page x of x | This is the number of the page of entries currently displayed and the total number of pages of entries. Type a page number to go to or use the arrows to navigate the pages of entries. |
| # | This field is a sequential value, and it is not associated with a specific VPN gateway. |
| Name | This field displays the name of the VPN gateway |
| My address | This field displays the interface or a domain name the ZyWALL uses for the VPN gateway. |
| Secure Gateway | This field displays the IP address(es) of the remote IPSec routers. |
| VPN Connection | This field displays VPN connections that use this VPN gateway. |

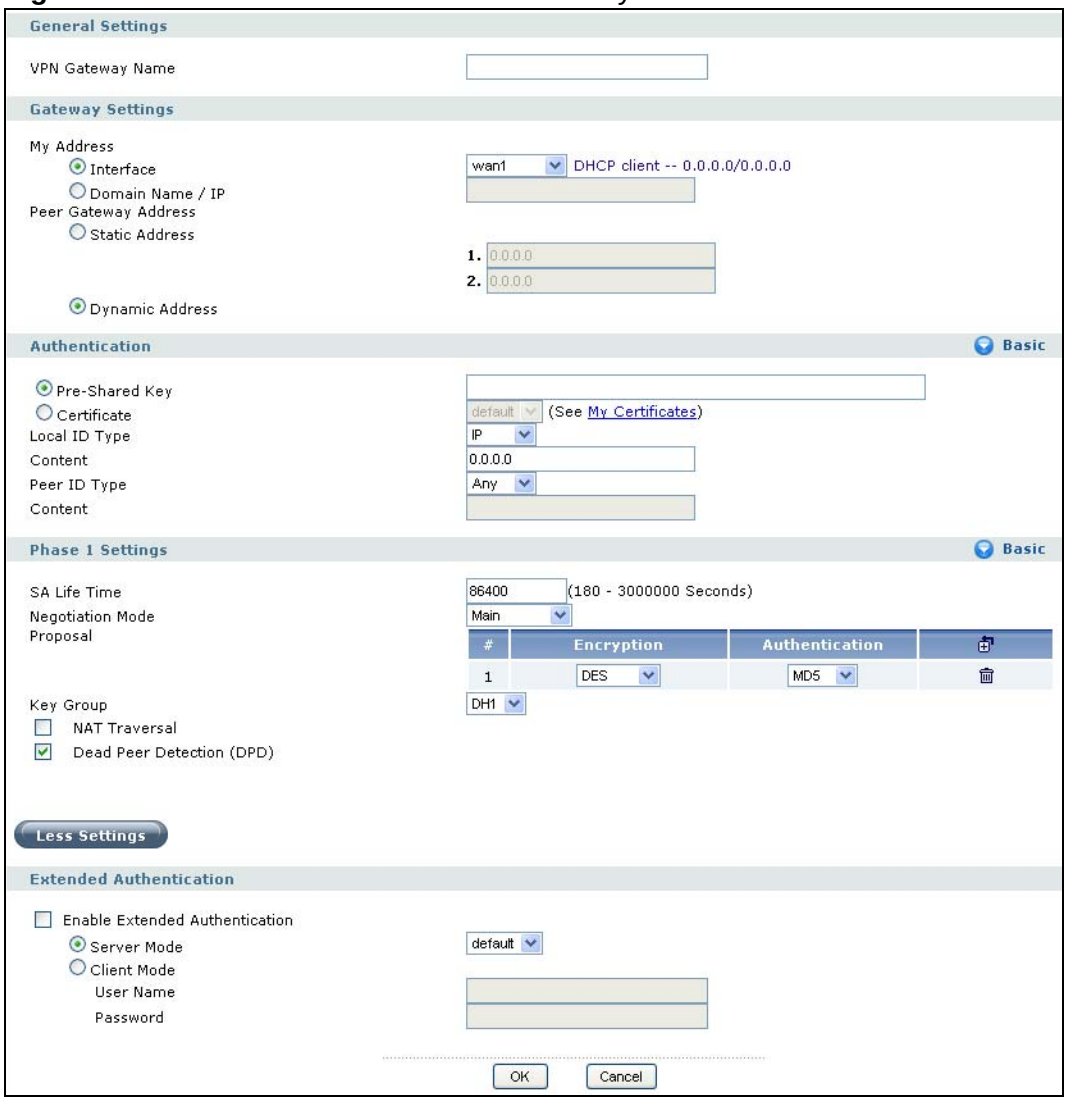
**Table 124** VPN > IPSec VPN > VPN Gateway (continued)

| LABEL | DESCRIPTION |
|---|---|
| Add icon | This column provides icons to add, edit, and remove VPN gateways, as well as to activate / deactivate VPN gateways.<br><br>To add a VPN gateway, click the **Add** icon at the top of the column. The **VPN Gateway Add/Edit** screen appears.<br><br>To edit a VPN gateway, click the **Edit** icon next to the gateway. The **VPN Gateway Add/Edit** screen appears accordingly.<br><br>To delete a VPN gateway, click on the **Remove** icon next to the gateway. The Web Configurator confirms that you want to delete the VPN gateway.<br><br>To activate or deactivate a VPN gateway, click the **Active** icon next to the gateway. Make sure you click **Apply** to save and apply the change. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 21.3.1 The VPN Gateway Add/Edit Screen

The **VPN Gateway Add/Edit** screen allows you to create a new VPN gateway policy or edit an existing one. To access this screen, go to the **VPN Gateway summary** screen (see Section 21.3 on page 379), and click either the **Add** icon or an **Edit** icon.

**Figure 247** VPN > IPSec VPN > VPN Gateway > Edit




Each field is described in the following table.

**Table 125** VPN > IPSec VPN > VPN Gateway > Edit

| LABEL | DESCRIPTION |
|---|---|
| General Settings | |
| VPN Gateway Name | Type the name used to identify this VPN gateway. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| Gateway Settings | |

**Table 125** VPN > IPSec VPN > VPN Gateway > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| My Address | Select how the IP address of the ZyWALL in the IKE SA is defined.<br><br>If you select **Interface**, select the Ethernet interface, VLAN interface, virtual Ethernet interface, virtual VLAN interface, PPPoE/PPTP interface, or auxiliary interface. The IP address of the ZyWALL in the IKE SA is the IP address of the interface.<br><br>If you select **Domain Name / IP**, enter the domain name or the IP address of the ZyWALL. The IP address of the ZyWALL in the IKE SA is the specified IP address or the IP address corresponding to the domain name. 0.0.0.0 is invalid. |
| Peer Gateway Address | Select how the IP address of the remote IPSec router in the IKE SA is defined.<br><br>Select **Static Address** to enter the domain name or the IP address of the remote IPSec router. You can provide a second IP address or domain name for the ZyWALL to try if it cannot establish an IKE SA with the first one.<br><br>Select **Dynamic Address** if the remote IPSec router has a dynamic IP address (and does not use DDNS). |
| Authentication | Click **Advanced** to display more settings. Click **Basic** to display fewer settings.<br><br>Note: The ZyWALL and remote IPSec router must use the same authentication method to establish the IKE SA. |
| Pre-Shared Key | Select this to have the ZyWALL and remote IPSec router use a pre-shared key (password) to identify each other when they negotiate the IKE SA. Type the pre-shared key in the field to the right. The pre-shared key can be<br><br>• 8 - 32 alphanumeric characters or ,;\|`~!@#$%^&*()_+\{}':./<>=-".<br>• 8 - 32 pairs of hexadecimal (0-9, A-F) characters, preceded by “0x”.<br><br>If you want to enter the key in hexadecimal, type “0x” at the beginning of the key. For example, "0x0123456789ABCDEF" is in hexadecimal format; in “0123456789ABCDEF” is in ASCII format. If you use hexadecimal, you must enter twice as many characters since you need to enter pairs.<br><br>The ZyWALL and remote IPSec router must use the same pre-shared key. |

**Table 125** VPN > IPSec VPN > VPN Gateway > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Certificate | Select this to have the ZyWALL and remote IPSec router use certificates to authenticate each other when they negotiate the IKE SA. Then select the certificate the ZyWALL uses to identify itself to the remote IPsec router.<br><br>This certificate is one of the certificates in **My Certificates**. If this certificate is self-signed, import it into the remote IPsec router. If this certificate is signed by a CA, the remote IPsec router must trust that CA.<br><br>Note: The IPSec routers must trust each other's certificates.<br><br>The ZyWALL uses one of its **Trusted Certificates** to authenticate the remote IPSec router's certificate. The trusted certificate can be a self-signed certificate or that of a trusted CA that signed the remote IPSec router's certificate. |
| Local ID Type | This field is read-only if the ZyWALL and remote IPSec router use certificates to identify each other. Select which type of identification is used to identify the ZyWALL during authentication. Choices are:<br><br>**IP** - the ZyWALL is identified by an IP address<br><br>**DNS** - the ZyWALL is identified by a domain name<br><br>**E-mail** - the ZyWALL is identified by an e-mail address |
| Content | This field is read-only if the ZyWALL and remote IPSec router use certificates to identify each other. Type the identity of the ZyWALL during authentication. The identity depends on the **Local ID Type**.<br><br>**IP** - type an IP address; if you type 0.0.0.0, the ZyWALL uses the IP address specified in the **My Address** field. This is not recommended in the following situations:<br><br>• There is a NAT router between the ZyWALL and remote IPSec router.<br>• You want the remote IPSec router to be able to distinguish between IPSec SA requests that come from IPSec routers with dynamic WAN IP addresses.<br><br>In these situations, use a different IP address, or use a different **Local ID Type**.<br><br>**DNS** - type the domain name; you can use up to 31 ASCII characters including spaces, although trailing spaces are truncated. This value is only used for identification and can be any string.<br><br>**E-mail** - the ZyWALL is identified by an e-mail address; you can use up to 31 ASCII characters including spaces, although trailing spaces are truncated. This value is only used for identification and can be any string. |

**Table 125** VPN > IPSec VPN > VPN Gateway > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Peer ID Type | Select which type of identification is used to identify the remote IPSec router during authentication. Choices are:<br>**IP** - the remote IPSec router is identified by an IP address<br>**DNS** - the remote IPSec router is identified by a domain name<br>**E-mail** - the remote IPSec router is identified by an e-mail address<br>**Any** - the ZyWALL does not check the identity of the remote IPSec router<br>If the ZyWALL and remote IPSec router use certificates, there is one more choice.<br>**Subject Name** - the remote IPSec router is identified by the subject name in the certificate |

**Table 125** VPN > IPSec VPN > VPN Gateway > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Content | This field is disabled if the **Peer ID Type** is **Any**. Type the identity of the remote IPSec router during authentication. The identity depends on the **Peer ID Type**.<br><br>If the ZyWALL and remote IPSec router do not use certificates,<br><br>**IP** - type an IP address; see the note at the end of this description.<br><br>**DNS** - type the domain name; you can use up to 31 ASCII characters including spaces, although trailing spaces are truncated. This value is only used for identification and can be any string.<br><br>**E-mail** - the ZyWALL is identified by an e-mail address; you can use up to 31 ASCII characters including spaces, although trailing spaces are truncated. This value is only used for identification and can be any string.<br><br>If the ZyWALL and remote IPSec router use certificates, type the following fields from the certificate used by the remote IPSec router.<br><br>**IP** - subject alternative name field; see the note at the end of this description.<br><br>**DNS** - subject alternative name field<br><br>**E-mail** - subject alternative name field<br><br>**Subject Name** - subject name (maximum 255 ASCII characters, including spaces)<br><br>Note: If **Peer ID Type** is **IP**, please read the rest of this section.<br><br>If you type 0.0.0.0, the ZyWALL uses the IP address specified in the **Secure Gateway Address** field. This is not recommended in the following situations:<br><br>• There is a NAT router between the ZyWALL and remote IPSec router.<br>• You want the remote IPSec router to be able to distinguish between IPSec SA requests that come from IPSec routers with dynamic WAN IP addresses.<br><br>In these situations, use a different IP address, or use a different **Peer ID Type**. |
| Phase 1 Settings | Click **Advanced** to display more settings. Click **Basic** to display fewer settings. |
| SA Life Time (Seconds) | Type the maximum number of seconds the IKE SA can last. When this time has passed, the ZyWALL and remote IPSec router have to update the encryption and authentication keys and re-negotiate the IKE SA. This does not affect any existing IPSec SAs, however. |

**Table 125** VPN > IPSec VPN > VPN Gateway > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Negotiation Mode | Select the negotiation mode to use to negotiate the IKE SA. Choices are<br>**Main** - this encrypts the ZyWALL's and remote IPSec router's identities but takes more time to establish the IKE SA<br>**Aggressive** - this is faster but does not encrypt the identities<br>The ZyWALL and the remote IPSec router must use the same negotiation mode. |
| Proposal | |
| # | This field is a sequential value, and it is not associated with a specific proposal. The sequence of proposals should not affect performance significantly. |
| Encryption | Select which key size and encryption algorithm to use in the IKE SA. Choices are:<br>**DES** - a 56-bit key with the DES encryption algorithm<br>**3DES** - a 168-bit key with the DES encryption algorithm<br>**AES128** - a 128-bit key with the AES encryption algorithm<br>**AES192** - a 192-bit key with the AES encryption algorithm<br>**AES256** - a 256-bit key with the AES encryption algorithm<br>The ZyWALL and the remote IPSec router must use the same key size and encryption algorithm. Longer keys require more processing power, resulting in increased latency and decreased throughput. |
| Authentication | Select which hash algorithm to use to authenticate packet data in the IPSec SA. Choices are **SHA1** and **MD5**. **SHA1** is generally considered stronger than **MD5**, but it is also slower.<br>The remote IPSec router must use the same authentication algorithm. |
| Add icon | This column contains icons to add and remove proposals.<br>To add a proposal, click the **Add** icon at the top of the column.<br>To remove a proposal, click the **Remove** icon next to the proposal. The ZyWALL confirms that you want to delete the proposal before doing so. |
| Key Group | Select which Diffie-Hellman key group (DH*x*) you want to use for encryption keys. Choices are:<br>**DH1** - use a 768-bit random number<br>**DH2** - use a 1024-bit random number<br>**DH5** - use a 1536-bit random number<br>The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. Both routers must use the same DH key group. |

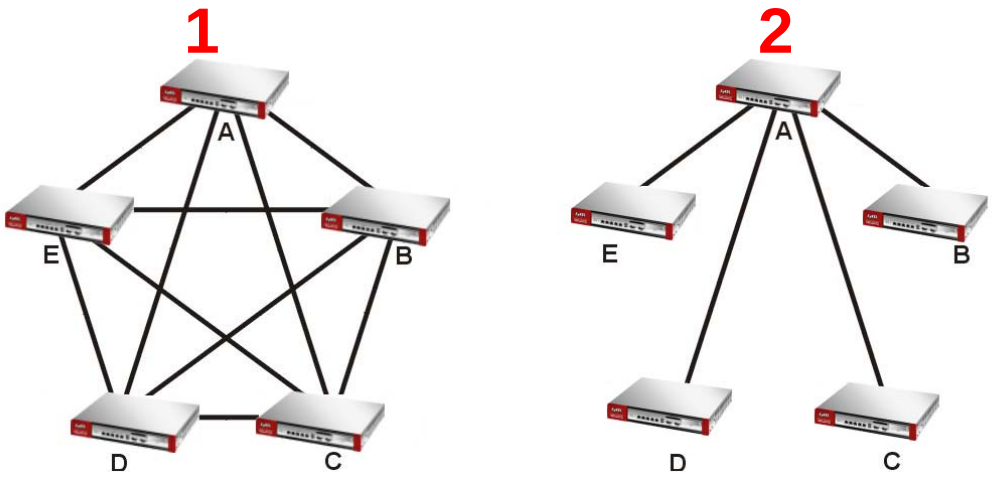
**Table 125** VPN > IPSec VPN > VPN Gateway > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| NAT Traversal | Select this if any of these conditions are satisfied.<br>• This IKE SA might be used to negotiate IPSec SA that use active protocol AH.<br>• There are one or more NAT routers between the ZyWALL and remote IPSec router, and these routers do not support IPSec pass-thru or a similar feature.<br>The remote IPSec router must also enable NAT traversal, and the NAT routers have to forward packets with UDP port 500 and UDP 4500 headers unchanged. |
| Dead Peer Detection (DPD) | Select this check box if you want the ZyWALL to make sure the remote IPSec router is there before it transmits data through the IKE SA. The remote IPSec router must support DPD. If there has been no traffic for at least 15 seconds, the ZyWALL sends a message to the remote IPSec router. If the remote IPSec router responds, the ZyWALL transmits the data. If the remote IPSec router does not respond, the ZyWALL shuts down the IKE SA.<br>If the remote IPSec router does not support DPD, see if you can use the VPN connection connectivity check (see Section 21.2.1 on page 368). |
| More Settings/ Less Settings | Click this button to show or hide the **Extended Authentication** fields. |
| Extended Authentication | When multiple IPSec routers use the same VPN tunnel to connect to a single VPN tunnel (telecommuters sharing a tunnel for example), use extended authentication to enforce a user name and password check. This way even though they all know the VPN tunnel's security settings, each still has to provide a unique user name and password. |
| Enable Extended Authentication | Select this if one of the routers (the ZyWALL or the remote IPSec router) verifies a user name and password from the other router using the local user database and/or an external server. |
| Server Mode | Select this if the ZyWALL authenticates the user name and password from the remote IPSec router. You also have to select the authentication method, which specifies how the ZyWALL authenticates this information. |
| Client Mode | Select this radio button if the ZyWALL provides a username and password to the remote IPSec router for authentication. You also have to provide the **User Name** and the **Password**. |
| User Name | This field is required if the ZyWALL is in **Client Mode** for extended authentication. Type the user name the ZyWALL sends to the remote IPSec router. The user name can be 1-31 ASCII characters. It is case-sensitive, but spaces are not allowed. |
| Password | This field is required if the ZyWALL is in **Client Mode** for extended authentication. Type the password the ZyWALL sends to the remote IPSec router. The password can be 1-31 ASCII characters. It is case-sensitive, but spaces are not allowed. |
| OK | Click **OK** to save your settings and exit this screen. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# 21.4 The VPN Concentrator Screen

A VPN concentrator combines several IPSec VPN connections into one secure network.

**Figure 248** VPN Topologies (Fully Meshed and Hub and Spoke)



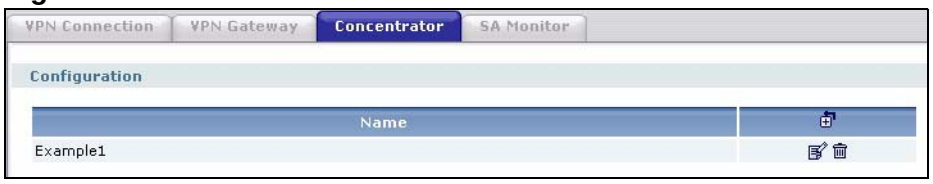

In a fully-meshed VPN topology (**1** in the figure), there is a VPN connection between every pair of routers. In a hub-and-spoke VPN topology (**2** in the figure), there is a VPN connection between each spoke router (**B**, **C**, **D**, and **E**) and the hub router (**A**), which uses the VPN concentrator. The VPN concentrator routes VPN traffic between the spoke routers and itself.

A VPN concentrator reduces the number of VPN connections that you have to set up and maintain in the network. You might also be able to consolidate the policy routes in each spoke router, depending on the IP addresses and subnets of each spoke.

However a VPN concentrator is not for every situation. The hub router is a single failure point, so a VPN concentrator is not as appropriate if the connection between spoke routers cannot be down occasionally (maintenance, for example). There is also more burden on the hub router. It receives VPN traffic from one spoke, decrypts it, inspects it to find out to which spoke to route it, encrypts it, and sends it to the appropriate spoke. Therefore, a VPN concentrator is more suitable when there is a minimum amount of traffic between spoke routers.

The **VPN Concentrator** summary screen displays the VPN concentrators in the ZyWALL. To access this screen, click **VPN** > **IPSec VPN** > **Concentrator**. The following screen appears.

**Figure 249** VPN > IPSec VPN > Concentrator




Each field is discussed in the following table. See Section 21.4.1 on page 389 for more information.

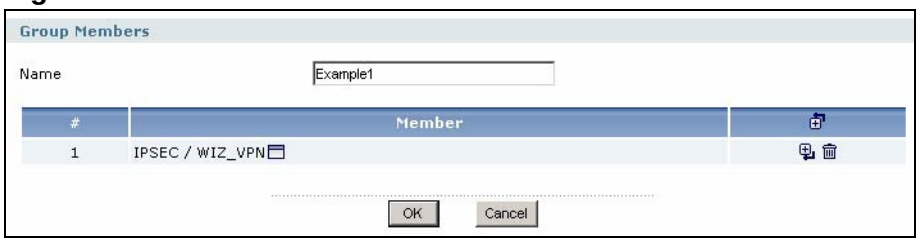
**Table 126** VPN > IPSec VPN > Concentrator

| LABEL | DESCRIPTION |
|---|---|
| # | |
| Name | This field displays the name of the VPN concentrator. |
| Add icon | This column provides icons to add, edit, and remove VPN concentrators.<br><br>To add a VPN concentrator, click the **Add** icon at the top of the column. The **VPN Concentrator Add/Edit** screen appears.<br><br>To edit a VPN concentrator, click the **Edit** icon next to the concentrator. The **VPN Concentrator Add/Edit** screen appears accordingly.<br><br>To delete a VPN concentrator, click on the **Remove** icon next to the concentrator. The Web Configurator confirms that you want to delete the VPN concentrator. |

## 21.4.1 The VPN Concentrator Add/Edit Screen

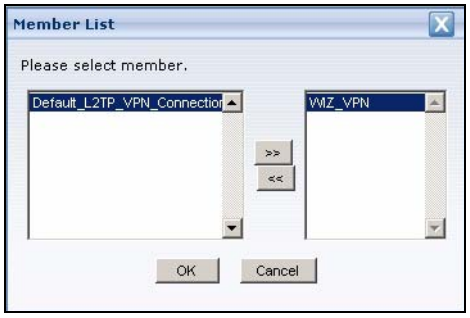
The **VPN Concentrator Add/Edit** screen allows you to create a new VPN concentrator or edit an existing one. To access this screen, go to the **VPN Concentrator summary** screen (see Section 21.4 on page 388), and click either the **Add** icon or an **Edit** icon.

**Figure 250** VPN > IPSec VPN > Concentrator > Edit



Each field is described in the following table.

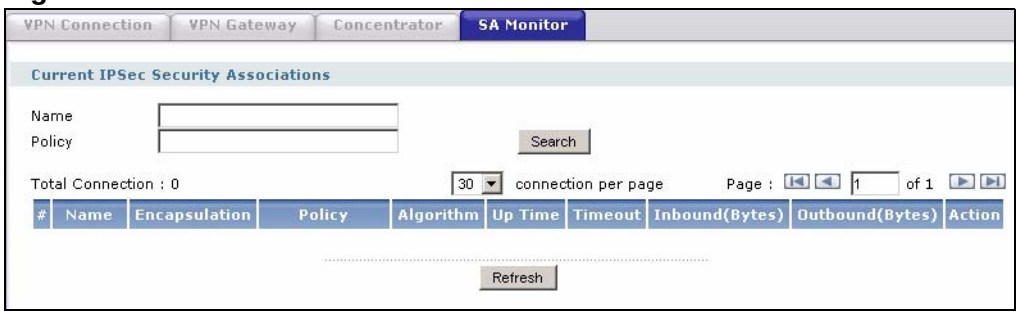
**Table 127** VPN > IPSec VPN > Concentrator > Edit

| LABEL | DESCRIPTION |
|---|---|
| Name | Enter the name of the concentrator. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| # | This field is a sequential value, and it is not associated with a specific member in the concentrator. |
| Member | This field displays the name of each member in the concentrator.<br><br>Note: You must disable policy enforcement in each member. See Section 21.2.1 on page 368.<br><br>Click the **Popup** icon to change this member in the group. The following screen appears.<br><br>IPSec VPN connection policies that do not belong to a VPN concentrator appear on the left. Select any VPN connection policies that you want to add to the VPN concentrator and click the right arrow button to add them.<br><br>The VPN concentrator's member VPN connections appear on the right. Select any VPN connections that you want to remove from the VPN concentrator, and click the left arrow button to remove them.<br><br>**Figure 251** Network > IPSec VPN > Concentrator > Edit > Member<br>  <br> |
| Add icon | This column provides icons to add members to and remove members from the concentrator.<br><br>Click an **Add** icon at the top of the column to add a new member at the beginning of the list, or click the **Add** icon next to an existing member to add a new member after the existing one. The **Member List** screen appears. See the member **Popup** description for more details.<br><br>To remove a member from the concentrator, click on the **Remove** icon next to the member. The Web Configurator confirms that you want to remove the member. |
| OK | Click **OK** to save your changes in the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# 21.5 The SA Monitor Screen

You can use the **SA Monitor** screen to display and to manage active IPSec SAs. To access this screen, click **VPN** > **IPSec VPN** > **SA Monitor**. The following screen appears. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

**Figure 252** VPN > IPSec VPN > SA Monitor




Each field is described in the following table.

**Table 128** VPN > IPSec VPN > SA Monitor

| LABEL | DESCRIPTION |
|---|---|
| Name | Enter the name of a IPSec SA here and click **Search** to find it (if it is associated). You can use a keyword or regular expression. Use up to 30 alphanumeric and _+-.()!$*^:?\|{}[]<>/ characters. See Regular Expressions in Searching IPSec SAs on page 398 for more details. |
| Policy | Enter the IP address(es) or names of the local and remote policies for an IPSec SA and click **Search** to find it. You can use a keyword or regular expression. Use up to 30 alphanumeric and _+-.()!$*^:?\|{}[]<>/ characters. See Regular Expressions in Searching IPSec SAs on page 398 for more details. |
| Search | Click this button to search for an IPSec SA that matches the information you specified above. |
| Total Connection | This field displays the total number of associated IPSec SAs. |
| connection per page | Select how many entries you want to display on each page. |
| Page x of x | This is the number of the page of entries currently displayed and the total number of pages of entries. Type a page number to go to or use the arrows to navigate the pages of entries. |
| # | This field is a sequential value, and it is not associated with a specific SA. |
| Name | This field displays the name of the IPSec SA. |
| Encapsulation | This field displays how the IPSec SA is encapsulated. |
| Policy | This field displays the content of the local and remote policies for this IPSec SA. The IP addresses, not the address objects, are displayed. |
| Algorithm | This field displays the encryption and authentication algorithms used in the SA. |

**Table 128** VPN > IPSec VPN > SA Monitor (continued)

| LABEL | DESCRIPTION |
|---|---|
| Up Time | This field displays how many seconds the IPSec SA has been active. This field displays **N / A** if the IPSec SA uses manual keys. |
| Timeout | This field displays how many seconds remain in the SA life time, before the ZyWALL automatically disconnects the IPSec SA. This field displays **N / A** if the IPSec SA uses manual keys. |
| Inbound (Bytes) | This field displays the amount of traffic that has gone through the IPSec SA from the remote IPSec router to the ZyWALL since the IPSec SA was established. |
| Outbound (Bytes) | This field displays the amount of traffic that has gone through the IPSec SA from the ZyWALL to the remote IPSec router since the IPSec SA was established. |
| Action | This field is displayed if the IPSec SA does not use manual keys.<br>Click the **Disconnect** icon next to an IPSec SA to disconnect it. |
| Refresh | Click **Refresh** to update the information in the display. |

# 21.6 IPSec VPN Background Information

Here is some more detailed IPSec VPN background information.

## IKE SA Overview

The IKE SA provides a secure connection between the ZyWALL and remote IPSec router.

It takes several steps to establish an IKE SA. The negotiation mode determines how many. There are two negotiation modes--main mode and aggressive mode. Main mode provides better security, while aggressive mode is faster.

Note: Both routers must use the same negotiation mode.

These modes are discussed in more detail in Negotiation Mode on page 396. Main mode is used in various examples in the rest of this section.

### IP Addresses of the ZyWALL and Remote IPSec Router

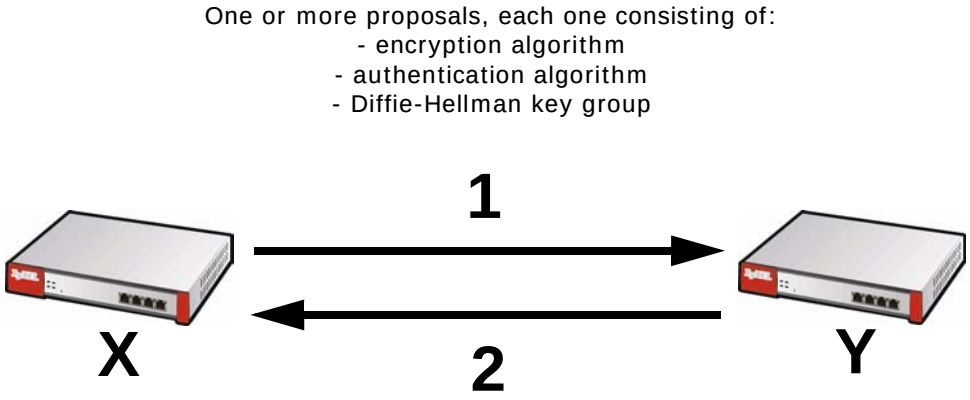
To set up an IKE SA, you have to specify the IP addresses of the ZyWALL and remote IPSec router. You can usually enter a static IP address or a domain name for either or both IP addresses. Sometimes, your ZyWALL might offer another alternative, such as using the IP address of a port or interface, as well.

You can also specify the IP address of the remote IPSec router as 0.0.0.0. This means that the remote IPSec router can have any IP address. In this case, only the remote IPSec router can initiate an IKE SA because the ZyWALL does not know the IP address of the remote IPSec router. This is often used for telecommuters.

## IKE SA Proposal

The IKE SA proposal is used to identify the encryption algorithm, authentication algorithm, and Diffie-Hellman (DH) key group that the ZyWALL and remote IPSec router use in the IKE SA. In main mode, this is done in steps 1 and 2, as illustrated next.

**Figure 253** IKE SA: Main Negotiation Mode, Steps 1 - 2: IKE SA Proposal




The ZyWALL sends one or more proposals to the remote IPSec router. (In some devices, you can only set up one proposal.) Each proposal consists of an encryption algorithm, authentication algorithm, and DH key group that the ZyWALL wants to use in the IKE SA. The remote IPSec router selects an acceptable proposal and sends the accepted proposal back to the ZyWALL. If the remote IPSec router rejects all of the proposals, the ZyWALL and remote IPSec router cannot establish an IKE SA.

Note: Both routers must use the same encryption algorithm, authentication algorithm, and DH key group.

In most ZyWALLs, you can select one of the following encryption algorithms for each proposal. The algorithms are listed in order from weakest to strongest.

- Data Encryption Standard (DES) is a widely used method of data encryption. It applies a 56-bit key to each 64-bit block of data.
- Triple DES (3DES) is a variant of DES. It iterates three times with three separate keys, effectively tripling the strength of DES.

- Advanced Encryption Standard (AES) is a newer method of data encryption that also uses a secret key. AES applies a 128-bit key to 128-bit blocks of data. It is faster than 3DES.

Some ZyWALLs also offer stronger forms of AES that apply 192-bit or 256-bit keys to 128-bit blocks of data.

In most ZyWALLs, you can select one of the following authentication algorithms for each proposal. The algorithms are listed in order from weakest to strongest.

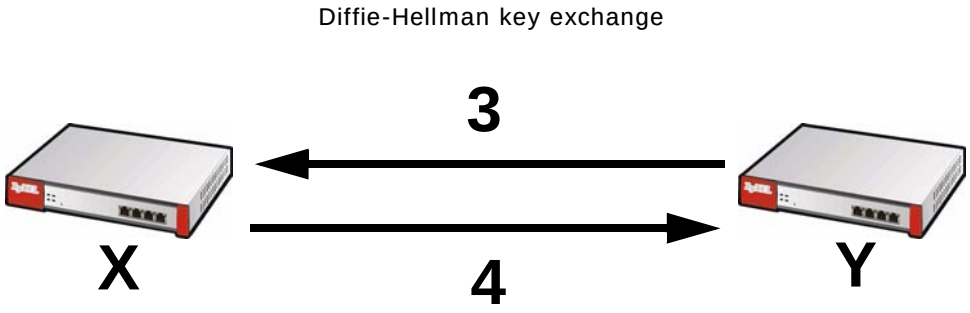
- MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.
- SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.

See Diffie-Hellman (DH) Key Exchange on page 394 for more information about DH key groups.

## Diffie-Hellman (DH) Key Exchange

The ZyWALL and the remote IPSec router use DH public-key cryptography to establish a shared secret. The shared secret is then used to generate encryption keys for the IKE SA and IPSec SA. In main mode, this is done in steps 3 and 4, as illustrated next.

**Figure 254** IKE SA: Main Negotiation Mode, Steps 3 - 4: DH Key Exchange



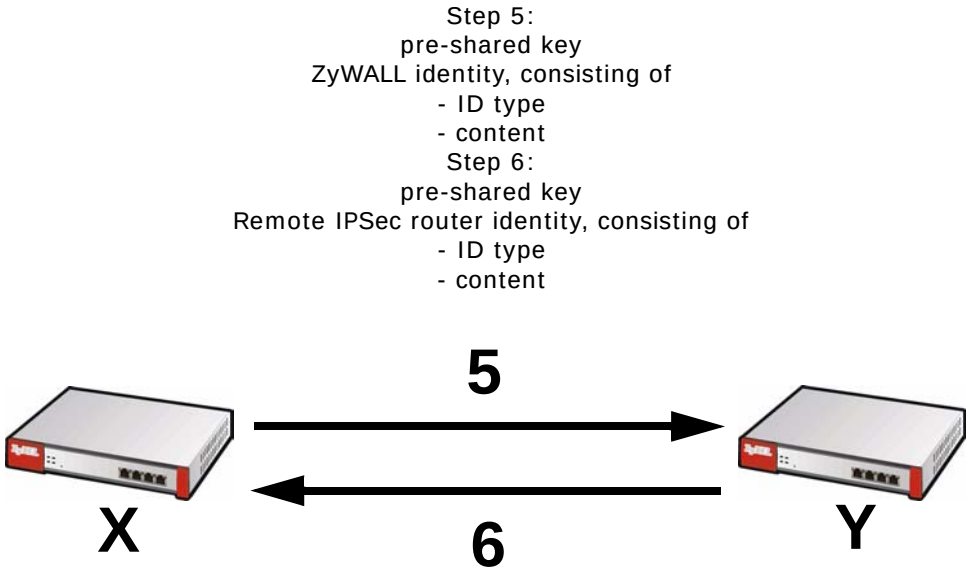

DH public-key cryptography is based on DH key groups. Each key group is a fixed number of bits long. The longer the key, the more secure the encryption, but also the longer it takes to encrypt and decrypt information. For example, DH2 keys (1024 bits) are more secure than DH1 keys (768 bits), but DH2 keys take longer to encrypt and decrypt.

## Authentication

Before the ZyWALL and remote IPSec router establish an IKE SA, they have to verify each other's identity. This process is based on pre-shared keys and router identities.

In main mode, the ZyWALL and remote IPSec router authenticate each other in steps 5 and 6, as illustrated below. The identities are also encrypted using the encryption algorithm and encryption key the ZyWALL and remote IPSec router selected in previous steps.

**Figure 255** IKE SA: Main Negotiation Mode, Steps 5 - 6: Authentication (continued)




You have to create (and distribute) a pre-shared key. The ZyWALL and remote IPSec router use it in the authentication process, though it is not actually transmitted or exchanged.

Note: The ZyWALL and the remote IPSec router must use the same pre-shared key.

Router identity consists of ID type and content. The ID type can be domain name, IP address, or e-mail address, and the content is a (properly-formatted) domain name, IP address, or e-mail address. The content is only used for identification. Any domain name or e-mail address that you enter does not have to actually exist. Similarly, any domain name or IP address that you enter does not have to correspond to the ZyWALL's or remote IPSec router's properties.

The ZyWALL and the remote IPSec router have their own identities, so both of them must store two sets of information, one for themselves and one for the other router. Local ID type and content refers to the ID type and content that applies to the router itself, and peer ID type and content refers to the ID type and content that applies to the other router.

Note: The ZyWALL's local and peer ID type and content must match the remote IPSec router's peer and local ID type and content, respectively.

For example, in Table 129 on page 396, the ZyWALL and the remote IPSec router authenticate each other successfully. In contrast, in Table 130 on page 396, the

ZyWALL and the remote IPSec router cannot authenticate each other and, therefore, cannot establish an IKE SA.

**Table 129** VPN Example: Matching ID Type and Content

| ZYWALL | REMOTE IPSEC ROUTER |
|---|---|
| Local ID type: E-mail | Local ID type: IP |
| Local ID content: tom@yourcompany.com | Local ID content: 1.1.1.2 |
| Peer ID type: IP | Peer ID type: E-mail |
| Peer ID content: 1.1.1.2 | Peer ID content: tom@yourcompany.com |

**Table 130** VPN Example: Mismatching ID Type and Content

| ZYWALL | REMOTE IPSEC ROUTER |
|---|---|
| Local ID type: E-mail | Local ID type: IP |
| Local ID content: tom@yourcompany.com | Local ID content: 1.1.1.2 |
| Peer ID type: IP | Peer ID type: E-mail |
| Peer ID content: 1.1.1.20 | Peer ID content: tom@yourcompany.com |

It is also possible to configure the ZyWALL to ignore the identity of the remote IPSec router. In this case, you usually set the peer ID type to **Any**. This is less secure, so you should only use this if your ZyWALL provides another way to check the identity of the remote IPSec router (for example, extended authentication) or if you are troubleshooting a VPN tunnel.

## Additional Topics for IKE SA

This section provides more information about IKE SA.

### Negotiation Mode

There are two negotiation modes--main mode and aggressive mode. Main mode provides better security, while aggressive mode is faster.

Main mode takes six steps to establish an IKE SA.

Steps 1 - 2: The ZyWALL sends its proposals to the remote IPSec router. The remote IPSec router selects an acceptable proposal and sends it back to the ZyWALL.

Steps 3 - 4: The ZyWALL and the remote IPSec router exchange pre-shared keys for authentication and participate in a Diffie-Hellman key exchange, based on the accepted DH key group, to establish a shared secret.

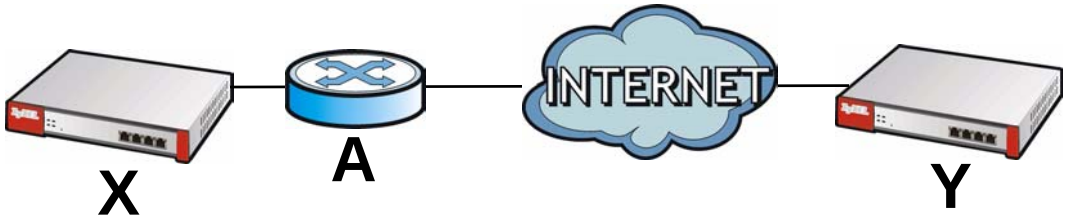
Steps 5 - 6: Finally, the ZyWALL and the remote IPSec router generate an encryption key (from the shared secret), encrypt their identities, and exchange their encrypted identity information for authentication.

In contrast, aggressive mode only takes three steps to establish an IKE SA. Aggressive mode does not provide as much security because the identity of the ZyWALL and the identity of the remote IPSec router are not encrypted. It is usually used in remote-access situations, where the address of the initiator is not known by the responder and both parties want to use pre-shared keys for authentication. For example, the remote IPSec router may be a telecommuter who does not have a static IP address.

### VPN, NAT, and NAT Traversal

In the following example, there is another router (**A**) between router **X** and router **Y**.

**Figure 256** VPN/NAT Example




If router **A** does NAT, it might change the IP addresses, port numbers, or both. If router **X** and router **Y** try to establish a VPN tunnel, the authentication fails because it depends on this information. The routers cannot establish a VPN tunnel.

Most routers like router **A** now have an IPSec pass-thru feature. This feature helps router **A** recognize VPN packets and route them appropriately. If router **A** has this feature, router **X** and router **Y** can establish a VPN tunnel as long as the active protocol is ESP. (See Active Protocol on page 399 for more information about active protocols.)

If router A does not have an IPSec pass-thru or if the active protocol is AH, you can solve this problem by enabling NAT traversal. In NAT traversal, router **X** and router **Y** add an extra header to the IKE SA and IPSec SA packets. If you configure router **A** to forward these packets unchanged, router **X** and router **Y** can establish a VPN tunnel.

You have to do the following things to set up NAT traversal.

- Enable NAT traversal on the ZyWALL and remote IPSec router.
- Configure the NAT router to forward packets with the extra header unchanged. (See the field description for detailed information about the extra header.)

The extra header may be UDP port 500 or UDP port 4500, depending on the standard(s) the ZyWALL and remote IPSec router support.

### Extended Authentication

Extended authentication is often used when multiple IPSec routers use the same VPN tunnel to connect to a single IPSec router. For example, this might be used with telecommuters.

In extended authentication, one of the routers (the ZyWALL or the remote IPSec router) provides a user name and password to the other router, which uses a local user database and/or an external server to verify the user name and password. If the user name or password is wrong, the routers do not establish an IKE SA.

You can set up the ZyWALL to provide a user name and password to the remote IPSec router, or you can set up the ZyWALL to check a user name and password that is provided by the remote IPSec router.

If you use extended authentication, it takes four more steps to establish an IKE SA. These steps occur at the end, regardless of the negotiation mode (steps 7-10 in main mode, steps 4-7 in aggressive mode).

### Certificates

It is possible for the ZyWALL and remote IPSec router to authenticate each other with certificates. In this case, you do not have to set up the pre-shared key, local identity, or remote identity because the certificates provide this information instead.

- Instead of using the pre-shared key, the ZyWALL and remote IPSec router check the signatures on each other's certificates. Unlike pre-shared keys, the signatures do not have to match.
- The local and peer ID type and content come from the certificates.

Note: You must set up the certificates for the ZyWALL and remote IPSec router first.

## Regular Expressions in Searching IPSec SAs

A question mark (?) lets a single character in the VPN connection or policy name vary. For example, use "a?c" (without the quotation marks) to specify abc, acc and so on.

Wildcards (*) let multiple VPN connection or policy names match the pattern. For example, use "*abc" (without the quotation marks) to specify any VPN connection or policy name that ends with "abc". A VPN connection named "testabc" would match. There could be any number (of any type) of characters in front of the "abc" at the end and the VPN connection or policy name would still match. A VPN connection or policy name named "testacc" for example would not match.

A * in the middle of a VPN connection or policy name has the ZyWALL check the beginning and end and ignore the middle. For example, with “abc*123”, any VPN connection or policy name starting with “abc” and ending in “123” matches, no matter how many characters are in between.

The whole VPN connection or policy name has to match if you do not use a question mark or asterisk.

# IPSec SA Overview

Once the ZyWALL and remote IPSec router have established the IKE SA, they can securely negotiate an IPSec SA through which to send data between computers on the networks.

Note: The IPSec SA stays connected even if the underlying IKE SA is not available anymore.

This section introduces the key components of an IPSec SA.

## Local Network and Remote Network

In an IPSec SA, the local network, the one(s) connected to the ZyWALL, may be called the local policy. Similarly, the remote network, the one(s) connected to the remote IPSec router, may be called the remote policy.

## Active Protocol

The active protocol controls the format of each packet. It also specifies how much of each packet is protected by the encryption and authentication algorithms. IPSec VPN includes two active protocols, AH (Authentication Header, RFC 2402) and ESP (Encapsulating Security Payload, RFC 2406).

Note: The ZyWALL and remote IPSec router must use the same active protocol.

Usually, you should select ESP. AH does not support encryption, and ESP is more suitable with NAT.

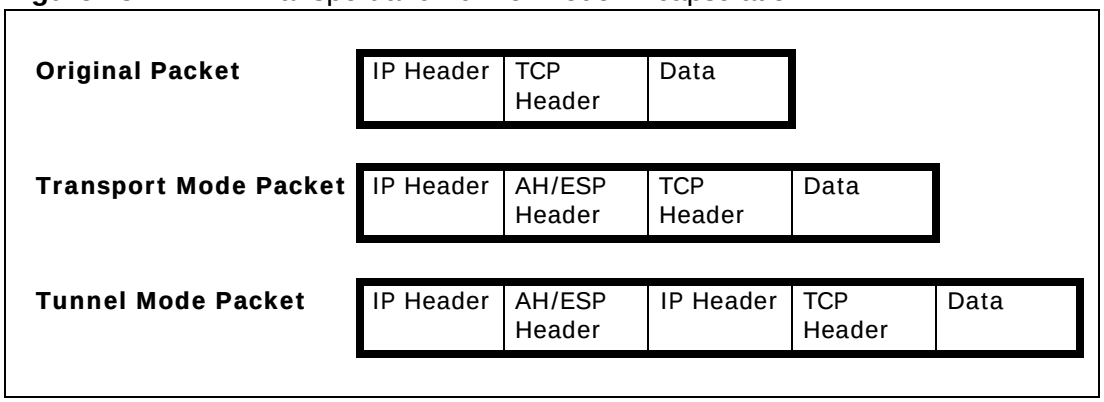
## Encapsulation

There are two ways to encapsulate packets. Usually, you should use tunnel mode because it is more secure. Transport mode is only used when the IPSec SA is used for communication between the ZyWALL and remote IPSec router (for example, for remote management), not between computers on the local and remote networks.

Note: The ZyWALL and remote IPSec router must use the same encapsulation.

These modes are illustrated below.

**Figure 257** VPN: Transport and Tunnel Mode Encapsulation




In tunnel mode, the ZyWALL uses the active protocol to encapsulate the entire IP packet. As a result, there are two IP headers:

- Outside header: The outside IP header contains the IP address of the ZyWALL or remote IPSec router, whichever is the destination.
- Inside header: The inside IP header contains the IP address of the computer behind the ZyWALL or remote IPSec router. The header for the active protocol (AH or ESP) appears between the IP headers.

In transport mode, the encapsulation depends on the active protocol. With AH, the ZyWALL includes part of the original IP header when it encapsulates the packet. With ESP, however, the ZyWALL does not include the IP header when it encapsulates the packet, so it is not possible to verify the integrity of the source IP address.

## IPSec SA Proposal and Perfect Forward Secrecy

An IPSec SA proposal is similar to an IKE SA proposal (see IKE SA Proposal on page 393), except that you also have the choice whether or not the ZyWALL and remote IPSec router perform a new DH key exchange every time an IPSec SA is established. This is called Perfect Forward Secrecy (PFS).

If you enable PFS, the ZyWALL and remote IPSec router perform a DH key exchange every time an IPSec SA is established, changing the root key from which encryption keys are generated. As a result, if one encryption key is compromised, other encryption keys remain secure.

If you do not enable PFS, the ZyWALL and remote IPSec router use the same root key that was generated when the IKE SA was established to generate encryption keys.

The DH key exchange is time-consuming and may be unnecessary for data that does not require such security.

## Additional Topics for IPSec SA

This section provides more information about IPSec SA in your ZyWALL.

### IPSec SA using Manual Keys

You might set up an IPSec SA using manual keys when you want to establish a VPN tunnel quickly, for example, for troubleshooting. You should only do this as a temporary solution, however, because it is not as secure as a regular IPSec SA.

In IPSec SAs using manual keys, the ZyWALL and remote IPSec router do not establish an IKE SA. They only establish an IPSec SA. As a result, an IPSec SA using manual keys has some characteristics of IKE SA and some characteristics of IPSec SA. There are also some differences between IPSec SA using manual keys and other types of SA.

### IPSec SA Proposal using Manual Keys

In an IPSec SA using manual keys, you can only specify one encryption algorithm and one authentication algorithm. You cannot specify several proposals. There is no DH key exchange, so you have to provide the encryption key and the authentication key the ZyWALL and remote IPSec router use.

Note: The ZyWALL and remote IPSec router must use the same encryption key and authentication key.

### Authentication and the Security Parameter Index (SPI)

For authentication, the ZyWALL and remote IPSec router use the SPI, instead of pre-shared keys, ID type and content. The SPI is an identification number.

Note: The ZyWALL and remote IPSec router must use the same SPI.

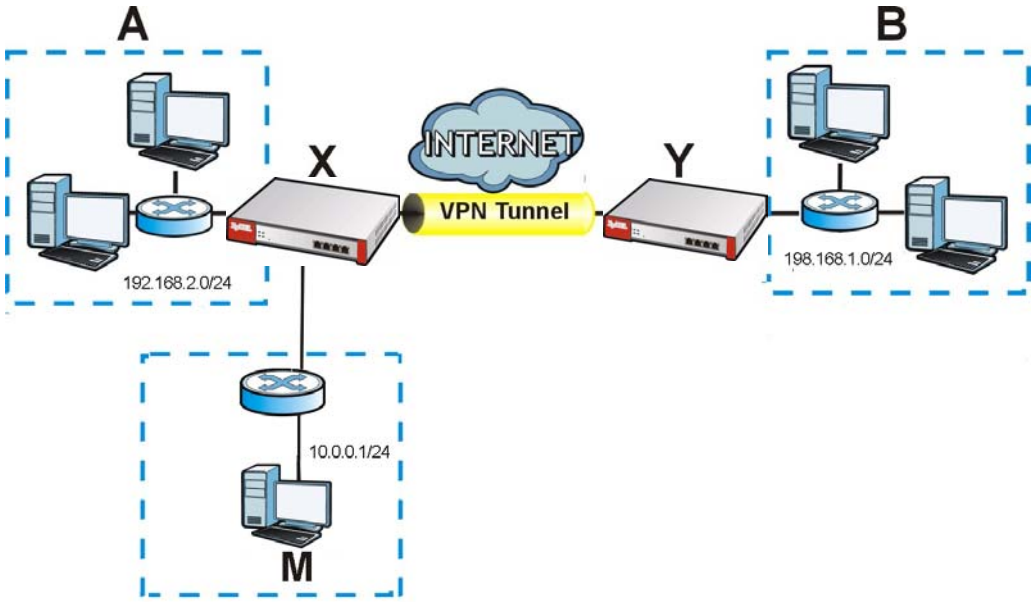
### NAT for Inbound and Outbound Traffic

The ZyWALL can translate the following types of network addresses in IPSec SA.

- Source address in outbound packets - this translation is necessary if you want the ZyWALL to route packets from computers outside the local network through the IPSec SA.
- Source address in inbound packets - this translation hides the source address of computers in the remote network.
- Destination address in inbound packets - this translation is used if you want to forward packets (for example, mail) from the remote network to a specific computer (like the mail server) in the local network.

Each kind of translation is explained below. The following example is used to help explain each one.

**Figure 258** VPN Example: NAT for Inbound and Outbound Traffic




### Source Address in Outbound Packets (Outbound Traffic, Source NAT)

This translation lets the ZyWALL route packets from computers that are not part of the specified local network (local policy) through the IPSec SA. For example, in Figure 258 on page 402, you have to configure this kind of translation if you want computer **M** to establish a connection with any computer in the remote network (**B**). If you do not configure it, the remote IPSec router may not route messages for computer **M** through the IPSec SA because computer **M**'s IP address is not part of its local policy.

To set up this NAT, you have to specify the following information:

- Source - the original source address; most likely, computer **M**'s network.
- Destination - the original destination address; the remote network (**B**).
- SNAT - the translated source address; the local network (**A**).

### Source Address in Inbound Packets (Inbound Traffic, Source NAT)

You can set up this translation if you want to change the source address of computers in the remote network. To set up this NAT, you have to specify the following information:

- Source - the original source address; the remote network (**B**).
- Destination - the original destination address; the local network (**A**).

- SNAT - the translated source address; a different IP address (range of addresses) to hide the original source address.

### Destination Address in Inbound Packets (Inbound Traffic, Destination NAT)

You can set up this translation if you want the ZyWALL to forward some packets from the remote network to a specific computer in the local network. For example, in Figure 258 on page 402, you can configure this kind of translation if you want to forward mail from the remote network to the mail server in the local network (**A**).

You have to specify one or more rules when you set up this kind of NAT. The ZyWALL checks these rules similar to the way it checks rules for a firewall. The first part of these rules define the conditions in which the rule apply.

- Original IP - the original destination address; the remote network (**B**).
- Protocol - the protocol [TCP, UDP, or both] used by the service requesting the connection.
- Original Port - the original destination port or range of destination ports; in Figure 258 on page 402, it might be port 25 for SMTP.

The second part of these rules controls the translation when the condition is satisfied.

- Mapped IP - the translated destination address; in Figure 258 on page 402, the IP address of the mail server in the local network (**A**).
- Mapped Port - the translated destination port or range of destination ports.

The original port range and the mapped port range must be the same size.

# 22

# SSL VPN

## 22.1 Overview

Use SSL VPN to allow users to use a web browser for secure remote user login (the remote users do not need a VPN router or VPN client software.

### 22.1.1 What You Can Do in the SSL VPN Screens

- Use the **VPN > SSL VPN > Access Privilege** screens (see Section 22.2 on page 407) to configure SSL access policies.
- Use the **VPN > SSL VPN > Connection Monitor** screen (see Section 22.3 on page 411) to list the users currently logged into the VPN SSL client portal. You can also log out individual users and delete related session information.
- Use the Click **VPN > SSL VPN** > **Global Setting** screen (see Section 22.4 on page 412) to set the IP address of the ZyWALL (or a gateway device) on your network for full tunnel mode access, enter access messages or upload a custom logo to be displayed on the remote user screen.

### 22.1.2 What You Need to Know About SSL VPN

There are two SSL VPN network access modes: reverse proxy and full tunnel.

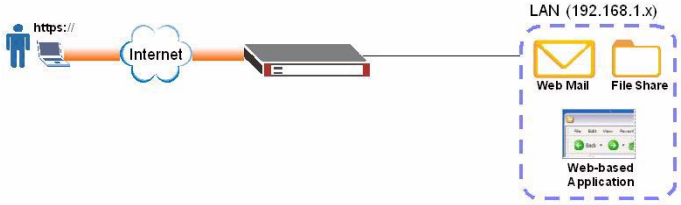
#### Reverse Proxy Mode

In reverse proxy mode, the ZyWALL is a proxy that acts on behalf of the local network servers (such as your web and mail servers). As the final destination, the ZyWALL appears to be the server to remote users. This provides an added layer of protection for your internal servers.

With reverse proxy mode, remote users can easily access any web-based applications on the local network by clicking on links or entering the provided URL.

You do not have to install additional client software on the remote user computers for access.

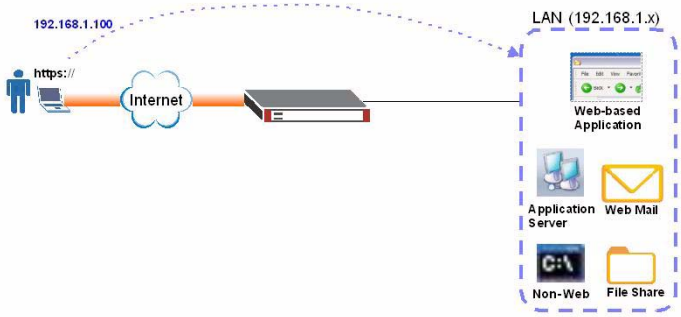
**Figure 259** Network Access Mode: Reverse Proxy




## Full Tunnel Mode

In full tunnel mode, a virtual connection is created for remote users with private IP addresses in the same subnet as the local network. This allows them to access network resources in the same way as if they were part of the internal network.

**Figure 260** Network Access Mode: Full Tunnel Mode




## SSL Access Policy

An SSL access policy allows the ZyWALL to perform the following tasks:

- limit user access to specific applications or files on the network.
- allow user access to specific networks.
- assign private IP addresses and provide DNS/WINS server information to remote users to access internal networks.

## SSL Access Policy Objects

The SSL access policies reference the following objects. If you update this information, in response to changes, the ZyWALL automatically propagates the

changes through the SSL policies that use the object(s). When you delete an SSL policy, the objects are not removed.

**Table 131** Objects

| OBJECT TYPE | OBJECT SCREEN | DESCRIPTION |
|---|---|---|
| User Accounts | User Account/ User Group | Configure a user account or user group to which you want to apply this SSL access policy. |
| Application | SSL Application | Configure an SSL application object to specify the type of application and the address of the local computer, server, or web site SSL users are to be able to access. |
| IP Pool | Address | Configure an address object that defines a range of private IP addresses to assign to user computers so they can access the internal network through a VPN connection. |
| Server Addresses | Address | Configure address objects for the IP addresses of the DNS and WINS servers that the ZyWALL sends to the VPN connection users. |
| VPN Network | Address | Configure an address object to specify which network segment users are allowed to access through a VPN connection. |

You cannot delete an object that is referenced by an SSL access policy. To delete the object, you must first unassociate the object from the SSL access policy.

### Finding Out More

- See Section 5.4.5 on page 88 for related information on these screens.
- See Section 22.5 on page 415 for how to establish an SSL VPN connection to the ZyWALL (after you have configured the SSL VPN settings on the ZyWALL).
- See Chapter 44 on page 721 for details on SSL application objects.

## 22.2 The SSL Access Privilege Screen

Click **VPN > SSL VPN** to open the **Access Privilege** screen. This screen lists the configured SSL access policies.

**Figure 261** VPN > SSL VPN > Access Privilege

The following table describes the labels in this screen.

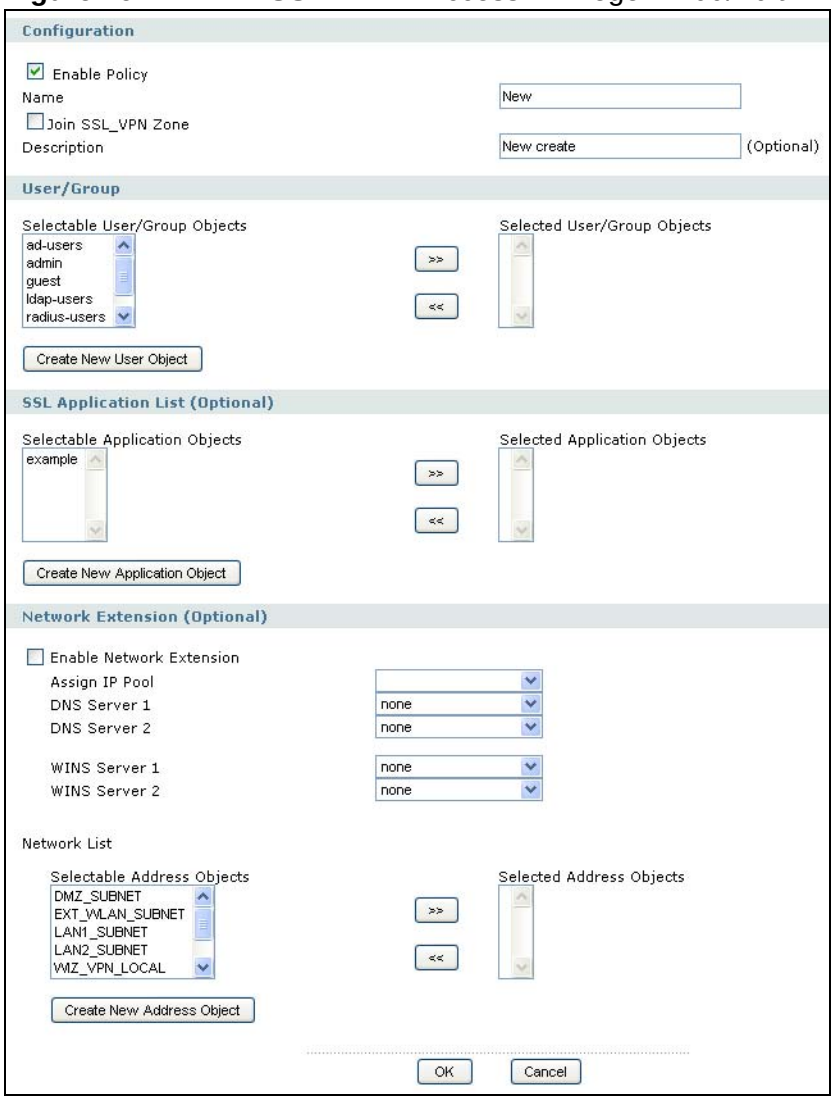
**Table 132** VPN > SSL VPN > Access Privilege

| LABEL | DESCRIPTION |
|---|---|
| # | This field displays the index number of the entry. |
| Name | This field displays the descriptive name of the SSL access policy for identification purposes. |
| User/Group | This field displays the user account or user group name(s) associated to an SSL access policy.<br>This field displays up to three names. |
| Application | This field displays the descriptive name of the SSL application object this policy uses. |
| Add icon | This column provides icons to add, edit, and remove policies.<br>To add a new policy, click the **Add** icon at the top of the column.<br>To activate or disable the policy, click the **Activate**/**Deactivate** icon.<br>To edit a policy, click the **Edit** icon next to the policy.<br>To delete a policy, click the **Remove** icon next to the policy.<br>To rearrange a policy in the list, click the **Move to N** icon next to the policy. |
| Apply | Click **Apply** to save the settings. |
| Reset | Click **Reset** to discard all changes. |

## 22.2.1 The SSL Access Policy Add/Edit Screen

To create a new or edit an existing SSL access policy, click the **Add** or **Edit** icon in the **Access Privilege** screen.

**Figure 262** VPN > SSL VPN > Access Privilege > Add/Edit




The following table describes the labels in this screen.

**Table 133** VPN > SSL VPN > Access Privilege > Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| Configuration | |
| Enable Policy | Select this option to activate this SSL access policy. |
| Name | Enter a descriptive name to identify this policy. You can enter up to 15 characters (“a-z”, A-Z”, “0-9”) with no spaces allowed. |

**Table 133** VPN > SSL VPN > Access Privilege > Add/Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Join SSL_VPN Zone | Select this check box to add the SSL access policy to the SSL_VPN security zone. Any security rules or settings configured for the SSL_VPN security zone will also apply to this SSL access policy . |
| Description | Enter additional information about this SSL access policy. You can enter up to 31 characters (“0-9”, “a-z”, “A-Z”, “-” and “_”). |
| User/Group | The **Selectable User/Group Objects** list displays the name(s) of the user account and/or user group(s) to which you have not applied an SSL access policy yet.<br><br>To associate a user or user group to this SSL access policy, select a user account or user group and click **>>** to add to the **Selected User/Group Objects** list. You can select more than one name.<br><br>To remove a user or user group, select the name(s) in the **Selected User/Group Objects** list and click **<<**. |
| Create New User Object | Click this to display a screen you use to create a new user account or user group name (see Section 37.2.1 on page 652 for details). |
| SSL Application List (Optional) | The **Selectable Application Objects** list displays the name(s) of the SSL application(s) you can select for this SSL access policy.<br><br>To associate an SSL application to this SSL access policy, select a name and click **>>** to add to the **Selected Application Objects** list. You can select more than one application.<br><br>To remove an SSL application, select the name(s) in the **Selected Application Objects** list and click **<<**. |
| Create New Application Object | Click this to create a new SSL application object. Refer to Chapter 44 on page 721 for more information. |
| Network Extension (Optional) | |
| Enable Network Extension | Select this option to create a VPN tunnel between the authenticated users and the internal network. This allows the users to access the resources on the network as if they were on the same local network.<br><br>Clear this option to disable this feature. Users can only access the applications as defined by the selected SSL application settings and the remote user computers are not made to be a part of the local network. |
| Assign IP Pool | Define a separate pool of IP addresses to assign to the SSL users. Select it here.<br><br>The SSL VPN IP pool cannot overlap with IP addresses on the ZyWALL's local networks (LAN and DMZ for example), the SSL user's network, or the networks you specify in the SSL VPN **Network List**. |
| DNS/WINS Server 1..2 | Select the name of the DNS or WINS server whose information the ZyWALL sends to the remote users. This allows them to access devices on the local network using domain names instead of IP addresses. |

**Table 133** VPN > SSL VPN > Access Privilege > Add/Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Network List | To allow user access to local network(s), select a network name in the **Selectable Address Objects** list and click **>>** to add to the **Selected Address Objects** list. You can select more than one network.<br><br>To block access to a network, select the network name in the **Selected Address Objects** list and click **<<**. |
| Create New Address Object | Click this to create a new network object. Refer to Chapter 38 on page 665 for more information. |
| OK | Click **Ok** to save the changes and return to the main **Access Privilege** screen. |
| Cancel | Click **Cancel** to discard all changes and return to the main **Access Privilege** screen. |

# 22.3 The SSL Connection Monitor Screen

The ZyWALL keeps track of the users who are currently logged into the VPN SSL client portal. Click **VPN > SSL VPN** in the navigation panel and click the **Connection Monitor** tab to display the user list.

Use this screen to do the following:

- View a list of active SSL VPN connections.
- Log out individual users and delete related session information.

Once a user logs out, the corresponding entry is removed from the **Connection Monitor** screen.

**Figure 263** VPN > SSL VPN > Connection Monitor


The following table describes the labels in this screen.

**Table 134** VPN > SSL VPN > Connection Monitor

| LABEL | DESCRIPTION |
|---|---|
| # | This field displays the index number. |
| User | This field displays the account user name used to establish this SSL VPN connection. |
| Access | This field displays the name of the SSL VPN application the user is accessing. |

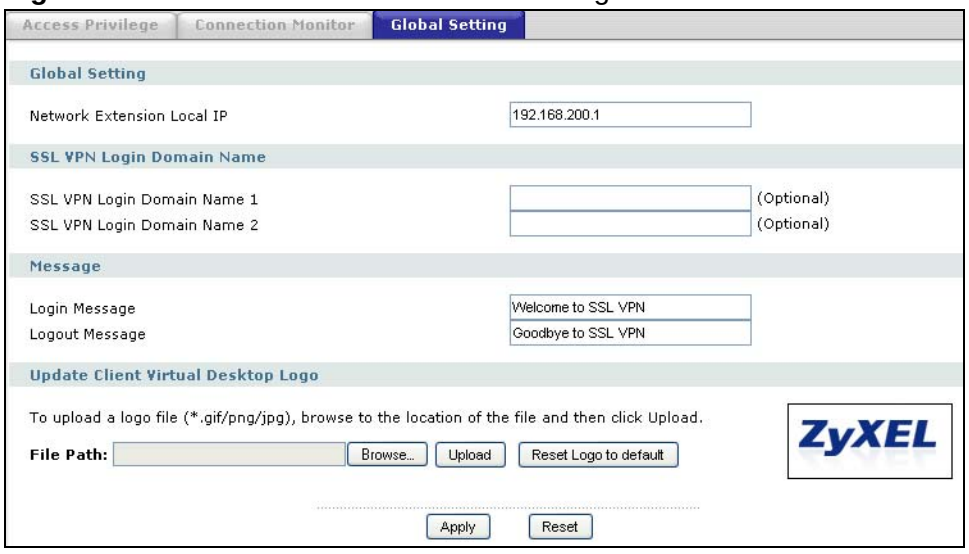
**Table 134** VPN > SSL VPN > Connection Monitor (continued)

| LABEL | DESCRIPTION |
|---|---|
| Login Address | This field displays the IP address the user used to establish this SSL VPN connection. |
| Connected Time | This field displays the time this connection was established. |
| Inbound (Bytes) | This field displays the number of bytes received by the ZyWALL on this connection. |
| Outbound (Bytes) | This field displays the number of bytes transmitted by the ZyWALL on this connection. |
| Action | Click the icon to terminate the connection of the user and delete corresponding session information from the ZyWALL. |
| Refresh | Click **Refresh** to update this screen. |

# 22.4 The SSL Global Setting Screen

Click **VPN > SSL VPN** and click the **Global Setting** tab to display the following screen. Use this screen to set the IP address of the ZyWALL (or a gateway device) on your network for full tunnel mode access, enter access messages or upload a custom logo to be displayed on the remote user screen.

**Figure 264** VPN > SSL VPN > Global Setting



The following table describes the labels in this screen.

**Table 135** VPN > SSL VPN > Global Setting

| LABEL | DESCRIPTION |
|---|---|
| Global Setting | |
| Network Extension Local IP | Specify the IP address of the ZyWALL (or a gateway device) for full tunnel mode SSL VPN access.<br><br>Leave this field to the default settings unless it conflicts with another interface. |
| SSL VPN Login Domain Name | |
| SSL VPN Login Domain Name 1/2 | Specify a domain name for users to use for SSL VPN login. The domain name must be registered to one of the ZyWALL's IP addresses or be one of the ZyWALL's DDNS entries. You can specify up to two domain names so you could use one domain name for each of two WAN ports. Do not include the host. For example, www.zyxel.com is a fully qualified domain name where "www" is the host; so you would just use "zyxel.com".<br><br>The ZyWALL displays the normal login screen without the button for logging into the Web Configurator as shown next.<br><br>**Figure 265** SSL VPN Login Screen<br>  |
| Message | |
| Login Message | Specify a message to display on the screen when a user logs in and an SSL VPN connection is established successfully. You can enter up to 60 characters ("a-z", A-Z", "0-9") with spaces allowed. |
| Logout Message | Specify a message to display on the screen when a user logs out and the SSL VPN connection is terminated successfully. You can enter up to 60 characters ("a-z", A-Z", "0-9") with spaces allowed. |

**Table 135** VPN > SSL VPN > Global Setting (continued)

| LABEL | DESCRIPTION |
|---|---|
| Update Client Virtual Desktop Logo | You can upload a graphic logo to be displayed on the web browser on the remote user computer. The ZyXEL company logo is the default logo.<br>Specify the location and file name of the logo graphic or click **Browse** to locate it.<br>Note: The logo graphic must be GIF, JPG, or PNG format. The graphic should use a resolution of 127 x 57 pixels to avoid distortion when displayed. The ZyWALL automatically resizes a graphic of a different resolution to 127 x 57 pixels. The file size must be 100 kilobytes or less. Transparent background is recommended. |
| Browse | Click **Browse** to locate the graphic file on your computer. |
| Upload | Click **Upload** to transfer the specified graphic file from your computer to the ZyWALL. |
| Reset Logo to Default | Click **Reset Logo to Default** to display the ZyXEL company logo on the remote user's web browser. |
| Apply | Click **Apply** to save the changes and/or start the logo file upload process. |
| Reset | Click **Reset** to start configuring this screen again. |

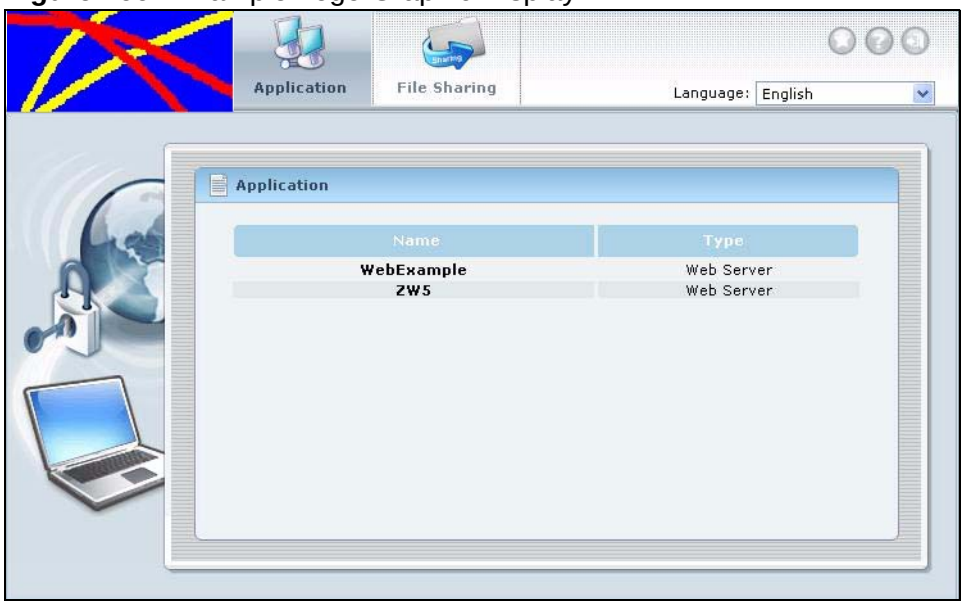
## 22.4.1 How to Upload a Custom Logo

Follow the steps below to upload a custom logo to display on the remote user SSL VPN screens.

1. Click **VPN > SSL VPN** and click the **Global Setting** tab to display the configuration screen.
2. Click **Browse** to locate the logo graphic. Make sure the file is in GIF, JPG, or PNG format.
3. Click **Apply** to start the file transfer process.
4. Log in as a user to verify that the new logo displays properly.

The following shows an example logo on the remote user screen.

**Figure 266** Example Logo Graphic Display

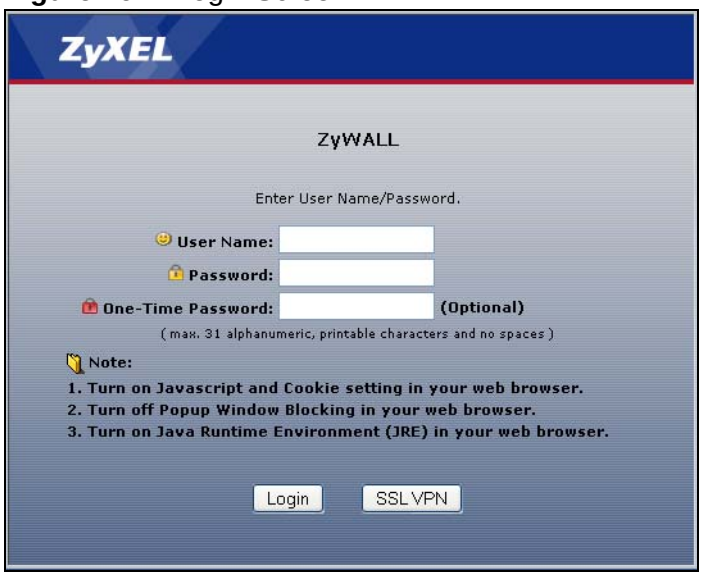



# 22.5 Establishing an SSL VPN Connection

After you have configured the SSL VPN settings on the ZyWALL, use the ZyWALL login screen's SSL VPN button to establish an SSL VPN connection. See Section 23.2 on page 418 for details.

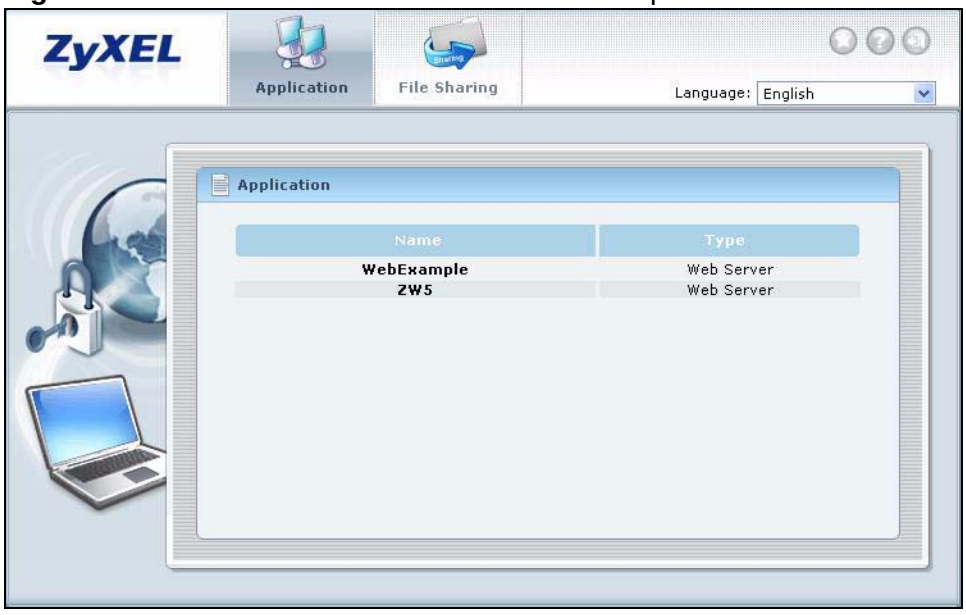
1 Display the ZyWALL's login screen and enter your user account information (the user name and password). Click **SSL VPN**.

**Figure 267** Login Screen




2 SSL VPN connection starts. This may take several minutes depending on your network connection. Once the connection is up, you should see the client portal screen. The following shows an example.

**Figure 268** SSL VPN Client Portal Screen Example




If the user account is not set up for SSL VPN access, an "SSL VPN connection is not activated" message displays in the **Login** screen. Clear the **Login to SSL VPN** check box and try logging in again.

For more information on user portal screens, refer to Chapter 23 on page 417.

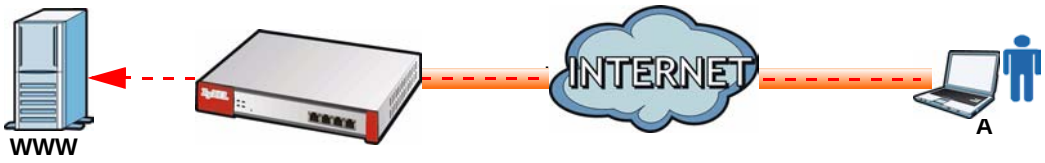
# 23

# SSL User Screens

## 23.1 Overview

This chapter introduces the remote user SSL VPN screens. The following figure shows a network example where a remote user (**A**) logs into the ZyWALL from the Internet to access the web server (**WWW**) on the local network.

**Figure 269** Network Example




### 23.1.1 What You Need to Know About the SSL User Screens

The ZyWALL can use SSL VPN to provide secure connections to network resources such as applications, files, intranet sites or e-mail through a web-based interface and using Microsoft Outlook Web Access (OWA).

#### Network Resource Access Methods

As a remote user, you can access resources on the local network using one of the following methods.

- Using a supported web browser

  Once you have successfully logged in through the ZyWALL, you can access intranet sites, web-based applications, or web-based e-mails using one of the supported web browsers.

- Using the ZyWALL SecuExtender client

  Once you have successfully logged into the ZyWALL, the ZyWALL automatically loads the ZyWALL SecuExtender client program to your computer. With the ZyWALL SecuExtender, you can access network resources, remote desktops and manage files as if you were on the local network. See Chapter 26 on page 437 for more on the ZyWALL SecuExtender.

### System Requirements

Here are the browser and computer system requirements for remote user access.

- Windows 2000, Vista, or a 32-bit version of XP or 2003
- Internet Explorer 5.5 and above (for Internet Explorer 7 or 8, JRE 1.6 must be enabled)
- Using RDP requires Internet Explorer
- Netscape 7.2 and above
- Firefox 1.0 and above
- Mozilla 1.7.3 and above
- Sun's Java (Java Runtime Environment or 'JRE') installed and enabled with a minimum version of 1.4.

### Required Information

A remote user needs the following information from the network administrator to log in and access network resources.

- the domain name or IP address of the ZyWALL
- the login account user name and password
- if also required, the user name and/or password to access the network resource

### Certificates

The remote user's computer establishes an HTTPS connection to the ZyWALL to access the login screen. If instructed by your network administrator, you must install or import a certificate (provided by the ZyWALL or your network administrator). Refer to Appendix D on page 915 for more information.

### Finding Out More

See Chapter 22 on page 405 for how to configure SSL VPN on the ZyWALL.

## 23.2 Remote User Login

This section shows you how to access and log into the network through the ZyWALL. Example screens for Internet Explorer are shown.

1 Open a web browser and enter the web site address or IP address of the ZyWALL. For example, “http://sslvpn.mycompany.com”.

**Figure 270** Enter the Address in a Web Browser

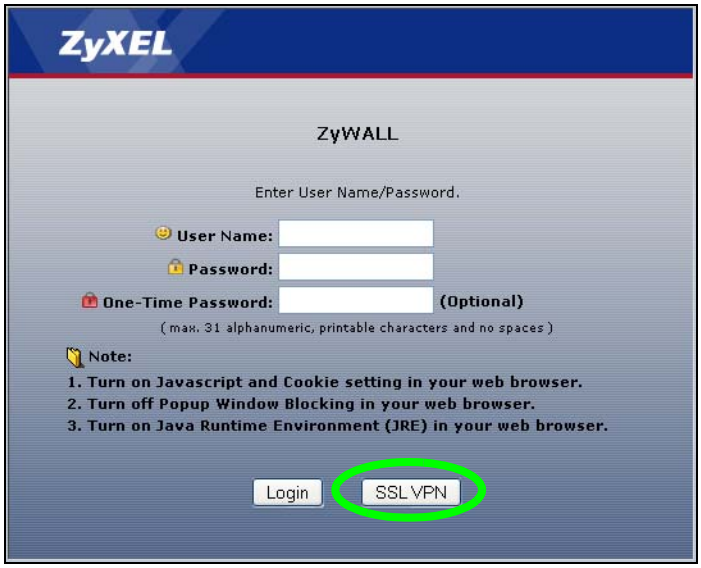

2 Click **OK** or **Yes** if a security screen displays.

**Figure 271** Login Security Screen


3 A login screen displays. Enter the user name and password of your login account. If a token password is also required, enter it in the **One-Time Password** field.

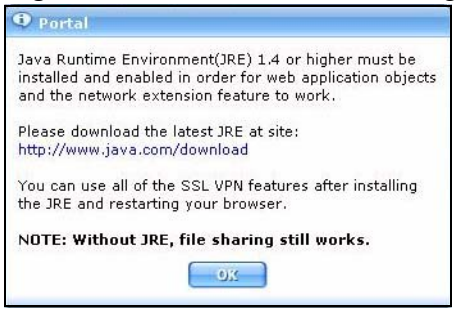
4 Click **SSL VPN** to log in and establish an SSL VPN connection to the network to access network resources.

**Figure 272** Login Screen



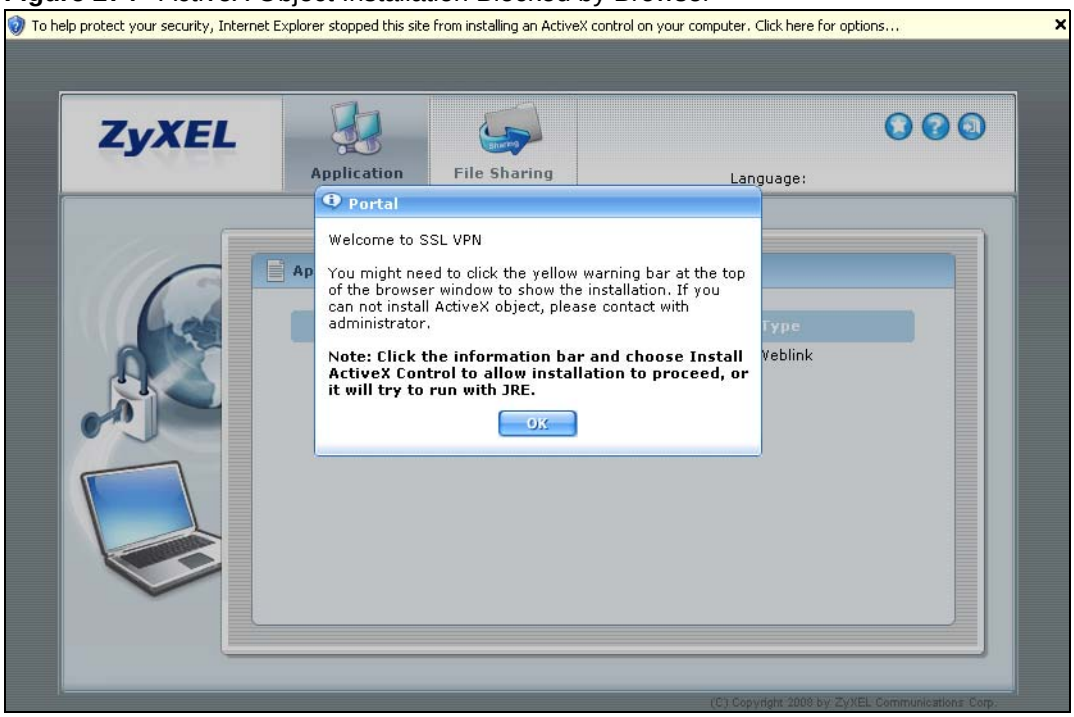
5 Your computer starts establishing a secure connection to the ZyWALL after a successful login. This may take up to two minutes. If you get a message about needing Java, download and install it and restart your browser and re-login. If a certificate warning screen displays, click **OK**, **Yes** or **Continue**.

**Figure 273** Java Needed Message




6 The ZyWALL tries to install the SecuExtender client. As shown next, you may have to click some pop-ups to get your browser to allow the installation.

**Figure 274** ActiveX Object Installation Blocked by Browser




7 The ZyWALL tries to install the SecuExtender client. You may need to click a pop-up to get your browser to allow this. In Internet Explorer, click **Install**.

**Figure 275** SecuExtender Blocked by Internet Explorer


**8** The ZyWALL tries to run the "ssltun" application. You may need to click something to get your browser to allow this. In Internet Explorer, click **Run**.

**Figure 276** SecuExtender Progress


**9** Click **Next** to use the setup wizard to install the SecuExtender client on your computer.

**Figure 277** SecuExtender Progress

**10** If a screen like the following displays, click **Continue Anyway** to finish installing the SecuExtender client on your computer.

**Figure 278** Hardware Installation Warning

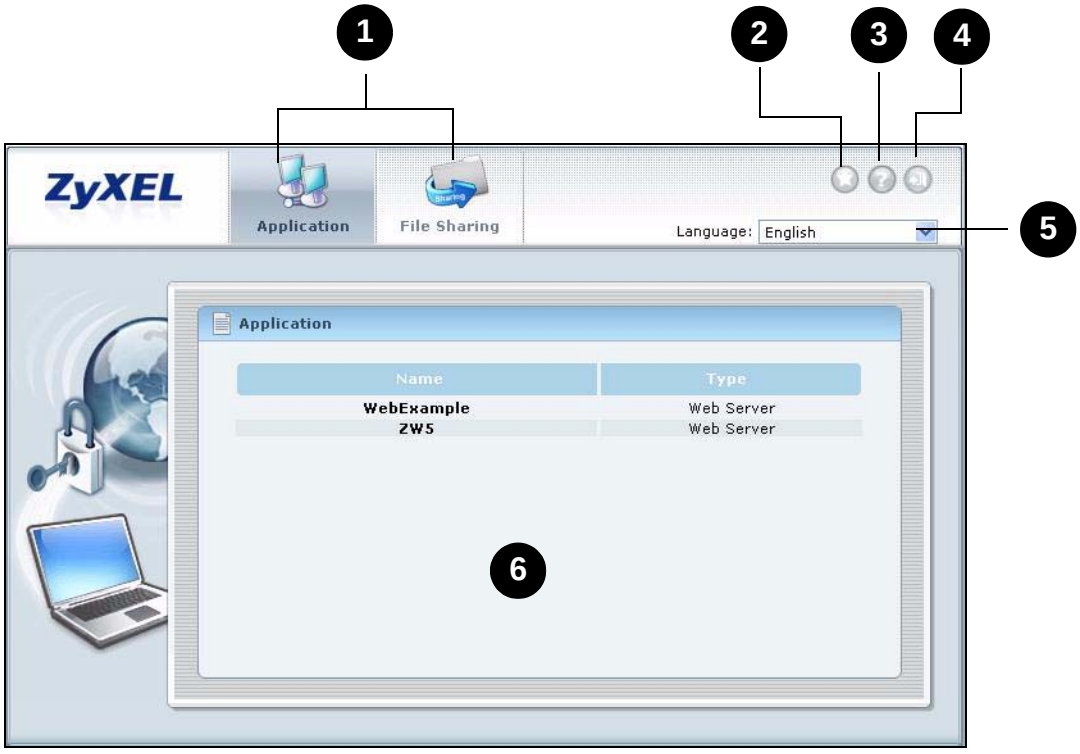

**11** The **Application** screen displays showing the list of resources available to you. See Figure 279 on page 423 for a screen example.

Note: Available resource links vary depending on the configuration your network administrator made.

# 23.3 The SSL VPN User Screens

This section describes the main elements in the remote user screens.

**Figure 279** Remote User Screen




The following table describes the various parts of a remote user screen.

**Table 136** Remote User Screen Overview

| # | DESCRIPTION |
|---|---|
| 1 | Click on a menu tab to go to the **Application** or **File Sharing** screen. |
| 2 | Click this icon to create a bookmark to the SSL VPN user screen in your web browser. |
| 3 | Click this icon to display the on-line help window. |
| 4 | Click this icon to log out and terminate the secure connection. |
| 5 | Select your preferred language for the interface. |
| 6 | This part of the screen displays a list of the resources available to you.<br>In the **Application** screen, click on a link to access or display the access method.<br>In the **File Sharing** screen, click on a link to open a file or directory. |

# 23.4 Bookmarking the ZyWALL

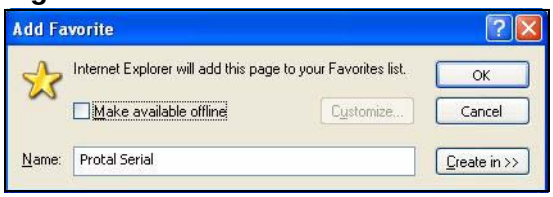
You can create a bookmark of the ZyWALL by clicking the **Add to Favorite** icon. This allows you to access the ZyWALL using the bookmark without having to enter the address every time.

1 In any remote user screen, click the **Add to Favorite** icon.

2 A screen displays. Accept the default name in the **Name** field or enter a descriptive name to identify this link.

3 Click **OK** to create a bookmark in your web browser.

**Figure 280** Add Favorite




# 23.5 Logging Out of the SSL VPN User Screens

To properly terminate a connection, click on the **Logout** icon in any remote user screen.

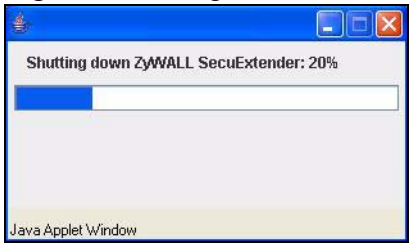
1 Click the **Logout** icon in any remote user screen.

2 A prompt window displays. Click **OK** to continue.

**Figure 281** Logout: Prompt

3 An information screen displays to indicate that the SSL VPN connection is about to terminate.

**Figure 282** Logout: Connection Termination Progress



# 24

# SSL User Application Screens

## 24.1 SSL User Application Screens Overview

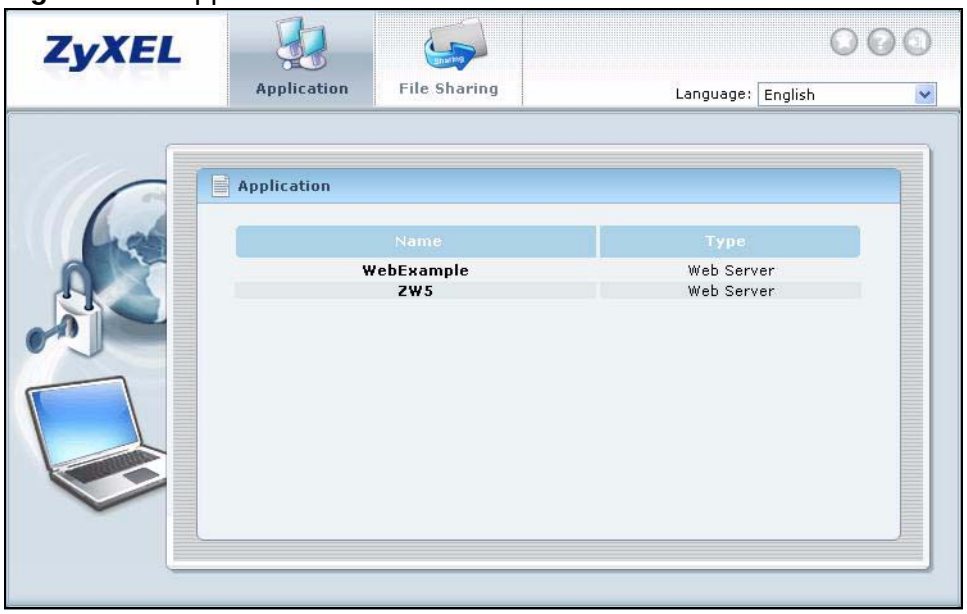
Use the **Application** screen to access web-based applications (such as web sites and e-mail) on the network through the SSL VPN connection. Which applications you can access depends on the ZyWALL's configuration.

## 24.2 The Application Screen

Click the **Application** tab to display the screen. The **Name** field displays the descriptive name for an application. The **Type** field displays wether the application is a web site (**Web Server**) or web-based e-mail using Microsoft Outlook Web Access (**OWA**).

To access a web-based application, simply click a link in the **Application** screen to display the web screen in a separate browser window.

**Figure 283** Application



# 25

# SSL User File Sharing

## 25.1 Overview

The **File Sharing** screen lets you access files on a file server through the SSL VPN connection.

### 25.1.1 What You Need to Know About the SSL VPN File Sharing

Use the **File Sharing** screen to display and access shared files/folders on a file server.

You can also perform the following actions:

- Access a folder.
- Open a file (if your web browser cannot open the file, you are prompted to download it).
- Save a file to your computer.
- Create a new folder.
- Rename a file or folder.
- Delete a file or folder.
- Upload a file.

Note: Available actions you can perform in the **File Sharing** screen vary depending on the rights granted to you on the file server.

# 25.2 The Main File Sharing Screen

The first **File Sharing** screen displays the name(s) of the shared folder(s) available. The following figure shows an example with one file share.

**Figure 284** File Sharing


# 25.3 Opening a File or Folder

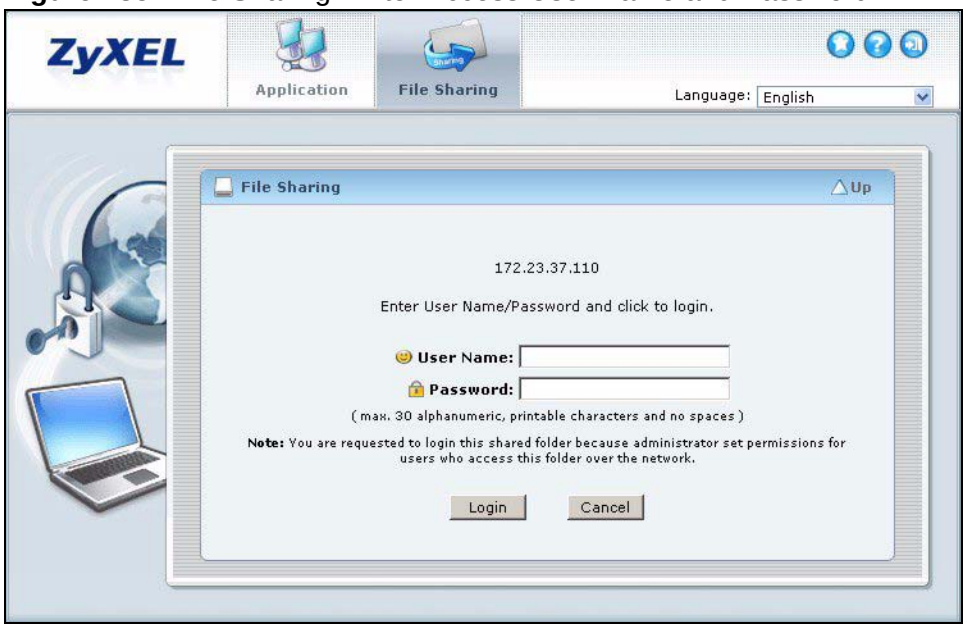
You can open a file if the file extension is recognized by the web browser and the associated application is installed on your computer.

1 Log in as a remote user and click the **File Sharing** tab.

2 Click on a file share icon.

3 If an access user name and password are required, a screen displays as shown in the following figure. Enter the account information and click **Login** to continue.

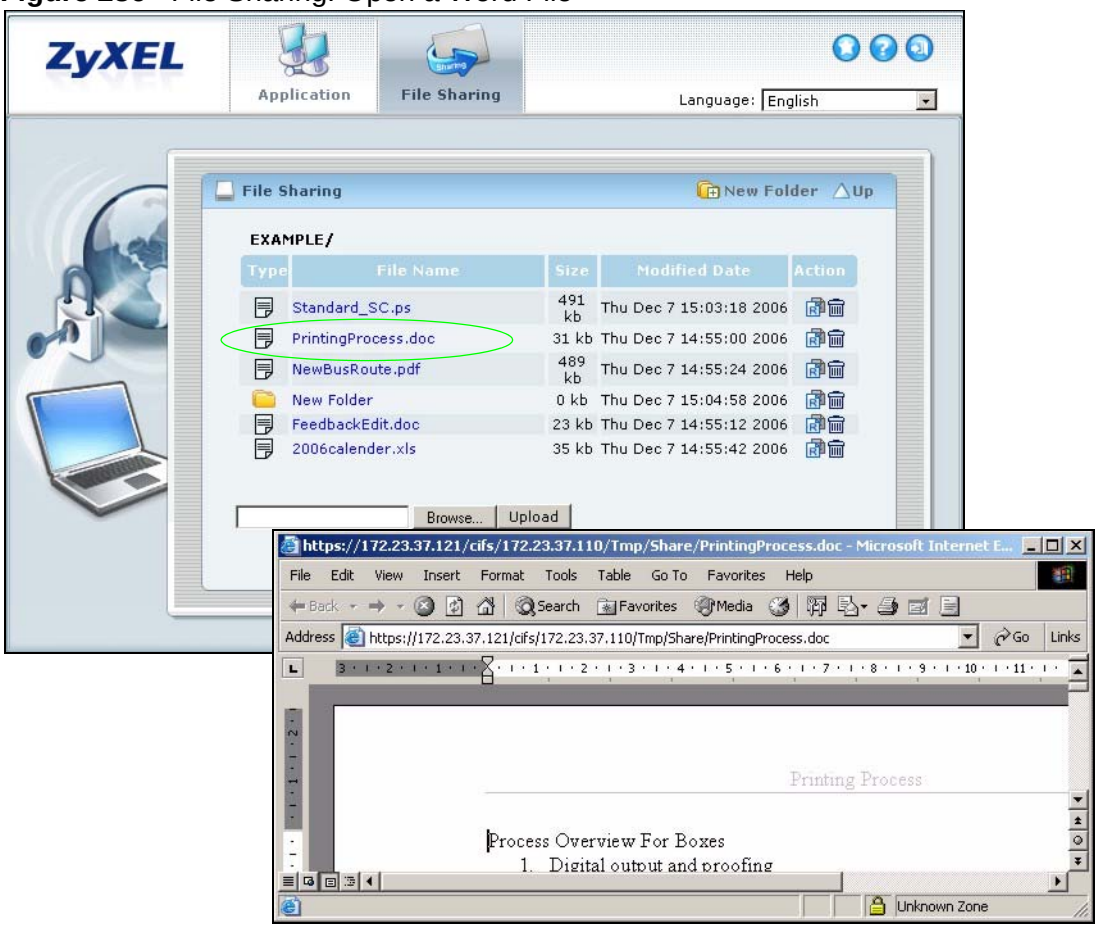
**Figure 285** File Sharing: Enter Access User Name and Password



4 A list of files/folders displays. Click on a file to open it in a separate browser window. You can also click a folder to access it.

For this example, click on a .doc file to open the Word document.

**Figure 286** File Sharing: Open a Word File




## 25.3.1 Downloading a File

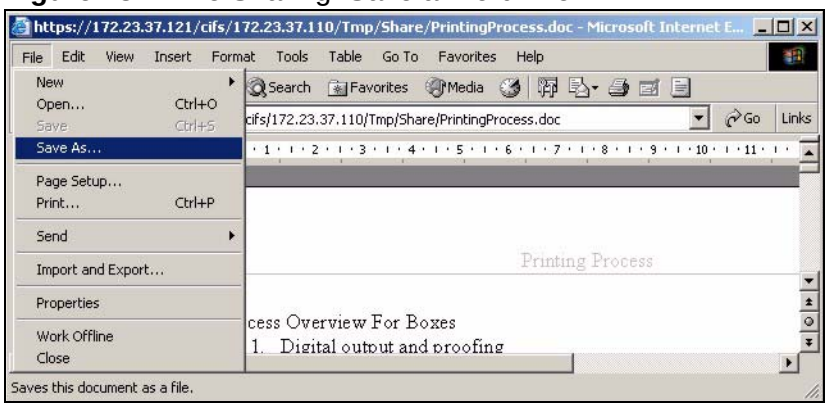
You are prompted to download a file which cannot be opened using a web browser.

Follow the on-screen instructions to download and save the file to your computer. Then launch the associated application to open the file.

### 25.3.2 Saving a File

After you have opened a file in a web browser, you can save a copy of the file by clicking **File > Save As** and following the on-screen instructions.

**Figure 287** File Sharing: Save a Word File



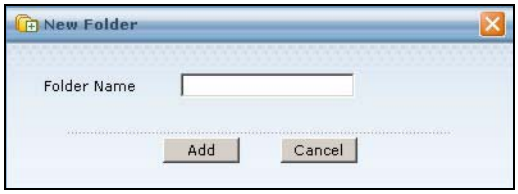

## 25.4 Creating a New Folder

To create a new folder in the file share location, click the **New Folder** icon.

Specify a descriptive name for the folder. You can enter up to 356 characters. Then click **Add**.

Note: Make sure the length of the folder name does not exceed the maximum allowed on the file server.

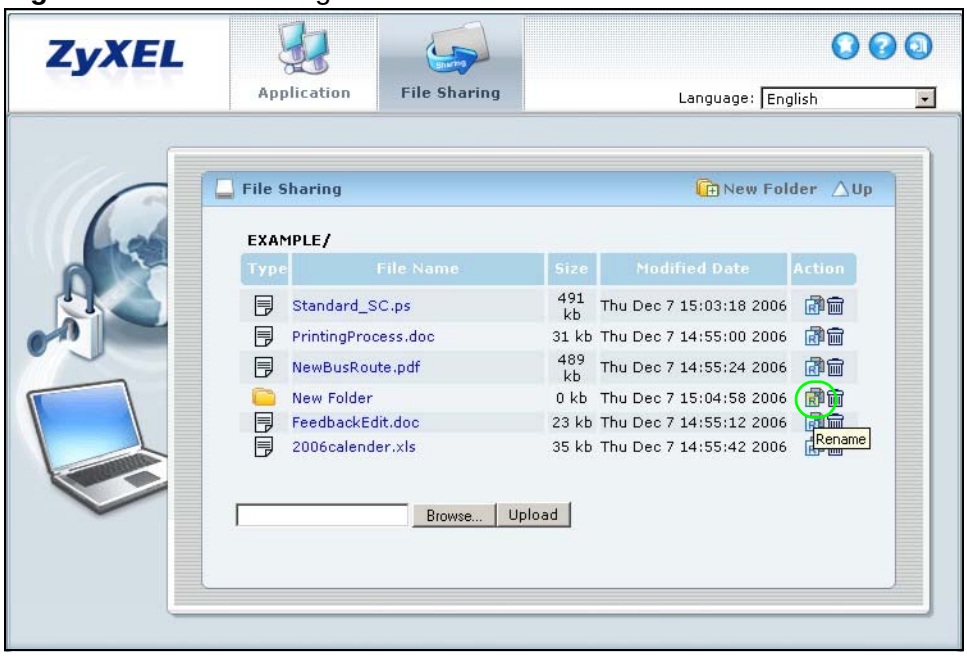
**Figure 288** File Sharing: Save a Word File



# 25.5 Renaming a File or Folder

To rename a file or folder, click the **Rename** icon next to the file/folder.

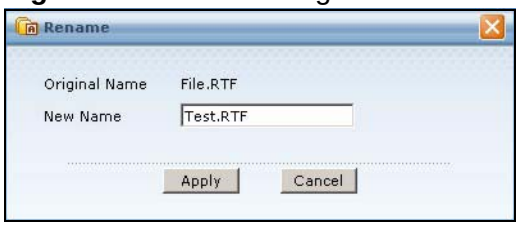
**Figure 289** File Sharing: Rename




A popup window displays. Specify the new name and/or file extension in the field provided. You can enter up to 356 characters. Then click **Apply**.

Note: Make sure the length of the name does not exceed the maximum allowed on the file server.
You may not be able to open a file if you change the file extension.

**Figure 290** File Sharing: Rename




# 25.6 Deleting a File or Folder

Click the **Delete** icon next to a file or folder to remove it.

# 25.7 Uploading a File

Follow the steps below to upload a file to the file server.

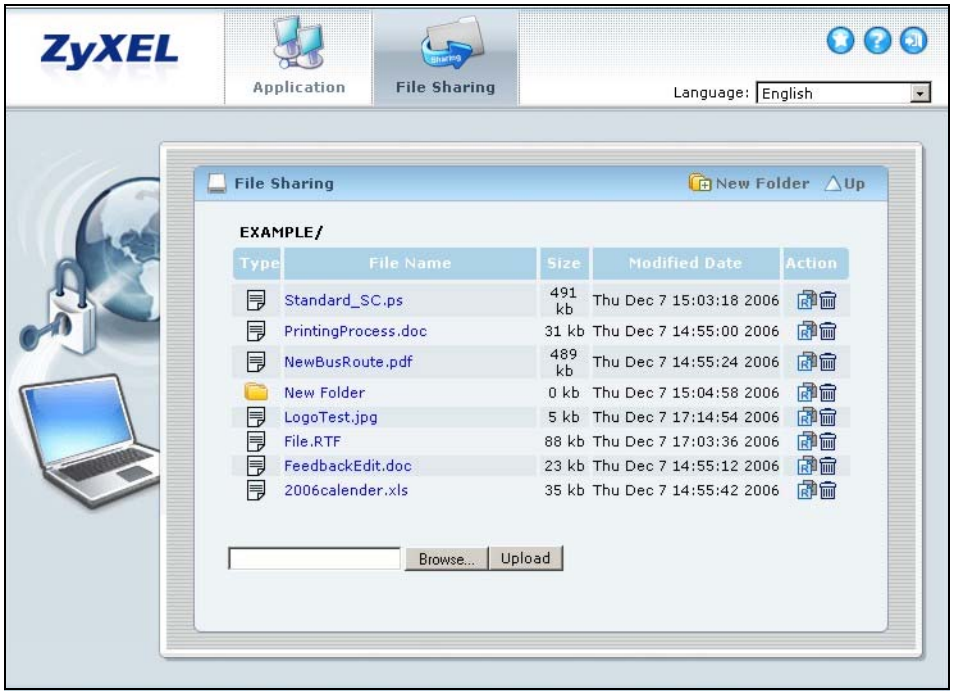
1 Log into the remote user screen and click the **File Sharing** tab.

2 Specify the location and/or name of the file you want to upload. Or click **Browse** to locate it.

3 Click **Upload** to send the file to the file server.

4 After the file is uploaded successfully, you should see the name of the file and a message in the screen.

**Figure 291** File Sharing: File Upload




Note: Uploading a file with the same name and file extension replaces the existing file on the file server. No warning message is displayed.

# 26

# ZyWALL SecuExtender

The ZyWALL automatically loads the ZyWALL SecuExtender client program to your computer after a successful login. The ZyWALL SecuExtender lets you:

- Access servers, remote desktops and manage files as if you were on the local network.
- Use applications like e-mail, file transfer, and remote desktop programs directly without using a browser. For example, you can use Outlook for e-mail instead of the ZyWALL's web-based e-mail.
- Use applications, even proprietary applications, for which the ZyWALL does not offer SSL application objects.

The applications must be installed on your computer. For example, to use the VNC remote desktop program, you must have the VNC client installed on your computer.

## 26.1 The ZyWALL SecuExtender Icon

The ZyWALL SecuExtender icon color indicates the SSL VPN tunnel's connection status.

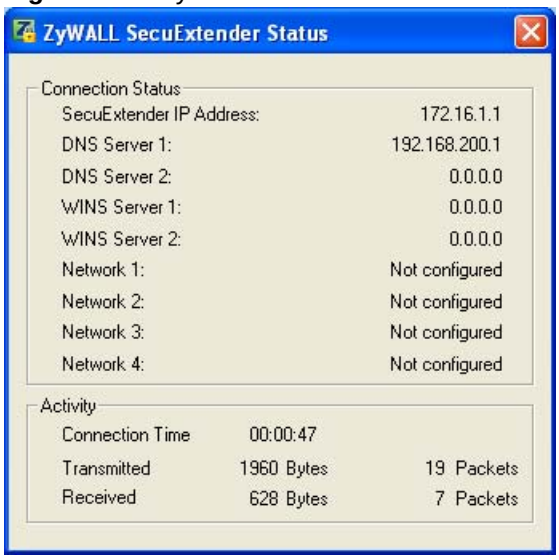
**Figure 292** ZyWALL SecuExtender Icon

- Red: the SSL VPN tunnel is not connected. You cannot connect to the SSL application and network resources.
- Green: the SSL VPN tunnel is connected. You can connect to the SSL application and network resources.You can also use another application to access resources behind the ZyWALL.
- Gray: the SSL VPN tunnel's connection is suspended. This means the SSL VPN tunnel is connected, but the ZyWALL SecuExtender will not send any traffic through it until you right-click the icon and resume the connection.

## 26.2 Statistics

Right-click the ZyWALL SecuExtender icon in the system tray and select **Status** to open the **Status** screen. Use this screen to view the ZyWALL SecuExtender's statistics.

**Figure 293** ZyWALL SecuExtender Status




The following table describes the labels in this screen.

**Table 137** ZyWALL SecuExtender Statistics

| LABEL | DESCRIPTION |
|---|---|
| Connection Status | |
| SecuExtender IP Address | This is the IP address the ZyWALL assigned to this remote user computer for an SSL VPN connection. |
| DNS Server 1/2 | These are the IP addresses of the DNS server and backup DNS server for the SSL VPN connection.<br>DNS (Domain Name System) maps a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. Your computer uses the DNS server specified here to resolve domain names for resources you access through the SSL VPN connection. |
| WINS Server 1/2 | These are the IP addresses of the WINS (Windows Internet Naming Service) and backup WINS servers for the SSL VPN connection. The WINS server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using. |
| Network 1~4 | These are the networks (including netmask) that you can access through the SSL VPN connection. |
| Activity | |
| Connected Time | This is how long the computer has been connected to the SSL VPN tunnel. |
| Transmitted | This is how many bytes and packets the computer has sent through the SSL VPN connection. |
| Received | This is how many bytes and packets the computer has received through the SSL VPN connection. |

## 26.3 View Log

If you have problems with the ZyWALL SecuExtender, customer support may request you to provide information from the log. Right-click the ZyWALL SecuExtender icon in the system tray and select **Log** to open a notepad file of the ZyWALL SecuExtender's log.

**Figure 294** ZyWALL SecuExtender Log Example

```
################################################################################
####################
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DETAIL]  Build Datetime: Feb 24
2009/10:25:07
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DEBUG]   rasphone.pbk:
C:\Documents and Settings\11746\rasphone.pbk
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DEBUG]   SecuExtender.log:
C:\Documents and Settings\11746\SecuExtender.log
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DETAIL]  Check Parameters
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DETAIL]  Connect to
172.23.31.19:443/10444
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DETAIL]  Parameter is OK
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DETAIL]  Checking System
status...
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DETAIL]  Checking service
(first) ...
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DETAIL]  SecuExtender Helper is
running
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DETAIL]  System is OK
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DEBUG]   Connect to 2887196435/
443
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DETAIL]  Handshake LoopCounter:
0
[ 2009/03/12 13:35:50 ][SecuExtender Agent][DETAIL]  611 bytes of handshake
data received
```

## 26.4 Suspend and Resume the Connection

When the ZyWALL SecuExtender icon in the system tray is green, you can right-click the icon and select **Suspend Connection** to keep the SSL VPN tunnel connected but not send any traffic through it until you right-click the icon and resume the connection.

## 26.5 Stop the Connection

Right-click the icon and select **Stop Connection** to disconnect the SSL VPN tunnel.

## 26.6 Uninstalling the ZyWALL SecuExtender

Do the following if you need to remove the ZyWALL SecuExtender.

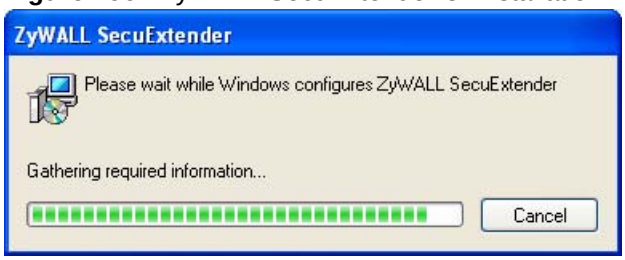
1. Click **start** > **All Programs** > **ZyXEL** > **ZyWALL SecuExtender** > **Uninstall**.

2 In the confirmation screen, click **Yes**.

**Figure 295** Uninstalling the ZyWALL SecuExtender Confirmation


3 Windows uninstalls the ZyWALL SecuExtender.

**Figure 296** ZyWALL SecuExtender Uninstallation



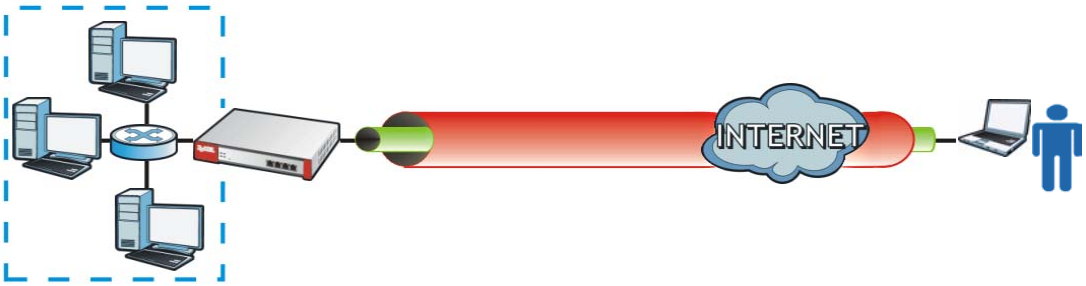
# 27

# L2TP VPN

## 27.1 Overview

L2TP VPN lets remote users use the L2TP and IPSec client software included with their computers' operating systems to securely connect to the network behind the ZyWALL. The remote users do not need their own IPSec gateways or VPN client software.

**Figure 297** L2TP VPN Overview




### 27.1.1 What You Can Do in the L2TP VPN Screens

- Use the **L2TP VPN** screen (see Section 27.2 on page 443) to configure the ZyWALL's L2TP VPN settings.
- Use the **L2TP VPN** screen (see Section 27.3 on page 444) to display and manage the ZyWALL's connected L2TP VPN sessions.

### 27.1.2 What You Need to Know About L2TP VPN

The Layer 2 Tunneling Protocol (L2TP) works at layer 2 (the data link layer) to tunnel network traffic between two peers over another network (like the Internet). In L2TP VPN, an IPSec VPN tunnel is established first and then an L2TP tunnel is built inside it. See Chapter 21 on page 363 for information on IPSec VPN.

#### IPSec Configuration Required for L2TP VPN

You must configure an IPSec VPN connection for L2TP VPN to use (see Chapter 21 on page 363 for details). The IPSec VPN connection must:

- Be enabled.
- Use transport mode.
- Not be a manual key VPN connection.
- Use **Pre-Shared Key** authentication.
- Use a VPN gateway with the **Secure Gateway** set to **0.0.0.0** if you need to allow L2TP VPN clients to connect from more than one IP address.

### Using the Default L2TP VPN Connection

**Default_L2TP_VPN_Connection** is pre-configured to be convenient to use for L2TP VPN. If you use it, edit the following.

Configure the local and remote policies as follows.

- For the **Local Policy**, create an address object that uses host type and contains the **My Address** IP address that you configured in the **Default_L2TP_VPN_GW**. Use this address object in the local policy.
- For the **Remote Policy**, create an address object that uses host type and an IP address of 0.0.0.0. Use this address object in the remote policy.

You must also edit the **Default_L2TP_VPN_GW** gateway entry.

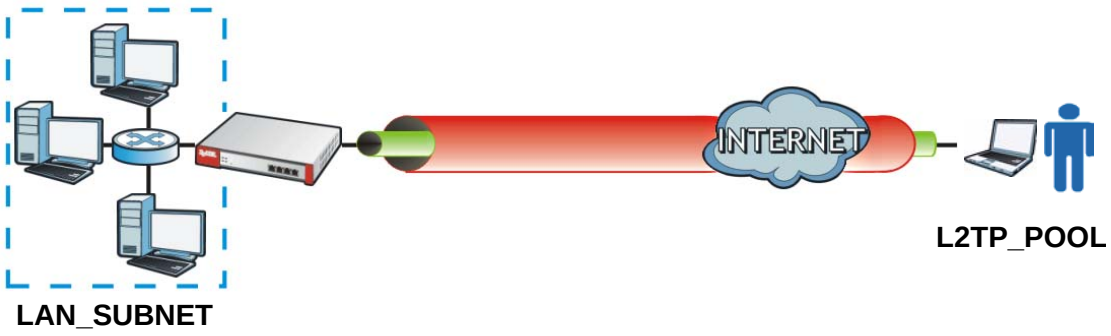
- Configure the **My Address** setting according to your requirements.
- Replace the default **Pre-Shared Key**.

### Policy Route

You must configure a policy route to let remote users access resources on a network behind the ZyWALL.

- Set the policy route's **Source Address** to the address object that you want to allow the remote users to access (**LAN_SUBNET** in the following figure).
- Set the **Destination Address** to the IP address pool that the ZyWALL assigns to the remote users (**L2TP_POOL** in the following figure).
- Set the next hop to be the VPN tunnel that you are using for L2TP.

**Figure 298** Policy Route for L2TP VPN



### Finding Out More

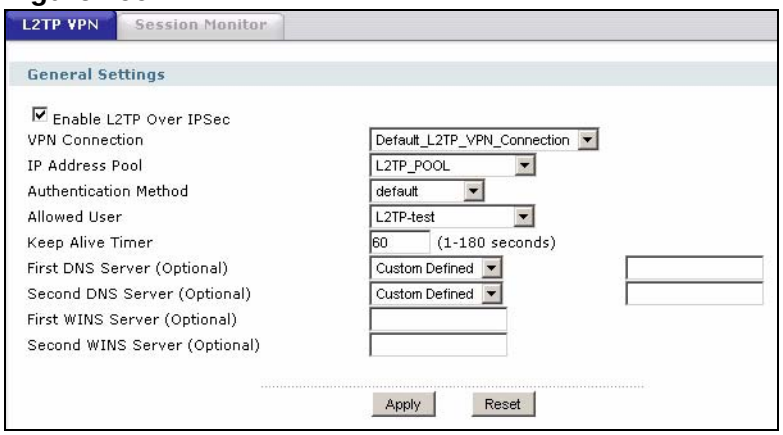
- See Section 5.4.6 on page 88 for related information on these screens.
- See Chapter 28 on page 447 for an example of how to create a basic L2TP VPN tunnel.

## 27.2 L2TP VPN Screen

Click **VPN > L2TP VPN** to open the following screen. Use this screen to configure the ZyWALL's L2TP VPN settings.

Note: Disconnect any existing L2TP VPN sessions before modifying L2TP VPN settings. The remote users must make any needed matching configuration changes and re-establish the sessions using the new settings.

**Figure 299** VPN > L2TP VPN




The following table describes the fields in this screen.

**Table 138** VPN > IPSec VPN > VPN Connection

| LABEL | DESCRIPTION |
|---|---|
| Enable L2TP Over IPSec | Use this field to turn the ZyWALL's L2TP VPN function on or off. |
| VPN Connection | Select the IPSec VPN connection the ZyWALL uses for L2TP VPN. All of the configured VPN connections display here, but the one you use must meet the requirements listed in IPSec Configuration Required for L2TP VPN on page 441.<br><br>Note: Modifying this VPN connection (or the VPN gateway that it uses) disconnects any existing L2TP VPN sessions. |
| IP Address Pool | Select the pool of IP addresses that the ZyWALL uses to assign to the L2TP VPN clients. Select **Create Object** to configure a new pool of IP addresses. |

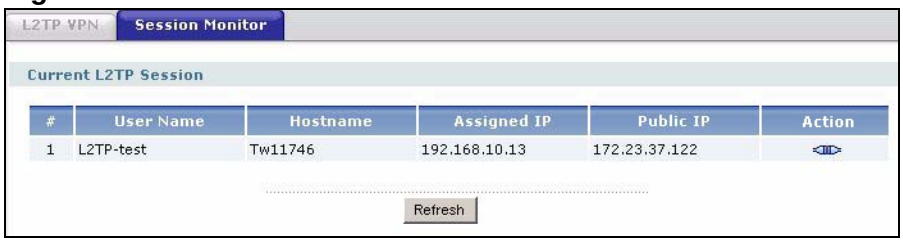
**Table 138** VPN > IPSec VPN > VPN Connection (continued)

| LABEL | DESCRIPTION |
|---|---|
| Authentication Method | Select how the ZyWALL authenticates a remote user before allowing access to the L2TP VPN tunnel.<br><br>The authentication method has the ZyWALL check a user's user name and password against the ZyWALL's local database, a remote LDAP, RADIUS, a Active Directory server, or more than one of these. See Chapter 42 on page 695 for how to create authentication method objects. |
| Allowed User | The remote user must log into the ZyWALL to use the L2TP VPN tunnel.<br><br>Select a user or user group that can use the L2TP VPN tunnel. Select **Create Object** to configure a new user account (see Section 37.2.1 on page 652 for details). Otherwise, select **any** to allow any user with a valid account and password on the ZyWALL to log in. |
| Keep Alive Timer | The ZyWALL sends a Hello message after waiting this long without receiving any traffic from the remote user. The ZyWALL disconnects the VPN tunnel if the remote user does not respond. |
| First DNS Server<br><br>Second DNS Server | Specify the IP addresses of DNS servers to assign to the remote users. You can specify these IP addresses two ways.<br><br>**Custom Defined** - enter a static IP address.<br><br>**From ISP** - use the IP address of a DNS server that another interface received from its DHCP server. |
| First WINS Server, Second WINS Server | The WINS (Windows Internet Naming Service) server keeps a mapping table of the computer names on your network and the IP addresses that they are currently using.<br><br>Type the IP addresses of up to two WINS servers to assign to the remote users. You can specify these IP addresses two ways. |
| Apply | Click **Apply** to save your changes in the ZyWALL. |
| Reset | Click **Cancel** to start configuring this screen afresh. |

# 27.3 L2TP VPN Session Monitor Screen

Click **VPN > L2TP VPN > Session Monitor** to open the following screen. Use this screen to display and manage the ZyWALL's connected L2TP VPN sessions.

**Figure 300** VPN > L2TP VPN > Session Monitor



The following table describes the fields in this screen.

**Table 139** VPN > L2TP VPN > Session Monitor

| LABEL | DESCRIPTION |
|---|---|
| # | This is the index number of a current L2TP VPN session. |
| User Name | This field displays the remote user's user name. |
| Hostname | This field displays the name of the computer that has this L2TP VPN connection with the ZyWALL. |
| Assigned IP | This field displays the IP address that the ZyWALL assigned for the remote user's computer to use within the L2TP VPN tunnel. |
| Public IP | This field displays the public IP address that the remote user is using to connect to the Internet. |
| Action | Click the **Disconnect** icon next to an L2TP VPN connection to disconnect it. |
| Refresh | Click **Refresh** to update the information in the display. |

# 28

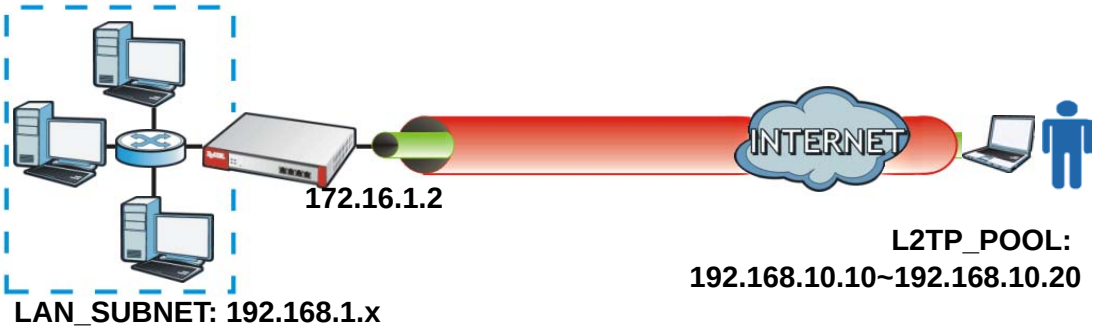
# L2TP VPN Example

This chapter shows how to create a basic L2TP VPN tunnel.

## 28.1 L2TP VPN Example

This chapter uses the following settings in creating a basic L2TP VPN tunnel.

**Figure 301** L2TP VPN Example

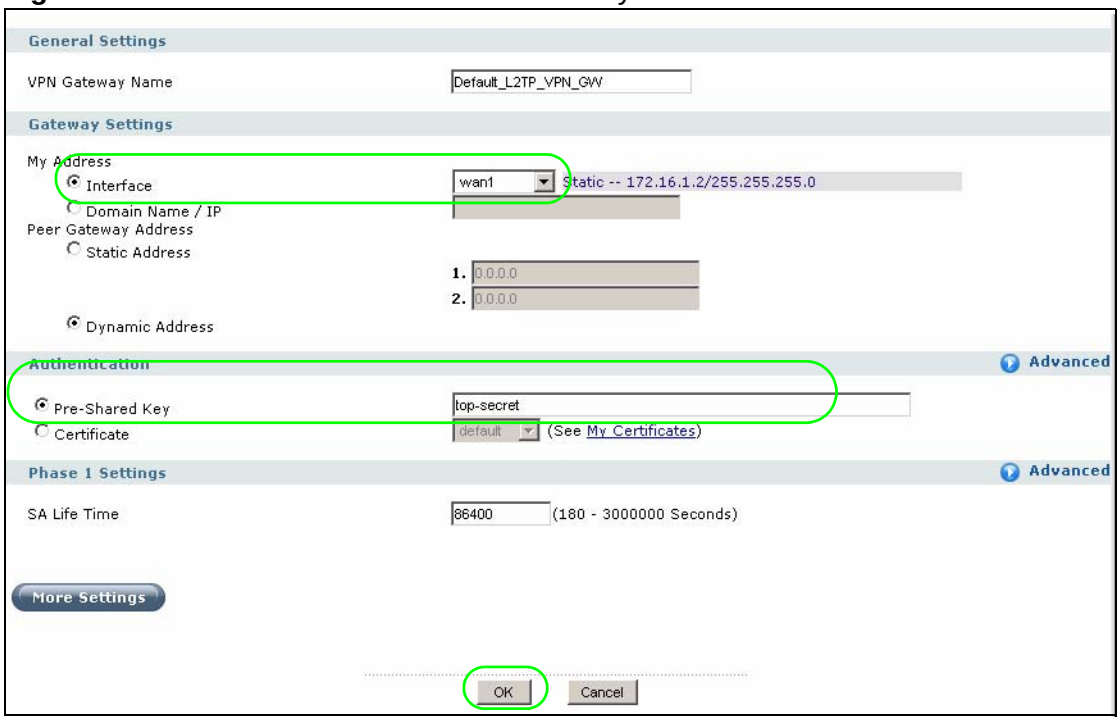



- The ZyWALL has a static IP address of 172.16.1.2 for the wan1 interface.
- The remote user has a dynamic public IP address and connects through the Internet.
- You configure an IP address pool object named **L2TP_POOL** to assign the remote users IP addresses from 192.168.10.10 to 192.168.10.20 for use in the L2TP VPN tunnel.
- The VPN rule allows the remote user to access the **LAN_SUBNET** which covers the 192.168.1.x subnet.

# 28.2 Configuring the Default L2TP VPN Gateway Example

1 Click **VPN** > **Network** > **IPSec VPN** > **VPN Gateway** to open the screen that lists the VPN gateways. Click the **Default_L2TP_VPN_GW** entry's **Edit** icon.

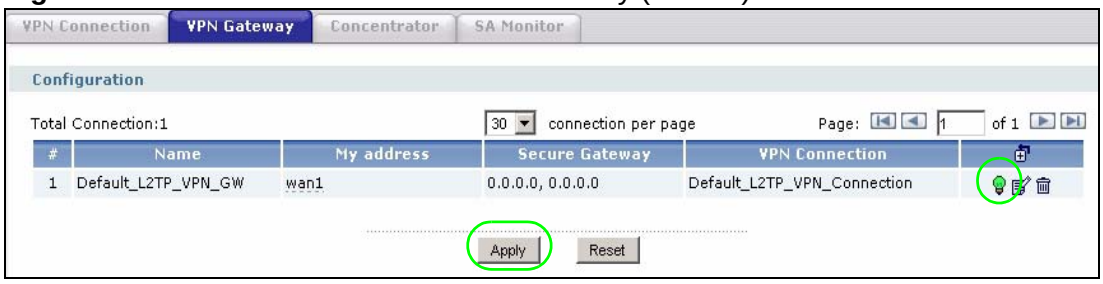
**Figure 302** VPN > IPSec VPN > VPN Gateway > Edit




- Configure the **My Address** setting. This example uses interface wan1 with static IP address 172.16.1.2.
- Select **Pre-Shared Key** and configure a password. This example uses **top-secret**. Click **OK**.

2 Click the **Default_L2TP_VPN_GW** entry's **Enable** icon and click **Apply** to turn on the entry.

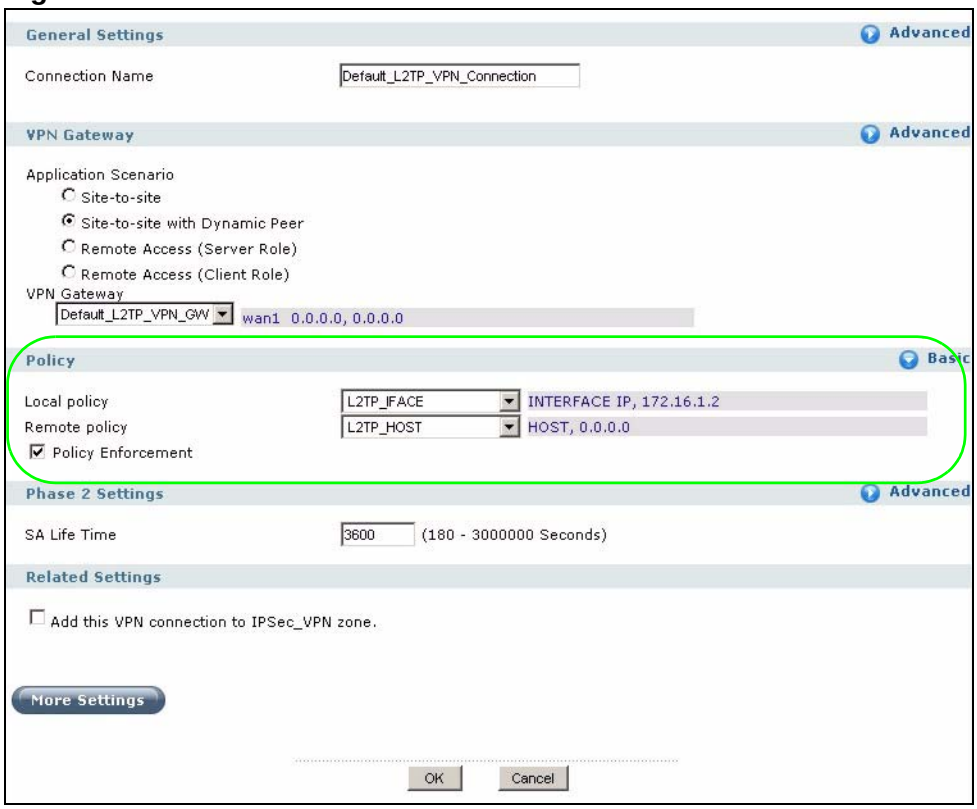
**Figure 303** VPN > IPSec VPN > VPN Gateway (Enable)



# 28.3 Configuring the Default L2TP VPN Connection Example

1 Click **VPN** > **Network** > **IPSec VPN** to open the screen that lists the VPN connections. Click the **Default_L2TP_VPN_Connection**'s **Edit** icon.

**Figure 304** VPN > IPSec VPN > VPN Connection > Edit

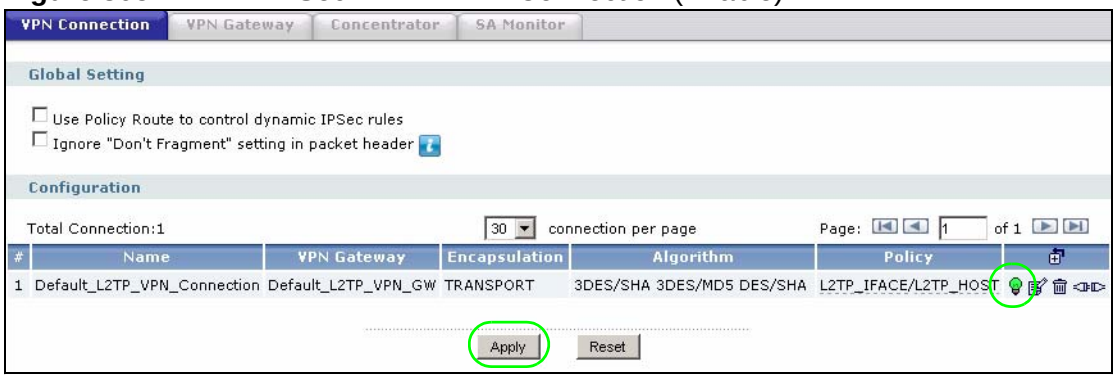



2 Click the **Policy** section's **Advanced** button. Enforce and configure the local and remote policies.

- For the **Local Policy**, create an address object that uses host type and contains the **My Address** IP address that you configured in the **Default_L2TP_VPN_GW**. The address object in this example uses the wan1 interface's IP address (172.16.1.2) and is named **L2TP_IFACE**.
- For the **Remote Policy**, create an address object that uses host type and an IP address of 0.0.0.0. It is named **L2TP_HOST** in this example.

3 Click the **Default_L2TP_VPN_Connection** entry's **Enable** icon and click **Apply** to turn on the entry.

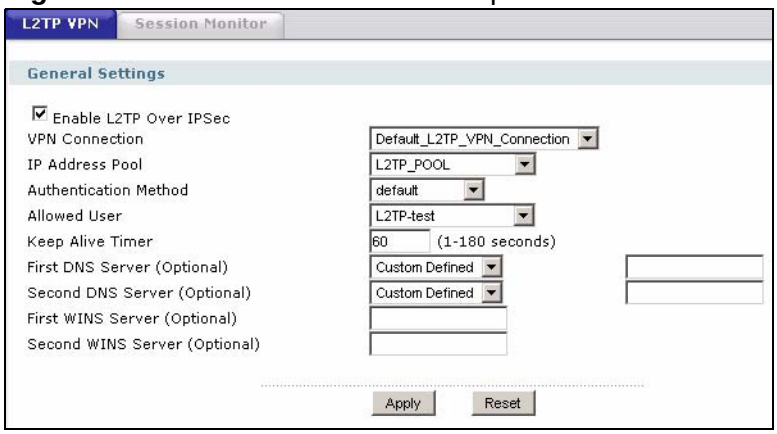
**Figure 305** VPN > IPSec VPN > VPN Connection (Enable)




# 28.4 Configuring the L2TP VPN Settings Example

1 Click **VPN > L2TP VPN** to open the following screen.

**Figure 306** VPN > L2TP VPN Example



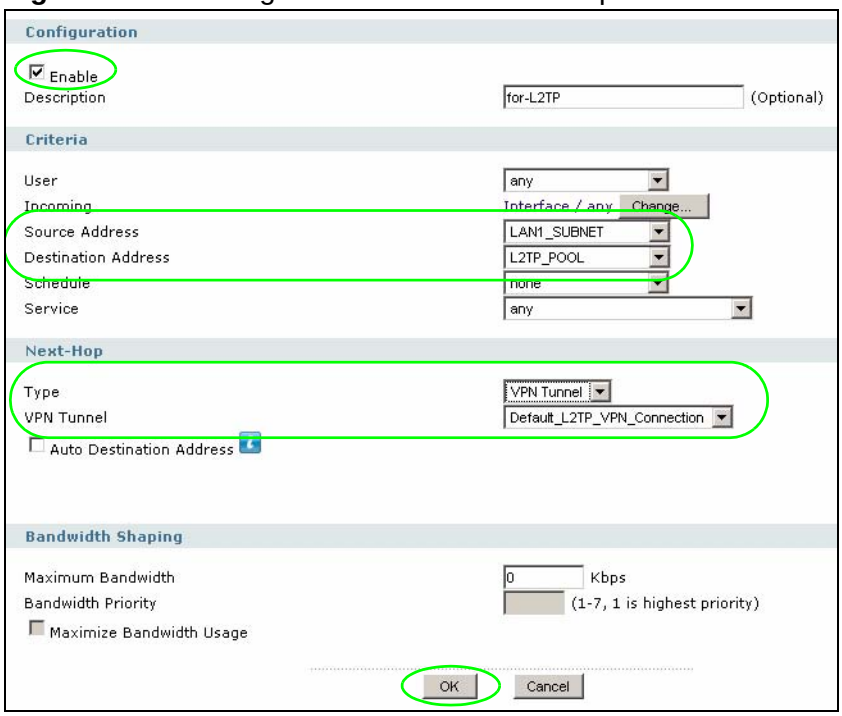

2 Configure the following.

- Enable the connection.
- Set it to use the **Default_L2TP_VPN_Connection** VPN connection.
- Configure an IP address pool for the range of 192.168.10.10 to 192.168.10.20. It is called **L2TP_POOL** here.
- This example uses the default authentication method (the ZyWALL's local user data base).
- Select a user or group of users that can use the tunnel. Here a user account named **L2TP-test** has been created.
- The other fields are left to the defaults in this example, click **Apply**.

# 28.5 Configuring the Policy Route for L2TP Example

1 Click **Routing > Add** to open the following screen.

**Figure 307** Routing > Add: L2TP VPN Example




2 Configure the following.

- Enable the policy route.
- Set the policy route's **Source Address** to the address object that you want to allow the remote users to access (**LAN1_SUBNET** in this example).
- Set the **Destination Address** to the IP address pool that the ZyWALL assigns to the remote users (**L2TP_POOL** in this example).
- Set the next hop to be the **Default_L2TP_VPN_Connection** VPN tunnel.
- Click **OK**.

# 28.6 Configuring L2TP VPN in Windows XP and 2000

The following sections cover how to configure L2TP in remote user computers using Windows XP and Windows 2000. The example settings in these sections go along with the L2TP VPN configuration example in Section 28.1 on page 447.

Before you configure the client, issue one of the following commands from the Windows command prompt to make sure the computer is running the Microsoft IPSec service. Make sure you include the quotes.

- For Windows XP. use `net start "ipsec services"`.
- For Windows 2000, use `net start "ipsec policy agent"`.

## 28.6.1 Configuring L2TP in Windows XP

In Windows XP do the following to establish an L2TP VPN connection.

1 Click **Start > Control Panel > Network Connections > New Connection Wizard**.

2 Click **Next** in the **Welcome** screen.

3 Select **Connect to the network at my workplace** and click **Next**.

**Figure 308** New Connection Wizard: Network Connection Type

4 Select **Virtual Private Network connection** and click **Next**.

**Figure 309** New Connection Wizard: Network Connection


5 Type **L2TP to ZyWALL** as the **Company Name**.

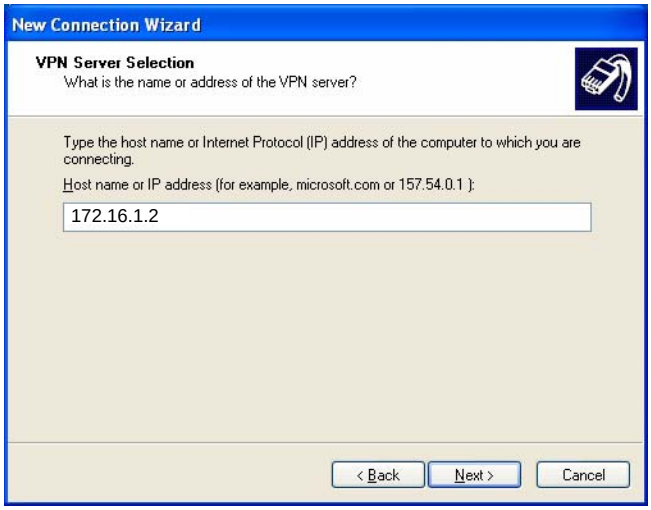
**Figure 310** New Connection Wizard: Connection Name

6 Select **Do not dial the initial connection** and click **Next**.

**Figure 311** New Connection Wizard: Public Network


7 Enter the domain name or WAN IP address configured as the **My Address** in the VPN gateway configuration that the ZyWALL is using for L2TP VPN (172.16.1.2 in this example).

**Figure 312** New Connection Wizard: VPN Server Selection



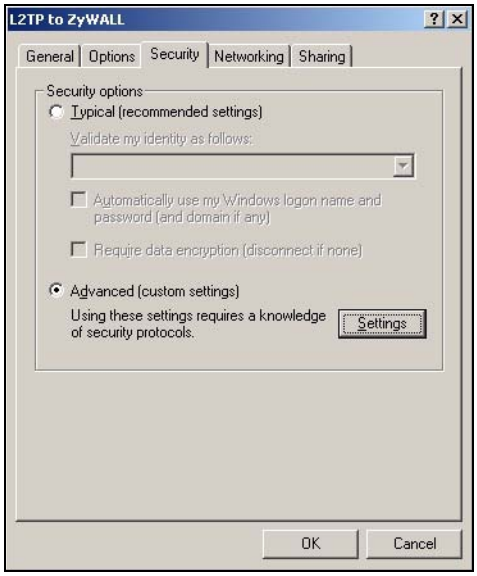

8 Click **Finish**.

9 The **Connect L2TP to ZyWALL** screen appears. Click **Properties > Security**.

**Figure 313** Connect L2TP to ZyWALL

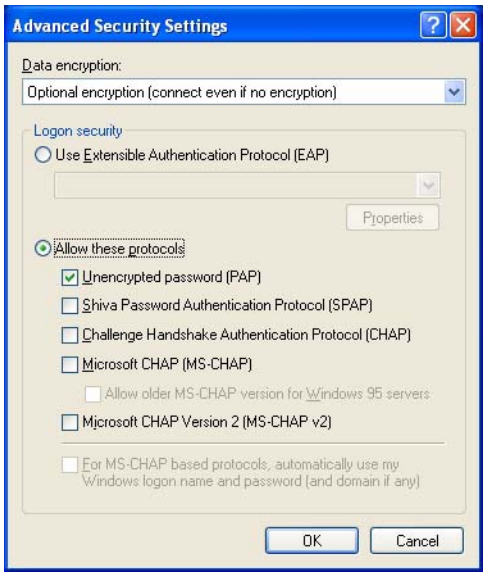

10 Click **Security**, select **Advanced (custom settings)** and click **Settings**.

**Figure 314** Connect L2TP to ZyWALL: Security



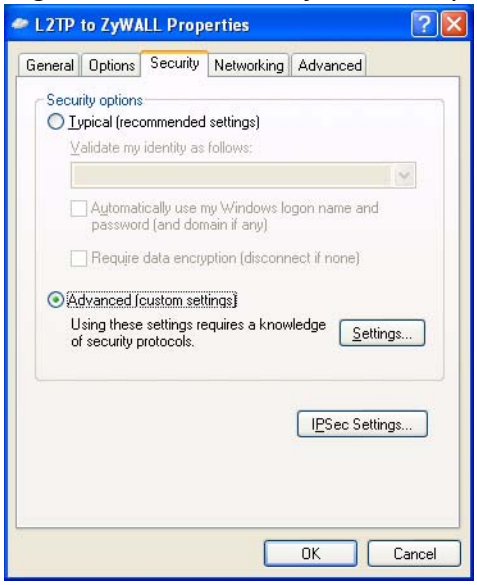
11 Select **Optional encryption (connect even if no encryption)** and the **Allow these protocols** radio button. Select **Unencrypted password (PAP)** and clear all of the other check boxes. Click **OK**.

**Figure 315** Connect ZyWALL L2TP: Security > Advanced




12 Click **IPSec Settings**.

**Figure 316** L2TP to ZyWALL Properties > Security

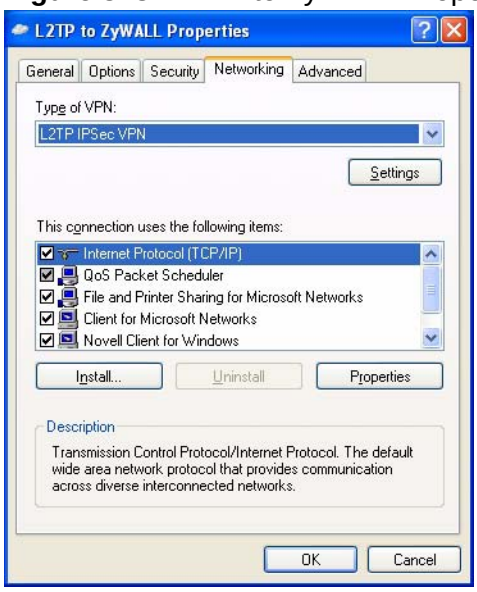


13 Select the **Use pre-shared key for authentication** check box and enter the pre-shared key used in the VPN gateway configuration that the ZyWALL is using for L2TP VPN. Click **OK**.

**Figure 317** L2TP to ZyWALL Properties > Security > IPSec Settings


14 Click **Networking**. Select **L2TP IPSec VPN** as the **Type of VPN**. Click **OK**.

**Figure 318** L2TP to ZyWALL Properties: Networking



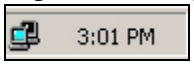

15 Enter the user name and password of your ZyWALL account. Click **Connect**.

**Figure 319** Connect L2TP to ZyWALL


16 A window appears while the user name and password are verified.

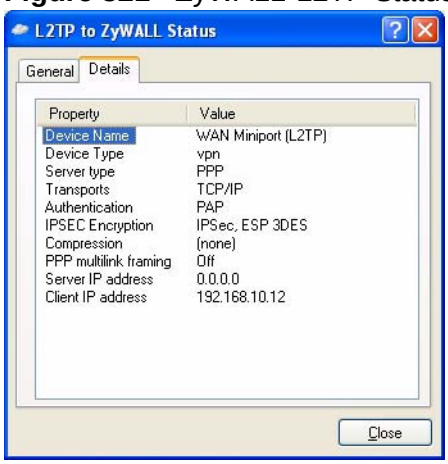
17 A ZyWALL-L2TP icon displays in your system tray. Double-click it to open a status screen.

**Figure 320** ZyWALL-L2TP System Tray Icon




18 Click **Details** to see the address that you received is from the L2TP range you specified on the ZyWALL (192.168.10.10-192.168.10.20).

**Figure 321** ZyWALL-L2TP Status: Details




19 Access a server or other network resource behind the ZyWALL to make sure your access works.

## 28.6.2 Configuring L2TP in Windows 2000

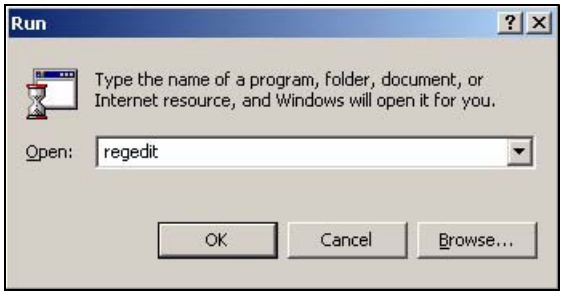
Windows 2000 does not support using pre-shared keys by default. Use the following procedures to edit the registry and then configure the computer to use the L2TP client.

### 28.6.2.1 Editing the Windows 2000 Registry

In Windows 2000, you need to create a registry entry and restart the computer to have it use pre-shared keys.

1 Click **Start > Run**. Type `regedit` and click **OK**.

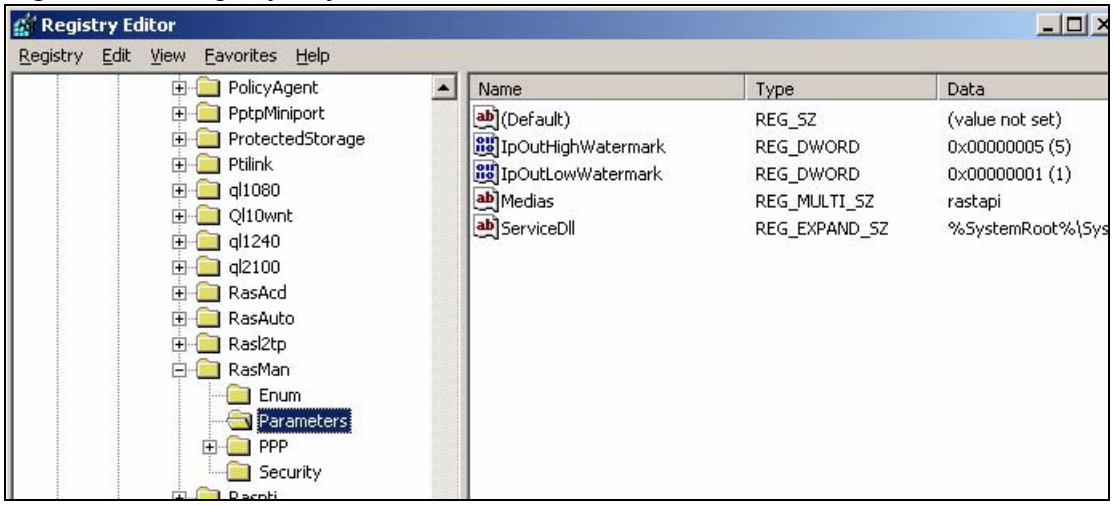
**Figure 322** Starting the Registry Editor




2 Click **Registry > Export Registry File** and save a backup copy of your registry. You can go back to using this backup if you misconfigure the registry settings.

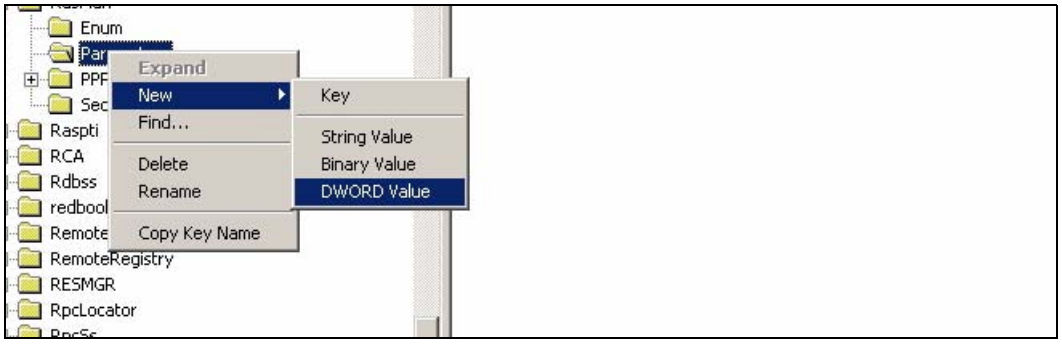
3 Select **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters**.

**Figure 323** Registry Key



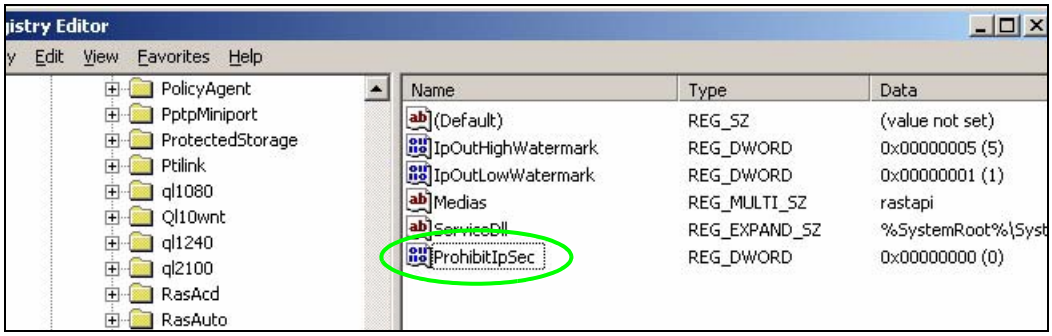

4 Right-click **Parameters** and select **New > DWORD Value**.

**Figure 324** New DWORD Value



5 Enter **ProhibitIpSec** as the name. And make sure the **Data** displays as 0's.

**Figure 325** ProhibitIpSec DWORD Value



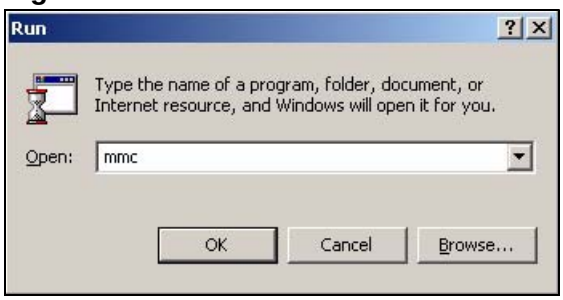

6 Restart the computer and continue with the next section.

## 28.6.2.2 Configure the Windows 2000 IPSec Policy

After you have created the registry entry and restarted the computer, use these directions to configure an IPSec policy for the computer to use.

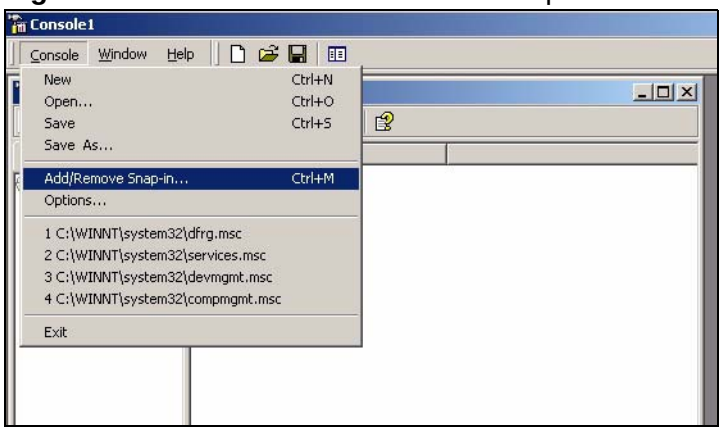
1 Click **Start > Run**. Type `mmc` and click **OK**.

**Figure 326** Run mmc



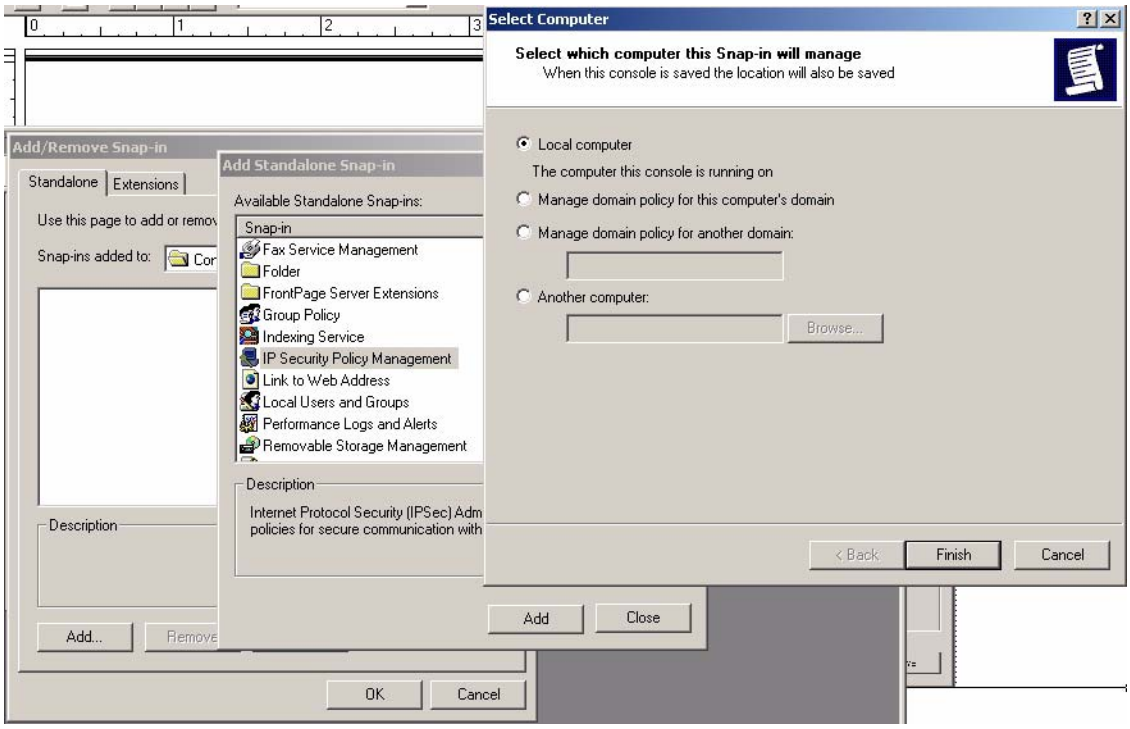

2 Click **Console > Add/Remove Snap-in**.

**Figure 327** Console > Add/Remove Snap-in



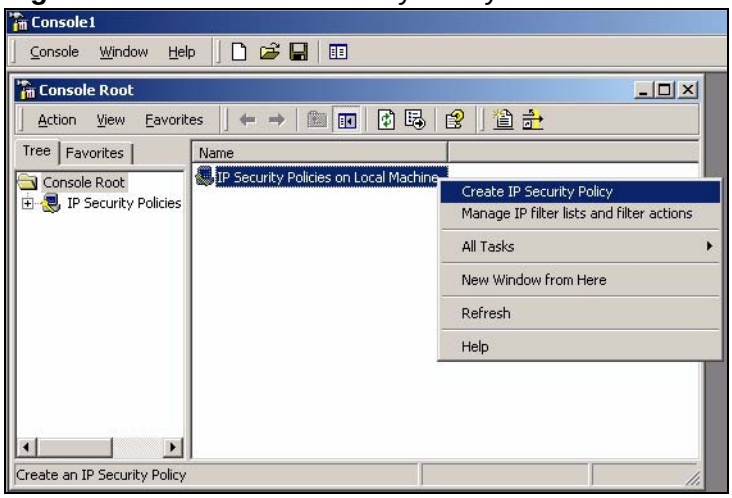
3 Click **Add > IP Security Policy Management >Add > Finish**. Click **Close > OK**.

**Figure 328** Add > IP Security Policy Management > Finish



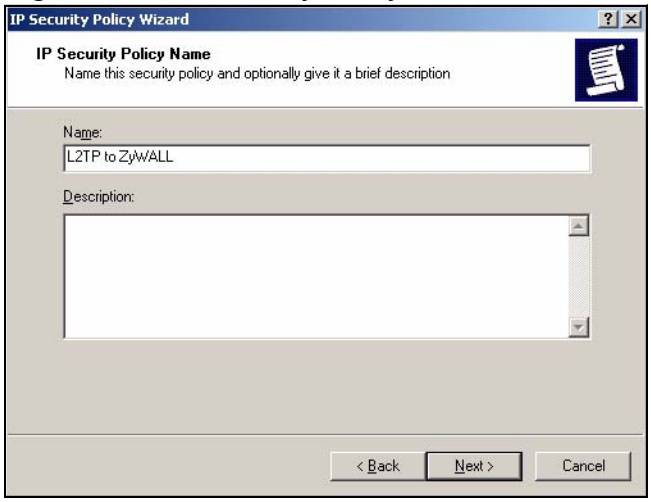

4 Right-click **IP Security Policies on Local Machine** and click **Create IP Security Policy**. Click **Next** in the welcome screen.

**Figure 329** Create IP Security Policy



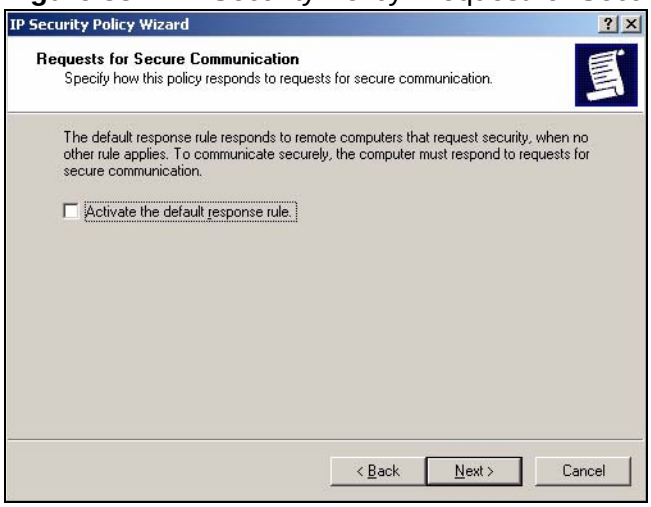
5 Name the IP security policy **L2TP to ZyWALL**, and click **Next**.

**Figure 330** IP Security Policy: Name



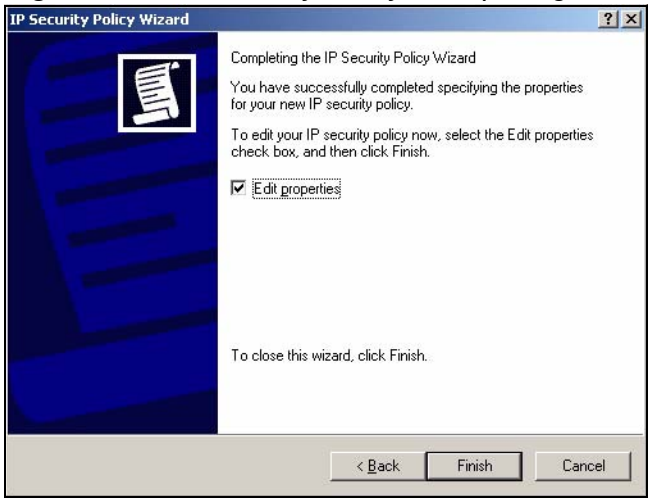

6 Clear the **Activate the default response rule** check box and click **Next**.

**Figure 331** IP Security Policy: Request for Secure Communication



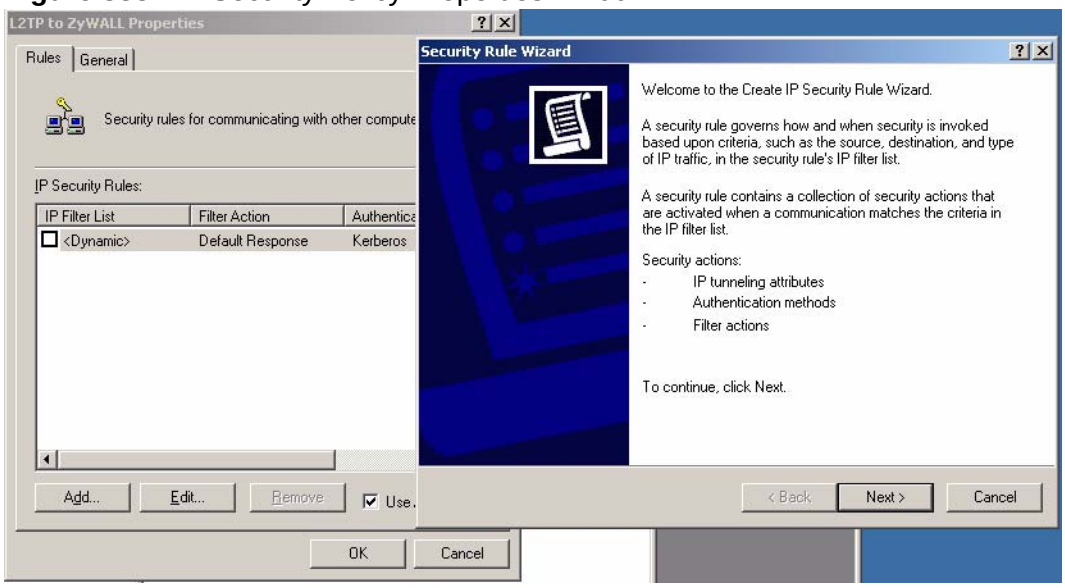
7 Leave the **Edit Properties** check box selected and click **Finish**.

**Figure 332** IP Security Policy: Completing the IP Security Policy Wizard



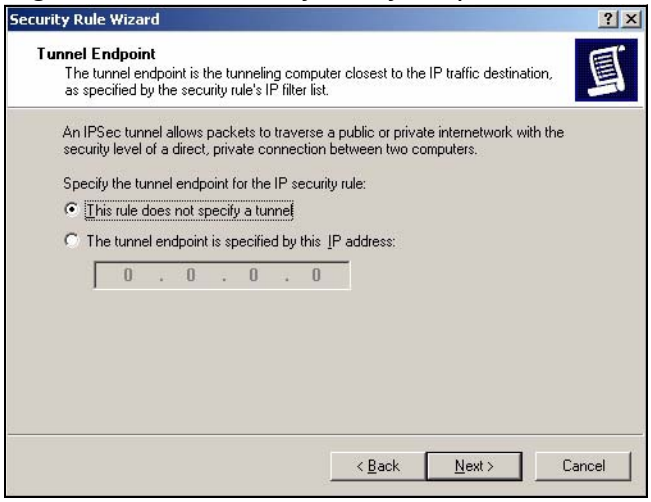

8 In the properties dialog box, click **Add > Next**.

**Figure 333** IP Security Policy Properties > Add



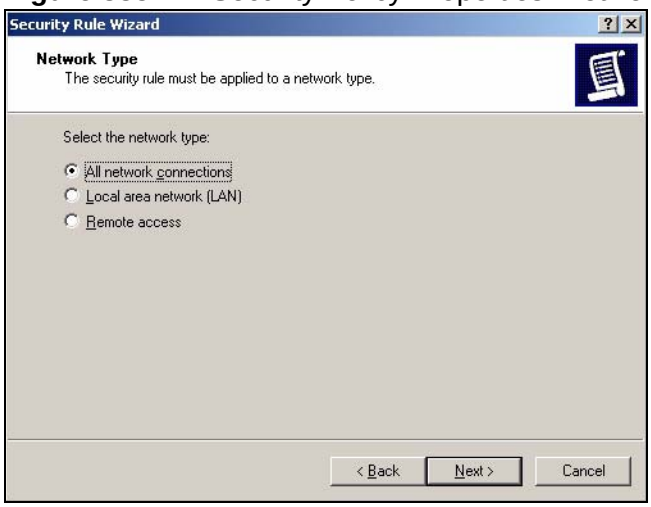
9 Select **This rule does not specify a tunnel** and click **Next**.

**Figure 334** IP Security Policy Properties: Tunnel Endpoint



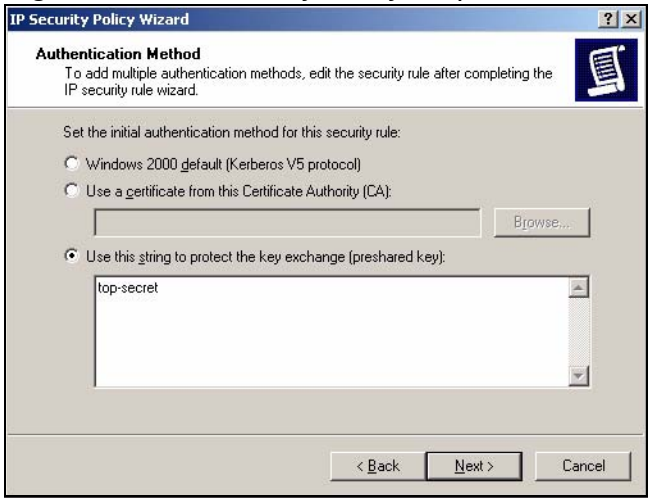

10 Select **All network connections** and click **Next**.

**Figure 335** IP Security Policy Properties: Network Type



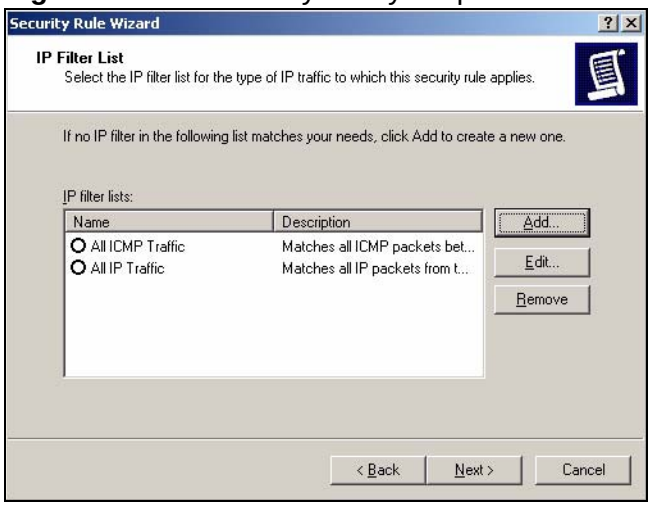
11 Select **Use this string to protect the key exchange (preshared key)**, type **password** in the text box, and click **Next**.

**Figure 336** IP Security Policy Properties: Authentication Method



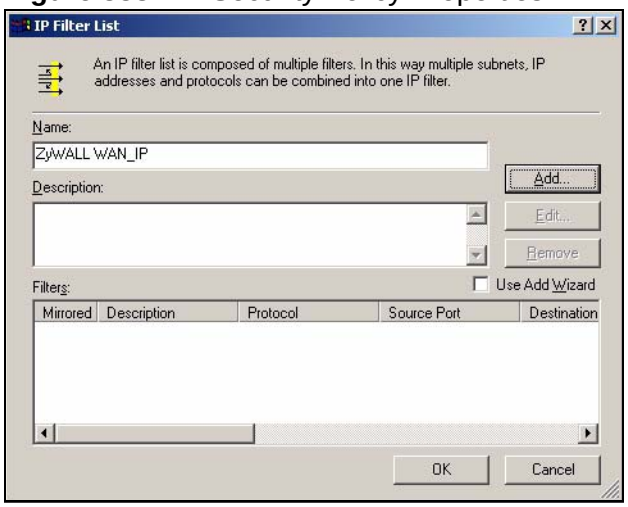

12 Click **Add**.

**Figure 337** IP Security Policy Properties: IP Filter List



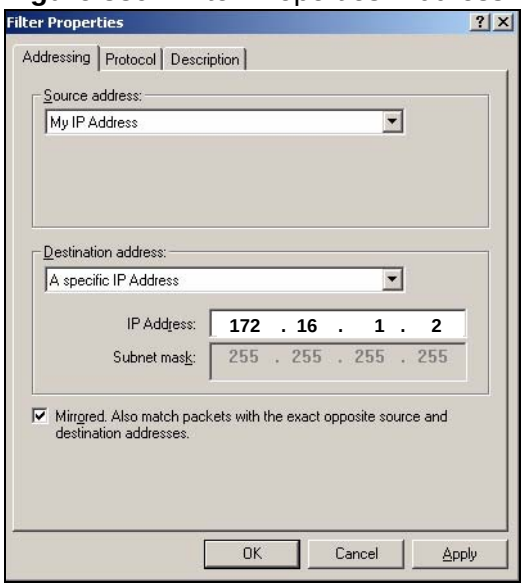
13 Type **ZyWALL WAN_IP** in the **Name** field. Clear the **Use Add Wizard** check box and click **Add**.

**Figure 338** IP Security Policy Properties: IP Filter List > Add



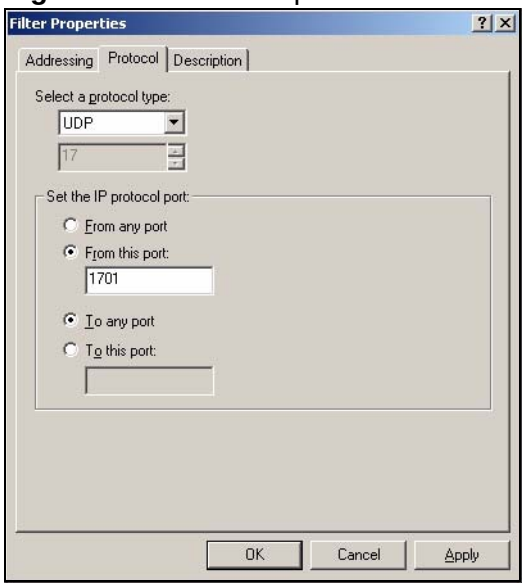

14 Configure the following in the **Addressing** tab. Select **My IP Address** in the **Source address** drop-down list box. Select **A specific IP Address** in the **Destination address** drop-down list box and type the ZyWALL's WAN IP address (172.16.1.2 in this example) in the **IP Address** field. Make certain the **Mirrored. Also match packets with the exact opposite source and destination addresses** check box is selected and click **Apply**.

**Figure 339** Filter Properties: Addressing



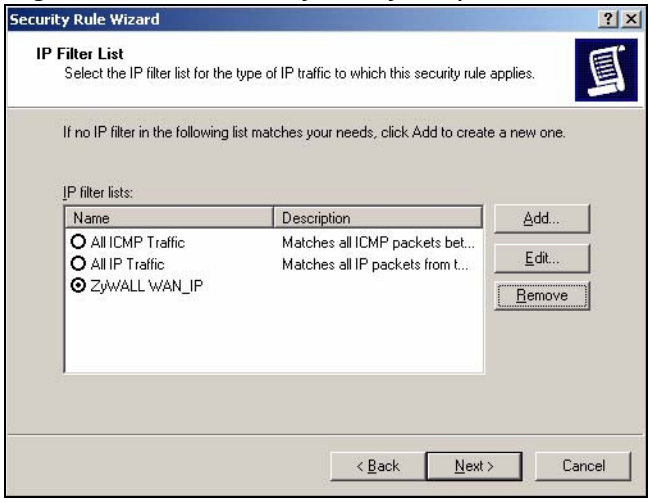
15 Configure the following in the **Filter Properties** window's **Protocol** tab. Set the protocol type to **UDP** from port 1701. Select **To any port**. Click **Apply**, **OK,** and then **Close**.

**Figure 340** Filter Properties: Protocol



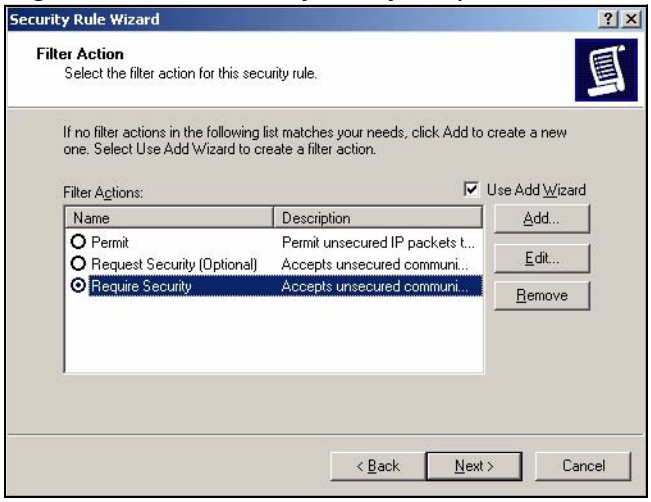

16 Select **ZyWALL WAN_IP** and click **Next**.

**Figure 341** IP Security Policy Properties: IP Filter List



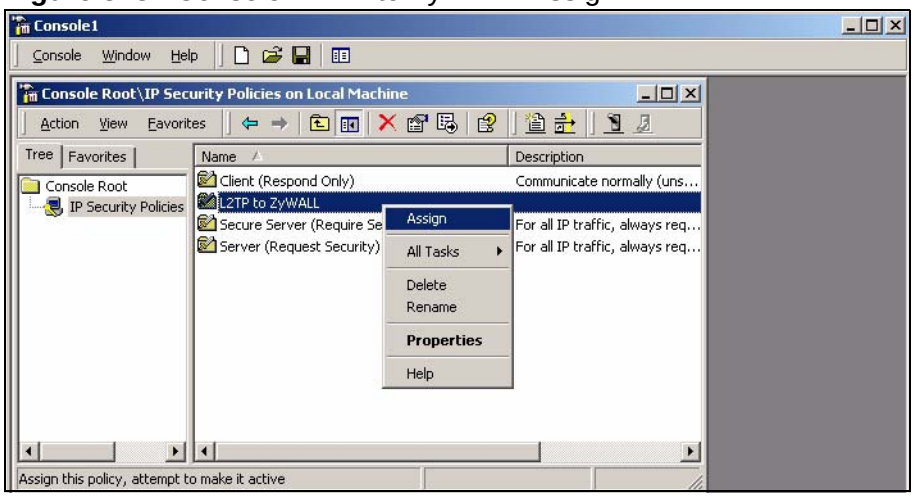
17 Select **Require Security** and click **Next**. Then click **Finish** and **Close**.

**Figure 342** IP Security Policy Properties: IP Filter List




18 In the **Console** window, right-click **L2TP to ZyWALL** and select **Assign**.

**Figure 343** Console: L2TP to ZyWALL Assign

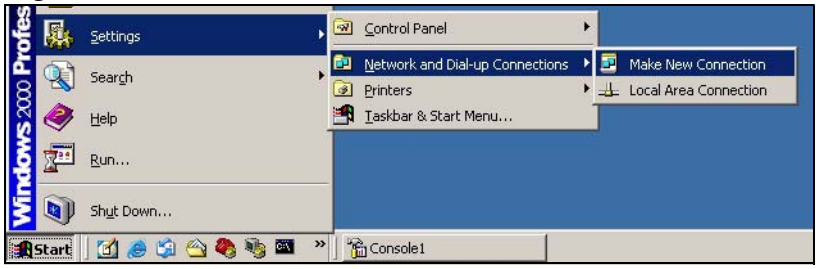



## 28.6.2.3 Configure the Windows 2000 Network Connection

After you have configured the IPSec policy, use these directions to create a network connection.

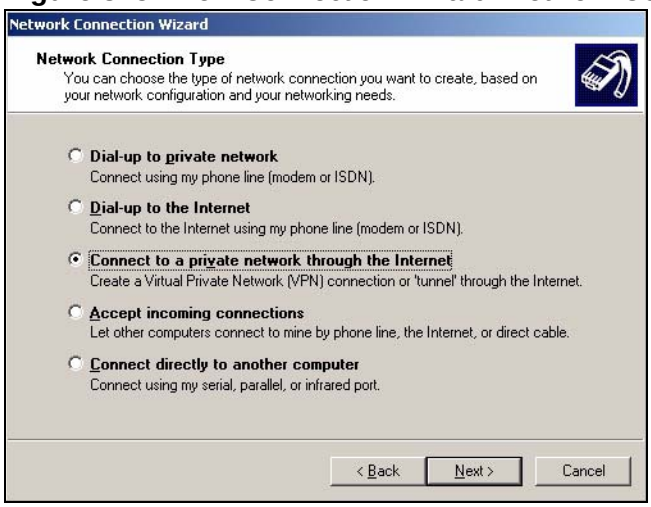
1 Click **Start > Settings > Network and Dial-up connections > Make New Connection**. In the wizard welcome screen, click **Next**.

**Figure 344** Start New Connection Wizard



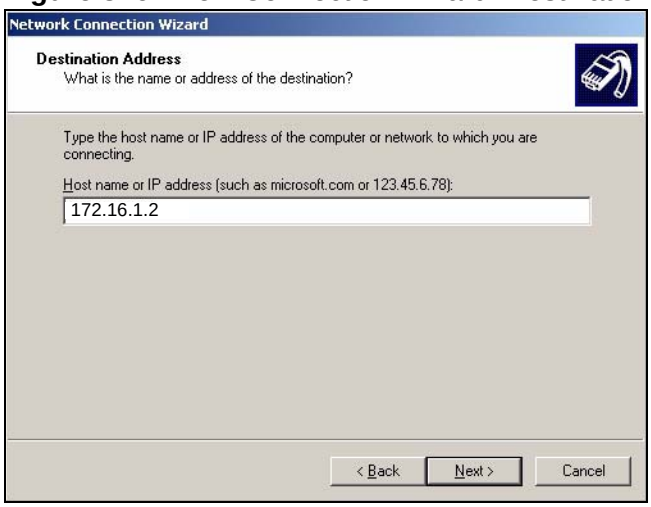

2 Select **Connect to a private network through the Internet** and click **Next**.

**Figure 345** New Connection Wizard: Network Connection Type



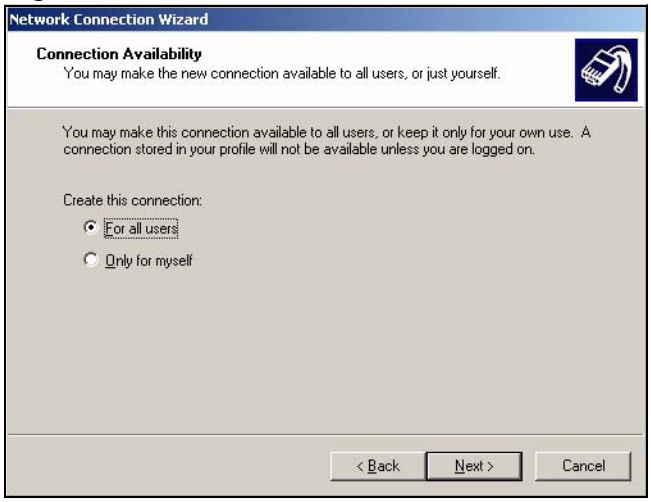

3 Enter the domain name or WAN IP address configured as the **My Address** in the VPN gateway configuration that the ZyWALL is using for L2TP VPN. Click **Next**.

**Figure 346** New Connection Wizard: Destination Address



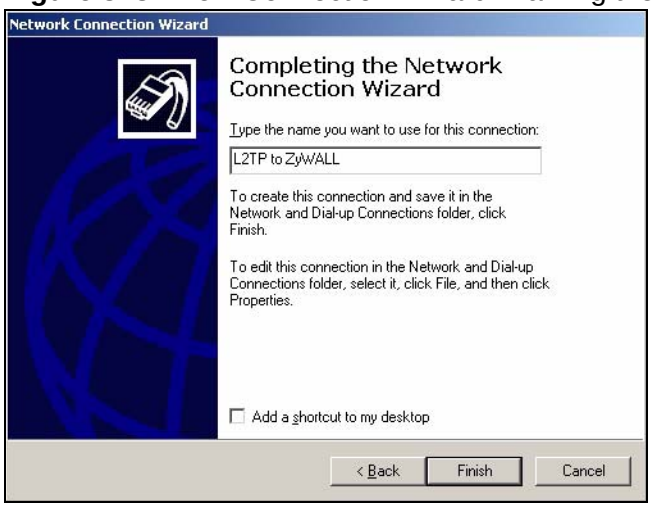
4 Select **For all users** and click **Next**.

**Figure 347** New Connection Wizard: Connection Availability



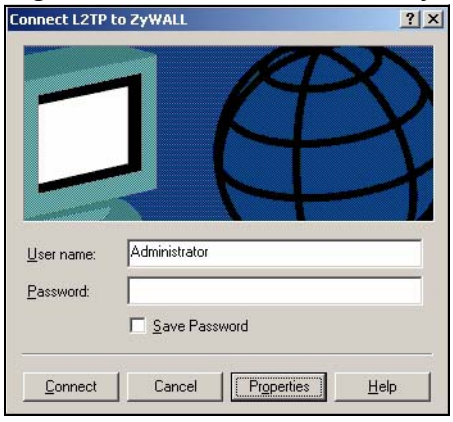

5 Name the connection **L2TP to ZyWALL** and click **Finish**.

**Figure 348** New Connection Wizard: Naming the Connection



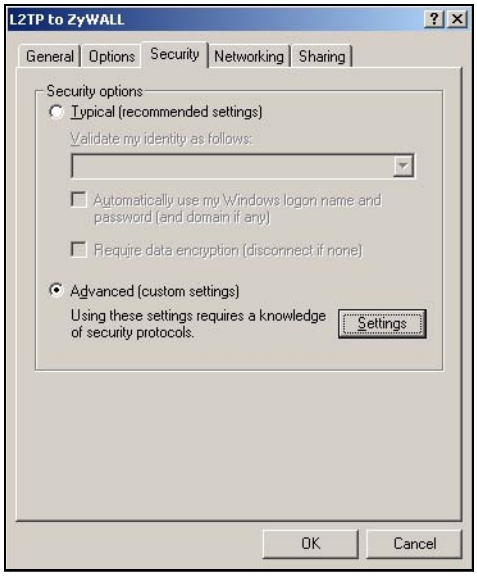

6 Click **Properties**.

**Figure 349** Connect L2TP to ZyWALL



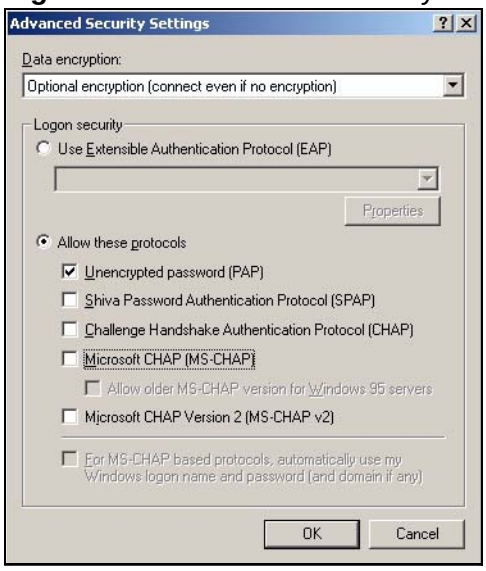
7 Click **Security** and select **Advanced (custom settings)** and click **Settings**.

**Figure 350** Connect L2TP to ZyWALL: Security



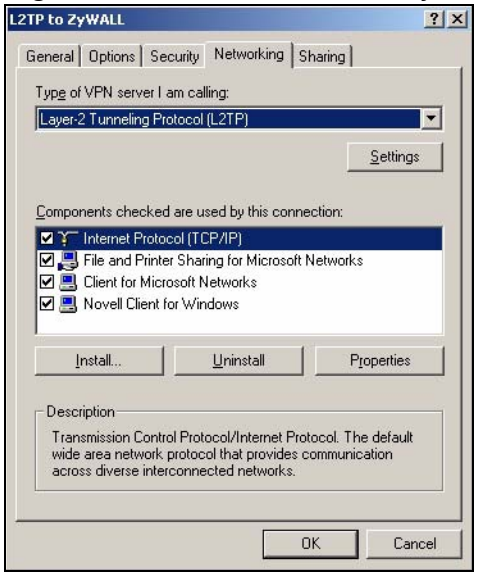

8 Select **Optional encryption allowed (connect even if no encryption)** and the **Allow these protocols** radio button. Select **Unencrypted password (PAP)** and clear all of the other check boxes. Click **OK**. Click **Yes** if a screen pops up.

**Figure 351** Connect L2TP to ZyWALL: Security > Advanced



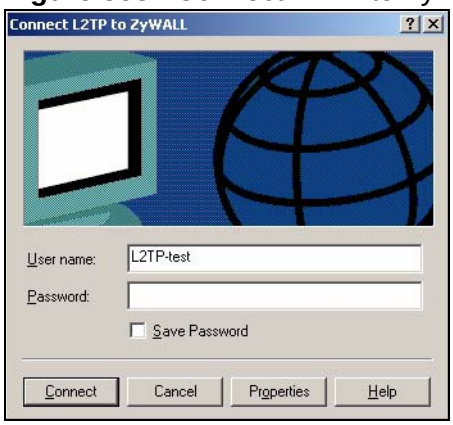
9 Click **Networking** and select **Layer 2 Tunneling Protocol (L2TP)** from the drop-down list box. Click **OK**.

**Figure 352** Connect L2TP to ZyWALL: Networking



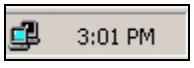

10 Enter your user name and password and click **Connect**. It may take up to one minute to establish the connection and register on the network.

**Figure 353** Connect L2TP to ZyWALL



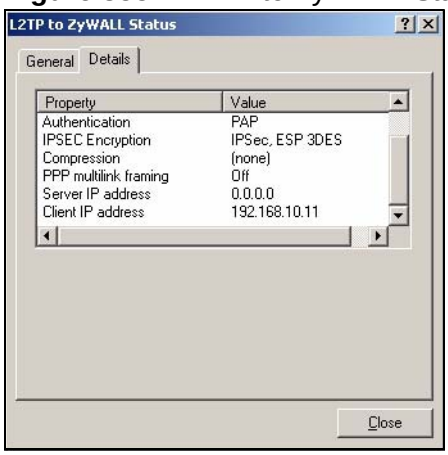

11 A ZyWALL-L2TP icon displays in your system tray. Double-click it to open a status screen.

**Figure 354** ZyWALL-L2TP System Tray Icon



12 Click **Details** and scroll down to see the address that you received is from the L2TP range you specified on the ZyWALL (192.168.10.10-192.168.10.20).

**Figure 355** L2TP to ZyWALL Status: Details




13 Access a server or other network resource behind the ZyWALL to make sure your access works.

# PART V
# Application Patrol

# 29

# Application Patrol

## 29.1 Overview

Application patrol provides a convenient way to manage the use of various applications on the network. It manages general protocols (for example, HTTP and FTP) and instant messenger (IM), peer-to-peer (P2P), Voice over IP (VoIP), and streaming (RSTP) applications. You can even control the use of a particular application's individual features (like text messaging, voice, video conferencing, and file transfers). Application patrol also has powerful bandwidth management including traffic prioritization to enhance the performance of delay-sensitive applications like voice and video.

There is also an option that gives SIP traffic priority over all other traffic going through the ZyWALL. This maximizes SIP traffic throughput for improved VoIP call sound quality.

### 29.1.1 What You Can Do in the Application Patrol Screens

- Use the **General** summary screen (see Section 29.2 on page 486) to enable and disable application patrol.
- Use the **Common**, **Instant Messenger**, **Peer to Peer**, **VoIP**, and **Streaming** (see Section 29.3 on page 488) screens to look at the applications the ZyWALL can recognize, and review the settings for each one. You can also enable and disable the rules for each application and specify the default and custom policies for each application.
- Use the **Application Patrol Edit** screen (see Section 29.3.1 on page 489) to edit the settings for an application.
- Use the **Application Policy Edit** screen (see Section 29.3.2 on page 491) to edit a group of settings for an application.
- Use the **Other** screens (see Section 29.4 on page 494) to control what the ZyWALL does when it does not recognize the application, and it identifies the conditions that refine this. It also lets you open the **Other Configuration Add / Edit** screen to create new conditions or edit existing ones.
- Use the **Statistics** screen (see Section 29.5 on page 499) to see a bandwidth usage graph and statistics for each protocol.

## 29.1.2 What You Need to Know About Application Patrol

If you want to use a service, make sure both the firewall and application patrol allow the service's packets to go through the ZyWALL.

Note: The ZyWALL checks firewall rules before it checks application patrol rules for traffic going through the ZyWALL.

Application patrol examines every TCP and UDP connection passing through the ZyWALL and identifies what application is using the connection. Then, you can specify, by application, whether or not the ZyWALL continues to route the connection.

### Configurable Application Policies

The ZyWALL has policies for individual applications. For each policy, you can specify the default action the ZyWALL takes once it identifies one of the service's connections.

You can also specify custom policies that have the ZyWALL forward, drop, or reject a service's connections based on criteria that you specify (like the source zone, destination zone, original destination port of the connection, schedule, user, source, and destination information). Your custom policies take priority over the policy's default settings.

### Classification of Applications

There are two ways the ZyWALL can identify the application. The first is called auto. The ZyWALL looks at the IP payload (OSI level-7 inspection) and attempts to match it with known patterns for specific applications. Usually, this occurs at the beginning of a connection, when the payload is more consistent across connections, and the ZyWALL examines several packets to make sure the match is correct.

Note: The ZyWALL allows the first eight packets to go through the firewall, regardless of the application patrol policy for the application. The ZyWALL examines these first eight packets to identify the application.

The second approach is called service ports. The ZyWALL uses only OSI level-4 information, such as ports, to identify what application is using the connection. This approach is available in case the ZyWALL identifies a lot of "false positives" for a particular application.

### Custom Ports for SIP and the SIP ALG

Configuring application patrol to use custom port numbers for SIP traffic also configures the SIP ALG (see Chapter 18 on page 327) to use the same port

numbers for SIP traffic. Likewise, configuring the SIP ALG to use custom port numbers for SIP traffic also configures application patrol to use the same port numbers for SIP traffic.

### Bandwidth Management

When you allow an application, you can restrict the bandwidth it uses or even the bandwidth that particular features in the application (like voice, video, or file sharing) use. This restriction may be ineffective in certain cases, however, such as using MSN to send files via P2P.

The application patrol bandwidth management is more flexible and powerful than the bandwidth management in policy routes. Application patrol controls TCP and UDP traffic. Use policy routes to manage other types of traffic (like ICMP).

Note: Bandwidth management in policy routes has priority over application patrol bandwidth management. It is recommended to use application patrol instead of policy routes to manage the bandwidth of TCP and UDP traffic.

### Connection and Packet Directions

Application patrol looks at the connection direction, that is from which zone the connection was initiated and to which zone the connection is going.

A connection has outbound and inbound packet flows. The ZyWALL controls the bandwidth of traffic of each flow as it is going out through an interface or VPN tunnel.

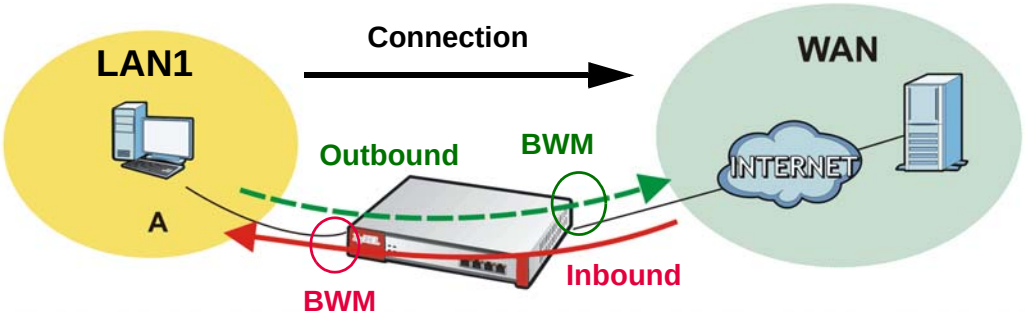
- The outbound traffic flows from the connection initiator to the connection responder.
- The inbound traffic flows from the connection responder to the connection initiator.

For example, a LAN1 to WAN connection is initiated from LAN1 and goes to the WAN.

- Outbound traffic goes from a LAN1 zone device to a WAN zone device. Bandwidth management is applied before sending the packets out a WAN zone interface on the ZyWALL.

- Inbound traffic comes back from the WAN zone device to the LAN1 zone device. Bandwidth management is applied before sending the traffic out a LAN1 zone interface.

**Figure 356** LAN1 to WAN Connection and Packet Directions

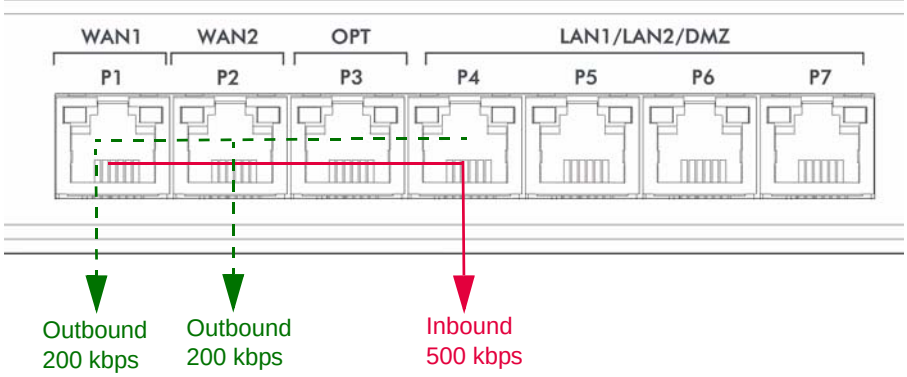



## Outbound and Inbound Bandwidth Limits

You can limit an application's outbound or inbound bandwidth. This limit keeps the traffic from using up too much of the out-going interface's bandwidth. This way you can make sure there is bandwidth for other applications. When you apply a bandwidth limit to outbound or inbound traffic, each member of the out-going zone can send up to the limit. Take a LAN1 to WAN policy for example.

- Outbound traffic is limited to 200 kbps. The connection initiator is on the LAN1 so outbound means the traffic traveling from the LAN1 to the WAN. Each of the WAN zone's two interfaces can send the limit of 200 kbps of traffic.
- Inbound traffic is limited to 500 kbs. The connection initiator is on the LAN1 so inbound means the traffic traveling from the WAN to the LAN1.

**Figure 357** LAN1 to WAN, Outbound 200 kbps, Inbound 500 kbps




## Bandwidth Management Priority

- The ZyWALL gives bandwidth to higher-priority traffic first, until it reaches its configured bandwidth rate.
- Then lower-priority traffic gets bandwidth.
- The ZyWALL uses a fairness-based (round-robin) scheduler to divide bandwidth among traffic flows with the same priority.

- The ZyWALL automatically treats traffic with bandwidth management disabled as priority 7 (the lowest priority).

### Maximize Bandwidth Usage

Maximize bandwidth usage allows applications with maximize bandwidth usage enabled to “borrow” any unused bandwidth on the out-going interface.

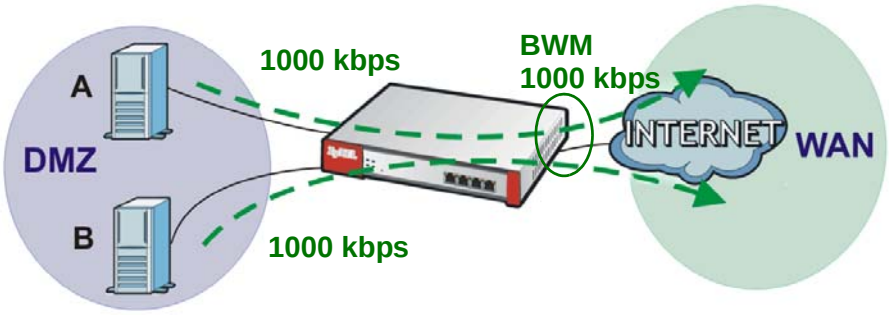
After each application gets its configured bandwidth rate, the ZyWALL uses the fairness- based scheduler to divide any unused bandwidth on the out-going interface amongst applications that need more bandwidth and have maximize bandwidth usage enabled.

Unused bandwidth is divided equally. Higher priority traffic does not get a larger portion of the unused bandwidth.

### Bandwidth Management Behavior

The following sections show how bandwidth management behaves with various settings. For example, you configure DMZ to WAN policies for FTP servers **A** and **B**. Each server tries to send 1000 kbps, but the WAN is set to a maximum outgoing speed of 1000 kbps. You configure policy A for server **A**’s traffic and policy B for server **B**’s traffic.

**Figure 358** Bandwidth Management Behavior




### Configured Rate Effect

In the following table the configured rates total less than the available bandwidth and maximize bandwidth usage is disabled, both servers get their configured rate.

**Table 140** Configured Rate Effect

| POLICY | CONFIGURED RATE | MAX. B. U. | PRIORITY | ACTUAL RATE |
|---|---|---|---|---|
| A | 300 kbps | No | 1 | 300 kbps |
| B | 200 kbps | No | 1 | 200 kbps |

### Priority Effect

Here the configured rates total more than the available bandwidth. Because server **A** has higher priority, it gets up to it's configured rate (800 kbps), leaving only 200 kbps for server **B**.

**Table 141** Priority Effect

| POLICY | CONFIGURED RATE | MAX. B. U. | PRIORITY | ACTUAL RATE |
|---|---|---|---|---|
| A | 800 kbps | Yes | 1 | 800 kbps |
| B | 1000 kbps | Yes | 2 | 200 kbps |

### Maximize Bandwidth Usage Effect

With maximize bandwidth usage enabled, after each server gets its configured rate, the rest of the available bandwidth is divided equally between the two. So server **A** gets its configured rate of 300 kbps and server **B** gets its configured rate of 200 kbps. Then the ZyWALL divides the remaining bandwidth (1000 - 500 = 500) equally between the two (500 / 2 = 250 kbps for each). The priority has no effect on how much of the unused bandwidth each server gets.

So server **A** gets its configured rate of 300 kbps plus 250 kbps for a total of 550 kbps. Server **B** gets its configured rate of 200 kbps plus 250 kbps for a total of 450 kbps.

**Table 142** Maximize Bandwidth Usage Effect

| POLICY | CONFIGURED RATE | MAX. B. U. | PRIORITY | ACTUAL RATE |
|---|---|---|---|---|
| A | 300 kbps | Yes | 1 | 550 kbps |
| B | 200 kbps | Yes | 2 | 450 kbps |

### Priority and Over Allotment of Bandwidth Effect

Server **A** has a configured rate that equals the total amount of available bandwidth and a higher priority. You should regard extreme over allotment of traffic with different priorities (as shown here) as a configuration error. Even though the ZyWALL still attempts to let all traffic get through and not be lost, regardless of its priority, server **B** gets almost no bandwidth with this configuration.

**Table 143** Priority and Over Allotment of Bandwidth Effect

| POLICY | CONFIGURED RATE | MAX. B. U. | PRIORITY | ACTUAL RATE |
|---|---|---|---|---|
| A | 1000 kbps | Yes | 1 | 999 kbps |
| B | 1000 kbps | Yes | 2 | 1 kbps |

### Finding Out More

- See Section 5.4.13 on page 92 for related information on these screens.
- See Section 6.6 on page 127 for an example of how to set up web surfing policies with bandwidth restrictions.

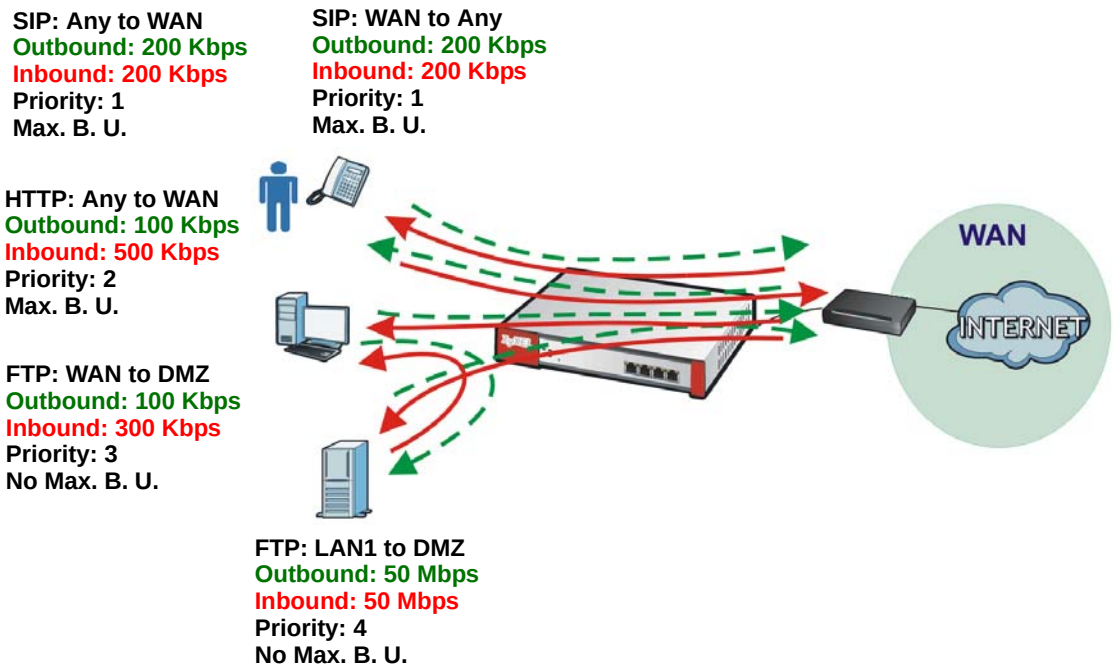
## 29.1.3 Application Patrol Bandwidth Management Examples

Bandwidth management is very useful when applications are competing for limited bandwidth. For example, say you have a WAN zone interface connected to an ADSL device with a 8 Mbps downstream and 1 Mbps upstream ADSL connection. The following sections give some simplified examples of using application patrol policies to manage applications competing for that 1 Mbps of upstream bandwidth.

Here is an overview of what the rules need to accomplish. See the following sections for more details.

- SIP traffic from VIP users must get through with the least possible delay regardless of if it is an outgoing call or an incoming call. The VIP users must be able to make and receive SIP calls no matter which interface they are connected to.
- HTTP traffic needs to be given priority over FTP traffic.
- FTP traffic from the WAN to the DMZ must be limited so it does not interfere with SIP and HTTP traffic.
- FTP traffic from the LAN1 to the DMZ can use more bandwidth since the interfaces support up to 1 Gbps connections, but it must be the lowest priority and limited so it does not interfere with SIP and HTTP traffic.

**Figure 359** Application Patrol Bandwidth Management Example



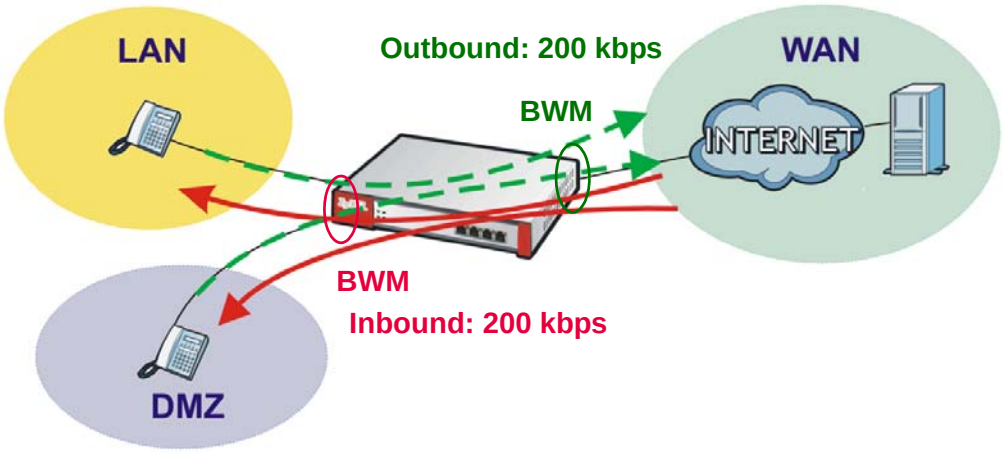
### 29.1.3.1 Setting the Interface's Bandwidth

Use the interface screens to set the WAN zone interface's upstream bandwidth to be equal to (or slightly less than) what the connected device can support. This example uses 1000 Kbps.

### 29.1.3.2 SIP Any to WAN Bandwidth Management Example

- Manage SIP traffic going to the WAN zone from a VIP user on the LAN or DMZ.
- Outbound traffic (to the WAN from the LAN and DMZ) is limited to 200 kbps. The ZyWALL applies this limit before sending the traffic to the WAN.
- Inbound traffic (to the LAN and DMZ from the WAN) is also limited to 200 kbps. The ZyWALL applies this limit before sending the traffic to LAN or DMZ.
- Highest priority (1). Set policies for other applications to lower priorities so the SIP traffic always gets the best treatment.
- Enable maximize bandwidth usage so the SIP traffic can borrow unused bandwidth.

**Figure 360** SIP Any to WAN Bandwidth Management Example




### 29.1.3.3 SIP WAN to Any Bandwidth Management Example

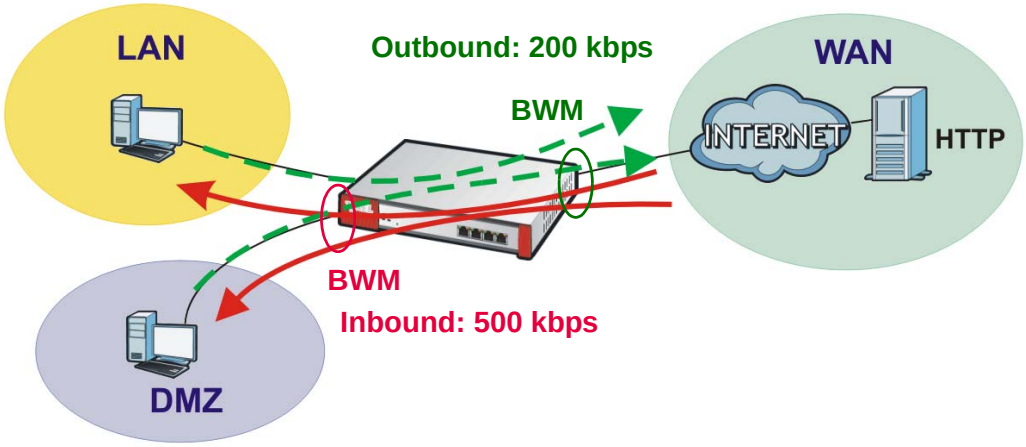
You also create a policy for calls coming in from the SIP server on the WAN. It is the same as the SIP Any to WAN policy, but with the directions reversed (WAN to Any instead of Any to WAN).

### 29.1.3.4 HTTP Any to WAN Bandwidth Management Example

- Inbound traffic gets more bandwidth as the local users will probably download more than they upload (and the ADSL connection supports this).
- Second highest priority (2). Set policies for other applications (except SIP) to lower priorities so the local users' HTTP traffic gets sent before non-SIP traffic.

- Enable maximize bandwidth usage so the HTTP traffic can borrow unused bandwidth.

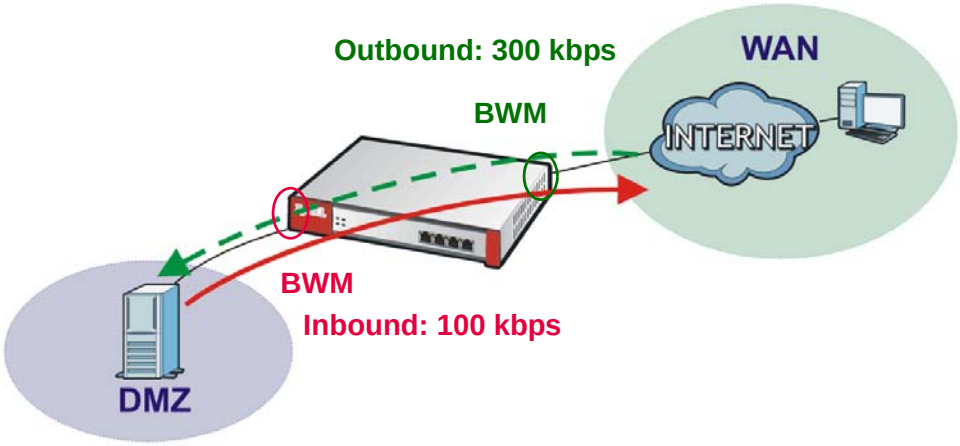
**Figure 361** HTTP Any to WAN Bandwidth Management Example




### 29.1.3.5 FTP WAN to DMZ Bandwidth Management Example

- ADSL supports more downstream than upstream so you allow remote users 300 kbps for uploads to the DMZ FTP server (outbound) but only 100 kbps for downloads (inbound).
- Third highest priority (3).
- Disable maximize bandwidth usage since you do not want to give FTP more bandwidth.

**Figure 362** FTP WAN to DMZ Bandwidth Management Example

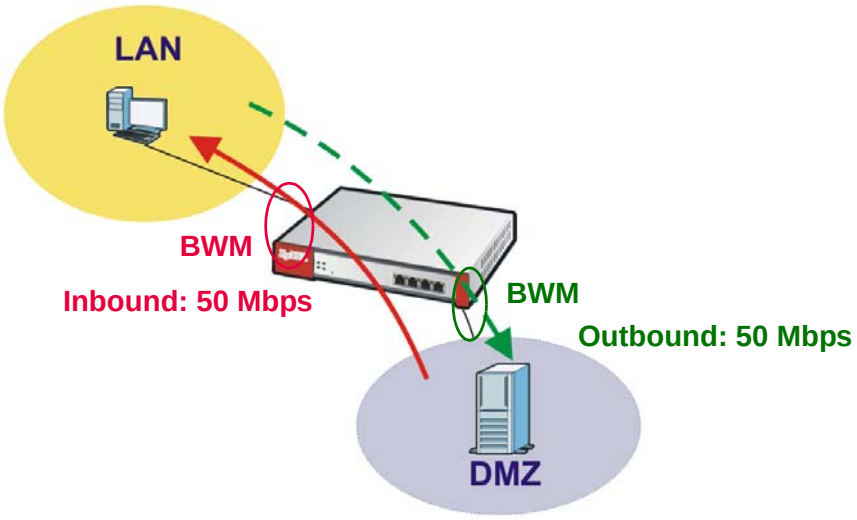



### 29.1.3.6 FTP LAN to DMZ Bandwidth Management Example

- The LAN and DMZ zone interfaces are connected to Ethernet networks (not an ADSL device) so you limit both outbound and inbound traffic to 50 Mbps.
- Fourth highest priority (4).

- Disable maximize bandwidth usage since you do not want to give FTP more bandwidth.

**Figure 363** FTP LAN to DMZ Bandwidth Management Example




# 29.2 Application Patrol General Screen

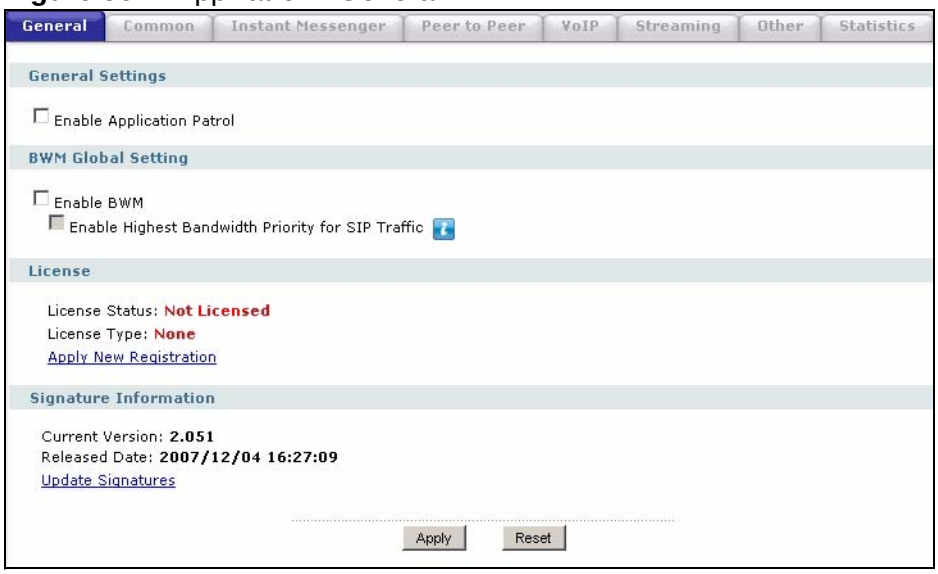
Use this screen to enable and disable application patrol. It also lists the registration status and details about the signature set the ZyWALL is using.

Note: You must register for the IDP/AppPatrol signature service (at least the trial) before you can use it.

See Chapter 8 on page 165 for how to register.

Click **AppPatrol** to open the following screen.

**Figure 364** AppPatrol > General




The following table describes the labels in this screen. See Section 29.3.1 on page 489 for more information as well.

**Table 144** AppPatrol > General

| LABEL | DESCRIPTION |
|---|---|
| Enable Application Patrol | Select this check box to turn on application patrol. |
| Enable BWM | This is a global setting for enabling or disabling bandwidth management on the ZyWALL. You must enable this setting to have individual policy routes or application patrol policies apply bandwidth management.<br><br>This same setting also appears in the **Network > Routing > Policy Route** screen. Enabling or disabling it in one screen also enables or disables it in the other screen. |
| Enable Highest Bandwidth Priority for SIP Traffic | Select this to maximize the throughput of SIP traffic to improve SIP-based VoIP call sound quality. This has the ZyWALL immediately send SIP traffic upon identifying it. The ZyWALL ignores any other application patrol rules for SIP traffic (so there is no bandwidth control for SIP traffic). When this option is enabled the ZyWALL also does not record SIP traffic bandwidth usage statistics. |
| Registration | The following fields display information about the current state of your subscription for IDP/application patrol signatures. |
| Registration Status | This field displays whether a service is activated (**Licensed**) or not (**Not Licensed**) or expired (**Expired**). |
| Registration Type | This field displays whether you applied for a trial application (**Trial**) or registered a service with your iCard's PIN number (**Standard**). **None** displays when the service is not activated. |
| Apply new Registration | This link appears if you have not registered for the service or only have the trial registration. Click this link to go to the screen where you can register for the service. |

**Table 144** AppPatrol > General (continued)

| LABEL | DESCRIPTION |
|---|---|
| Signature Information | The following fields display information on the current signature set that the ZyWALL is using. |
| Current Version | This field displays the IDP signature and anomaly rule set version number. This number gets larger as the set is enhanced. |
| Released Date | This field displays the date and time the set was released. |
| Update Signatures | Click this link to go to the screen you can use to download signatures from the update server. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

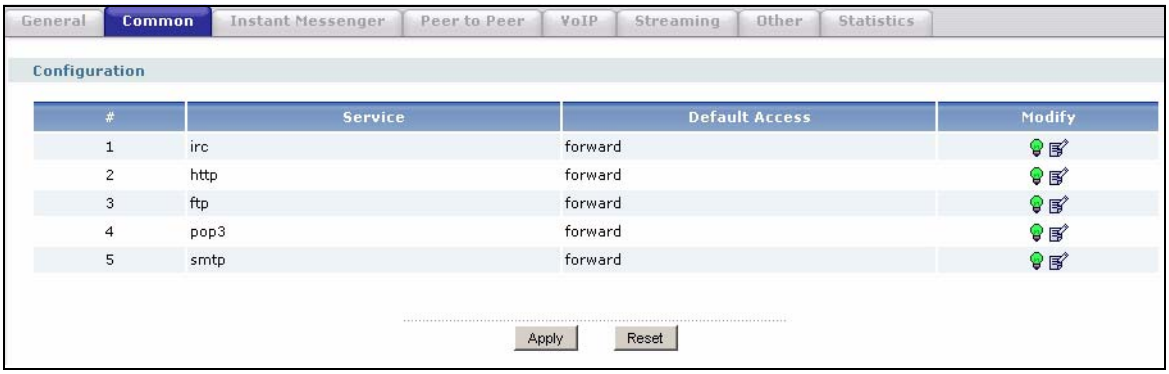
# 29.3 Application Patrol Applications

Use the application patrol **Common**, **Instant Messenger**, **Peer to Peer**, **VoIP**, or **Streaming** screen to manage traffic of individual applications.

Use the **Common** screen (shown here as an example) to manage traffic of the most commonly used web, file transfer and e-mail protocols.

Click **AppPatrol > Common** to open the following screen.

**Figure 365** AppPatrol > Common




The following table describes the labels in this screen. See Section 29.3.1 on page 489 for more information as well.

**Table 145** AppPatrol > Common

| LABEL | DESCRIPTION |
|---|---|
| # | This field is a sequential value, and it is not associated with a specific application. |
| Service | This field displays the name of the application. |

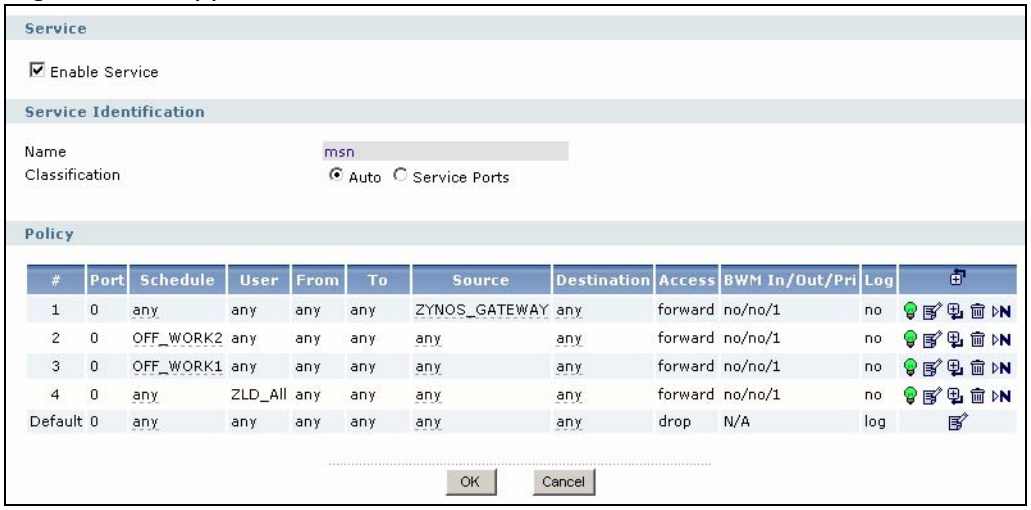
**Table 145** AppPatrol > Common (continued)

| LABEL | DESCRIPTION |
|---|---|
| Default Access | This field displays what the ZyWALL does with packets for this application. Choices are: **forward**, **drop**, and **reject**. |
| Modify | This column provides icons to activate and deactivate each application and to edit the settings for each one.<br><br>To activate or deactivate patrol for an application, click the **Active** icon for the corresponding application. Make sure you click **Apply** to save and apply the change.<br><br>To edit the settings for an application, click the **Edit** icon next to the application. The **Configuration Edit** screen appears. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 29.3.1 The Application Patrol Edit Screen

Use this screen to edit the settings for an application. To access this screen, go to the application patrol **Common**, **Instant Messenger**, **Peer to Peer**, **VoIP**, or **Streaming** screen and click an application's **Edit** icon. The screen displayed here is for the MSN instant messenger service.

**Figure 366** Application Edit




The following table describes the labels in this screen.

**Table 146** Application Edit

| LABEL | DESCRIPTION |
|---|---|
| Service | |
| Enable Service | Select this check box to turn on patrol for this application. |
| Service Identification | |

**Table 146** Application Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Name | This field displays the name of the application. |
| Classification | Specify how the ZyWALL should identify this application. Choices are:<br>**Auto** - the ZyWALL identifies this application by matching the IP payload with the application's pattern(s).<br>**Service Ports** - the ZyWALL identifies this application by looking at the destination port in the IP header. |
| Service Port | This is available if the **Classification** is **Service Ports**. You can view and edit the ports used to identify this application. |
| Add icon | When the **Classification** is **Service Ports**, this column provides icons to add and remove port numbers used to identify the application.<br>Click **Add** add a port number. Type the destination port number in the **Service Port** field.<br>Click **Remove** to delete a port number. The Web Configurator confirms that you want to delete the port number before doing so. |
| Policy | |
| # | This field is a sequential value, and it is not associated with a specific condition.<br>Note: The ZyWALL checks conditions in the order they appear in the list. While this sequence does not affect the functionality, you might improve the performance of the ZyWALL by putting more common conditions at the top of the list. |
| Port | This field displays the specific port number to which this policy applies. |
| Schedule | This is the schedule that defines when the policy applies. **any** means the policy is active at all times if enabled. |
| User | This is the user name or user group to which the policy applies. If **any** displays, the policy applies to all users. |
| From | This is the source zone of the traffic to which this policy applies. |
| To | This is the destination zone of the traffic to which this policy applies. |
| Source | This is the source address or address group for whom this policy applies. If **any** displays, the policy is effective for every source. |
| Destination | This is the destination address or address group for whom this policy applies. If **any** displays, the policy is effective for every destination. |
| Access | This field displays what the ZyWALL does with packets for this application that match this policy.<br>**forward** - the ZyWALL routes the packets for this application.<br>**Drop** - the ZyWALL does not route the packets for this application and does not notify the client of its decision.<br>**Reject** - the ZyWALL does not route the packets for this application and notifies the client of its decision. |

**Table 146** Application Edit (continued)

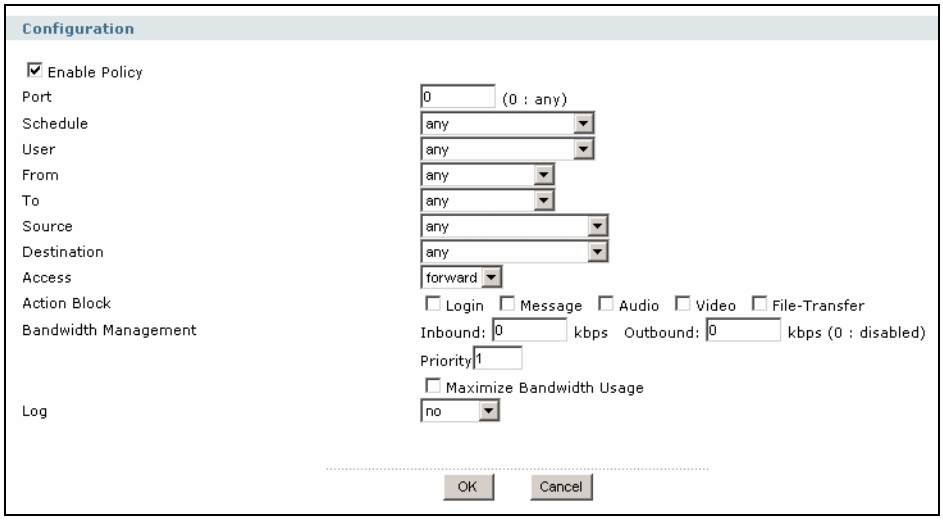
| LABEL | DESCRIPTION |
|---|---|
| BWM | These fields show the amount of bandwidth the application's traffic that matches the policy can use. These fields only apply when **Access** is set to **forward**.<br><br>**In** - This is how much inbound bandwidth, in kilobits per second, this policy allows the application to use. Inbound refers to the traffic the ZyWALL sends to a connection's initiator. If **no** displays here, this policy does not apply bandwidth management for the application's incoming traffic.<br><br>**Out** - This is how much outbound bandwidth, in kilobits per second, this policy allows the application to use. Outbound refers to the traffic the ZyWALL sends out from a connection's initiator. If **no** displays here, this policy does not apply bandwidth management for the application's outgoing traffic.<br><br>**Pri** - This is the priority for this application's traffic that matches this policy. The smaller the number, the higher the priority. The traffic of an application with higher priority is given bandwidth before traffic of an application with lower priority. The ZyWALL ignores this number if the incoming and outgoing limits are both set to 0. In this case the traffic is automatically treated as being set to the lowest priority (7) regardless of this field's configuration. |
| Log | This field shows whether the ZyWALL generates a log (**log**), a log and alert (**log alert**) or neither (**no**) when the application's traffic matches this policy. |
| Add icon | Click the **Add** icon in the heading row to add a new first entry.<br><br>The **Active** icon displays whether the entry is enabled or not. Click the **Active** icon to activate or deactivate the entry. Make sure you click **Apply** to save and apply the change.<br><br>Click the **Edit** icon to go to the screen where you can edit the entry.<br><br>Click the **Add** icon in an entry to add a new entry below the current entry.<br><br>Click the **Remove** icon to delete an existing entry from the ZyWALL. A window displays asking you to confirm that you want to delete the entry.<br><br>To move an entry up or down in the list, click on the **Move to N** icon next to the entry, and type the line number (**#** field) of where you want to move the entry. The **#** field is updated accordingly. The ordering of the entries is important as they are applied in order of their numbering. |
| OK | Click **OK** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving your changes. |

## 29.3.2 The Application Patrol Policy Edit Screen

The **Application Policy Edit** screen allows you to edit a group of settings for an application. To access this screen, go to the application patrol **Common**, **Instant Messenger**, **Peer to Peer**, **VoIP**, or **Streaming** screen and click an application's

**Edit** icon. Then click the **Add** icon or an **Edit** icon in the **Policy** table. The screen displayed here is for the MSN instant messenger service.

**Figure 367** Application Policy Edit




The following table describes the labels in this screen.

**Table 147** Application Policy Edit

| LABEL | DESCRIPTION |
|---|---|
| Enable Policy | Select this check box to turn on this policy for the application. |
| Port | Use this field to specify a specific port number to which to apply this policy. Type zero, if this policy applies for every port number. |
| Schedule | Select a schedule that defines when the policy applies or select **Create Object** to configure a new one (see Chapter 40 on page 677 for details). Otherwise, select **none** to make the policy always effective. |
| User | Select a user name or user group to which to apply the policy. Select **Create Object** to configure a new user account (see Section 37.2.1 on page 652 for details). Select **any** to apply the policy for every user. |
| From | Select the source zone of the traffic to which this policy applies. |
| To | Select the destination zone of the traffic to which this policy applies. |
| Source | Select a source address or address group for whom this policy applies. Select **Create Object** to configure a new one. Select **any** if the policy is effective for every source. |
| Destination | Select a destination address or address group for whom this policy applies. Select **Create Object** to configure a new one. Select **any** if the policy is effective for every destination. |
| Access | This field controls what the ZyWALL does with packets for this application that match this policy. Choices are:<br><br>**forward** - the ZyWALL routes the packets for this application.<br><br>**Drop** - the ZyWALL does not route the packets for this application and does not notify the client of its decision.<br><br>**Reject** - the ZyWALL does not route the packets for this application and notifies the client of its decision. |

**Table 147** Application Policy Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Action Block | For some applications, you can select individual uses of the application that the policy will have the ZyWALL block. These fields only apply when **Access** is set to **forward**.<br><br>**Login** - Select this option to block users from logging in to a server for this application.<br><br>**Message** - Select this option to block users from sending or receiving instant messages.<br><br>**Audio** - Select this option to block users from sending or receiving audio traffic.<br><br>**Video** - Select this option to block users from sending or receiving video traffic.<br><br>**File Transfer** - Select this option to block users from sending or receiving files. |
| Bandwidth Management | Configure these fields to set the amount of bandwidth the application can use. These fields only apply when **Access** is set to **forward**.<br><br>You must also enable bandwidth management in the main application patrol screen (**AppPatrol > General**) in order to apply bandwidth shaping. |
| Inbound kbps | Type how much inbound bandwidth, in kilobits per second, this policy allows the application to use. Inbound refers to the traffic the ZyWALL sends to a connection's initiator.<br><br>If you enter **0** here, this policy does not apply bandwidth management for the application's traffic that the ZyWALL sends to the initiator. Traffic with bandwidth management disabled (inbound and outbound are both set to 0) is automatically treated as the lowest priority (7).<br><br>If the sum of the bandwidths for routes using the same next hop is higher than the actual transmission speed, lower priority traffic may not be sent if higher priority traffic uses all of the actual bandwidth. |
| Outbound kbps | Type how much outbound bandwidth, in kilobits per second, this policy allows the application to use. Outbound refers to the traffic the ZyWALL sends out from a connection's initiator.<br><br>If you enter **0** here, this policy does not apply bandwidth management for the application's traffic that the ZyWALL sends out from the initiator. Traffic with bandwidth management disabled (inbound and outbound are both set to 0) is automatically treated as the lowest priority (7).<br><br>If the sum of the bandwidths for routes using the same next hop is higher than the actual transmission speed, lower priority traffic may not be sent if higher priority traffic uses all of the actual bandwidth. |

**Table 147** Application Policy Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Priority | Enter a number between 1 and 7 to set the priority for this application's traffic that matches this policy. The smaller the number, the higher the priority.<br><br>The ZyWALL gives traffic of an application with higher priority bandwidth before traffic of an application with lower priority.<br><br>The ZyWALL uses a fairness-based (round-robin) scheduler to divide bandwidth between applications with the same priority.<br><br>The number in this field is ignored if the incoming and outgoing limits are both set to 0. In this case the traffic is automatically treated as being set to the lowest priority (7) regardless of this field's configuration. |
| Maximize Bandwidth Usage | Enable maximize bandwidth usage to let the traffic matching this policy "borrow" any unused bandwidth on the out-going interface.<br><br>After each application gets its configured bandwidth rate, the ZyWALL uses the fairness- based scheduler to divide any unused bandwidth on the out-going interface amongst applications that need more bandwidth and have maximize bandwidth usage enabled. |
| Log | Select whether to have the ZyWALL generate a log (**log**), log and alert (**log alert**) or neither (**no**) when the application's traffic matches this policy. See Chapter 47 on page 793 for more on logs. |
| OK | Click **OK** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving your changes. |

# 29.4 The Other Applications Screen

Sometimes, the ZyWALL cannot identify the application. For example, the application might be a new application, or the packets might arrive out of sequence. (The ZyWALL does not reorder packets when identifying the application.)

The **Other** (applications) screen controls the default policy for TCP and UDP traffic that the ZyWALL cannot identify. You can use source zone, destination zone, destination port, schedule, user, source, and destination information as criteria to create a sequence of specific conditions, similar to the sequence of rules used by firewalls, to specify what the ZyWALL should do more precisely. You can also control the bandwidth used by these other applications.This screen also allows you to add, edit, and remove conditions to this default policy.

Click **AppPatrol > Other** to open the **Other (**applications) screen.

**Figure 368** AppPatrol > Other


The following table describes the labels in this screen. See Section 29.4.1 on page 497 for more information as well.

**Table 148** AppPatrol > Other

| LABEL | DESCRIPTION |
|---|---|
| # | This field is a sequential value, and it is not associated with a specific condition.<br><br>Note: The ZyWALL checks conditions in the order they appear in the list. While this sequence does not affect the functionality, you might improve the performance of the ZyWALL by putting more common conditions at the top of the list. |
| Port | This field displays the specific port number to which this policy applies. |
| Schedule | This is the schedule that defines when the policy applies. **any** means the policy always applies. |
| User | This is the user name or user group to which the policy applies. If **any** displays, the policy applies to all users. |
| From | This is the source zone of the traffic to which this policy applies. |
| To | This is the destination zone of the traffic to which this policy applies. |
| Source | This is the source address or address group for whom this policy applies. If **any** displays, the policy is effective for every source. |
| Destination | This is the destination address or address group for whom this policy applies. If **any** displays, the policy is effective for every destination. |
| Protocol | This is the protocol of the traffic to which this policy applies. |
| Access | This field displays what the ZyWALL does with packets that match this policy.<br><br>**forward** - the ZyWALL routes the packets.<br><br>**Drop** - the ZyWALL does not route the packets and does not notify the client of its decision.<br><br>**Reject** - the ZyWALL does not route the packets and notifies the client of its decision. |

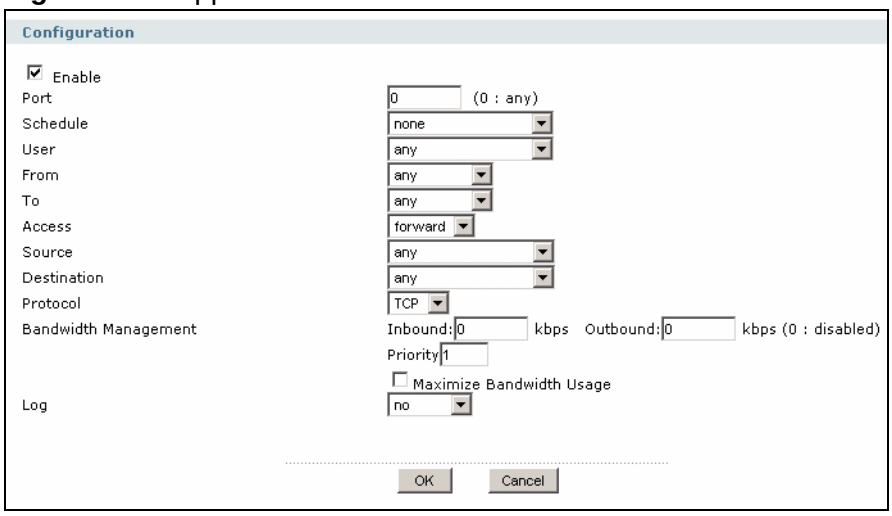
**Table 148** AppPatrol > Other (continued)

| LABEL | DESCRIPTION |
|---|---|
| BWM | These fields show the amount of bandwidth the traffic can use. These fields only apply when **Access** is set to **forward**.<br><br>**In** - This is how much inbound bandwidth, in kilobits per second, this policy allows the matching traffic to use. Inbound refers to the traffic the ZyWALL sends to a connection's initiator. If **no** displays here, this policy does not apply bandwidth management for the inbound traffic.<br><br>**Out** - This is how much outgoing bandwidth, in kilobits per second, this policy allows the matching traffic to use. Outbound refers to the traffic the ZyWALL sends out from a connection's initiator. If **no** displays here, this policy does not apply bandwidth management for the outbound traffic.<br><br>**Pri** - This is the priority for the traffic that matches this policy. The smaller the number, the higher the priority. Traffic with a higher priority is given bandwidth before traffic with a lower priority. The ZyWALL ignores this number if the incoming and outgoing limits are both set to 0. In this case the traffic is automatically treated as being set to the lowest priority (7) regardless of this field's configuration. |
| Log | Select whether to have the ZyWALL generate a log (**log**), log and alert (**log alert**) or neither (**no**) when traffic matches this policy. See Chapter 47 on page 793 for more on logs. |
| Add icon | Click the **Add** icon in the heading row to add a new first entry.<br><br>The **Active** icon displays whether the entry is enabled or not. Click the **Active** icon to activate or deactivate the entry. Make sure you click **Apply** to save and apply the change.<br><br>Click the **Edit** icon to go to the screen where you can edit the entry.<br><br>Click the **Add** icon in an entry to add a new entry below the current entry.<br><br>Click the **Remove** icon to delete an existing entry from the ZyWALL. A window displays asking you to confirm that you want to delete the entry.<br><br>To move an entry up or down in the list, click on the **Move to N** icon next to the entry, and type the line number (**#** field) of where you want to move the entry. The **#** field is updated accordingly. The ordering of the entries is important as they are applied in order of their numbering. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 29.4.1 The Other Applications Add/Edit Screen

The **Other Configuration Add/Edit** screen allows you to create a new condition or edit an existing one. To access this screen, go to the **Other Protocol** screen (see Section 29.4 on page 494), and click either the **Add** icon or an **Edit** icon.

**Figure 369** AppPatrol > Other > Edit




The following table describes the labels in this screen.

**Table 149** AppPatrol > Other > Edit

| LABEL | DESCRIPTION |
|---|---|
| Enable | Select this check box to turn on this policy. |
| Port | Use this field to specify a specific port number to which to apply this policy. Type zero, if this policy applies for every port number. |
| Schedule | Select a schedule that defines when the policy applies or select **Create Object** to configure a new one (see Chapter 40 on page 677 for details). Otherwise, select **any** to make the policy always effective. |
| User | Select a user name or user group to which to apply the policy. Select **Create Object** to configure a new user account (see Section 37.2.1 on page 652 for details). Select **any** to apply the policy for every user. |
| From | Select the source zone of the traffic to which this policy applies. |
| To | Select the destination zone of the traffic to which this policy applies. |
| Access | This field controls what the ZyWALL does with packets that match this policy. Choices are:<br><br>**forward** - the ZyWALL routes the packets.<br><br>**Drop** - the ZyWALL does not route the packets and does not notify the client of its decision.<br><br>**Reject** - the ZyWALL does not route the packets and notifies the client of its decision. |
| Source | Select a source address or address group for whom this policy applies. Select **Create Object** to configure a new one. Select **any** if the policy is effective for every source. |

**Table 149** AppPatrol > Other > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Destination | Select a destination address or address group for whom this policy applies. Select **Create Object** to configure a new one. Select **any** if the policy is effective for every destination. |
| Protocol | Select the protocol for which this condition applies. Choices are: **TCP** and **UDP**. Select **any** to apply the policy to both TCP and UDP traffic. |
| Bandwidth Management | Configure these fields to set the amount of bandwidth the application can use. These fields only apply when **Access** is set to **forward**. |
| Inbound kbps | Type how much inbound bandwidth, in kilobits per second, this policy allows the traffic to use. Inbound refers to the traffic the ZyWALL sends to a connection's initiator.<br><br>If you enter **0** here, this policy does not apply bandwidth management for the matching traffic that the ZyWALL sends to the initiator. Traffic with bandwidth management disabled (inbound and outbound are both set to 0) is automatically treated as the lowest priority (7).<br><br>If the sum of the bandwidths for routes using the same next hop is higher than the actual transmission speed, lower priority traffic may not be sent if higher priority traffic uses all of the actual bandwidth. |
| Outbound kbps | Type how much outbound bandwidth, in kilobits per second, this policy allows the traffic to use. Outbound refers to the traffic the ZyWALL sends out from a connection's initiator.<br><br>If you enter **0** here, this policy does not apply bandwidth management for the matching traffic that the ZyWALL sends out from the initiator. Traffic with bandwidth management disabled (inbound and outbound are both set to 0) is automatically treated as the lowest priority (7).<br><br>If the sum of the bandwidths for routes using the same next hop is higher than the actual transmission speed, lower priority traffic may not be sent if higher priority traffic uses all of the actual bandwidth. |
| Priority | Enter a number between 1 and 7 to set the priority for traffic that matches this policy. The smaller the number, the higher the priority.<br><br>Traffic with a higher priority is given bandwidth before traffic with a lower priority.<br><br>The ZyWALL uses a fairness-based (round-robin) scheduler to divide bandwidth between traffic flows with the same priority.<br><br>The number in this field is ignored if the incoming and outgoing limits are both set to 0. In this case the traffic is automatically treated as being set to the lowest priority (7) regardless of this field's configuration. |
| Maximize Bandwidth Usage | Enable maximize bandwidth usage to let the traffic matching this policy "borrow" any unused bandwidth on the out-going interface.<br><br>After each application or type of traffic gets its configured bandwidth rate, the ZyWALL uses the fairness- based scheduler to divide any unused bandwidth on the out-going interface amongst applications and traffic types that need more bandwidth and have maximize bandwidth usage enabled. |

**Table 149** AppPatrol > Other > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Log | This field controls what kind of record the ZyWALL creates when traffic matches this policy. Please see Chapter 47 on page 793 for more information.<br>**no** - the ZyWALL does not record anything<br>**log** - the ZyWALL creates a record in the log<br>**log alert** - the ZyWALL creates an alert |
| OK | Click **OK** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving your changes. |

# 29.5 Application Patrol Statistics

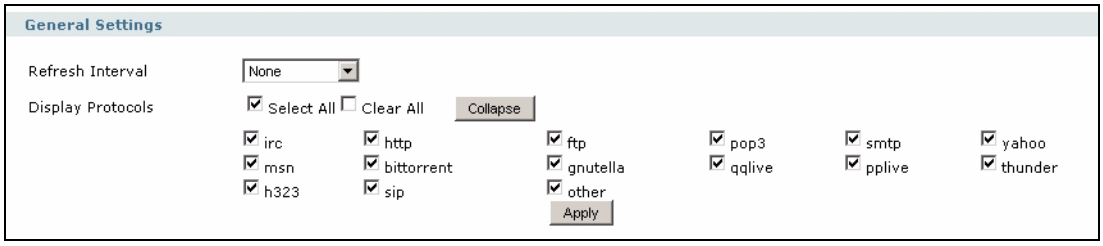
This screen displays a bandwidth usage graph and statistics for selected protocols.

Click **AppPatrol > Statistics** to open the following screen.

## 29.5.1 Application Patrol Statistics: General Setup

Use the top of the **AppPatrol > Statistics** screen to configure what to display.

**Figure 370** AppPatrol > Statistics: General Setup




The following table describes the labels in this screen.

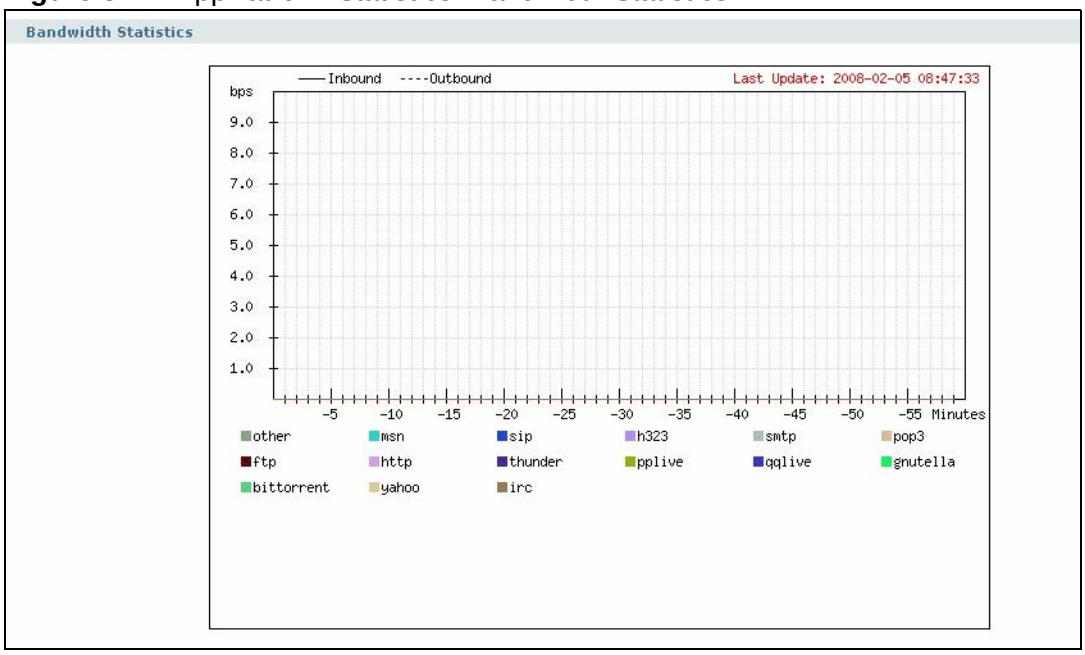
**Table 150** AppPatrol > Statistics: General Setup

| LABEL | DESCRIPTION |
|---|---|
| Refresh Interval | Select how often you want the statistics display to update. |
| Display Protocols | Select the protocols for which to display statistics.<br>**Select All** selects all of the protocols.<br>**Clear All** clears all of the protocols.<br>Click **Expand** to display individual protocols. **Collapse** hides them.<br>Statistics for the selected protocols display after you click **Apply**. |

## 29.5.2 Application Patrol Statistics: Bandwidth Statistics

The middle of the **AppPatrol > Statistics** screen displays a bandwidth usage line graph for the selected protocols.

**Figure 371** AppPatrol > Statistics: Bandwidth Statistics




- The y-axis represents the amount of bandwidth used.
- The x-axis shows the time period over which the bandwidth usage occurred.
- A solid line represents a protocol's incoming bandwidth usage. This is the protocol's traffic that the ZyWALL sends to the initiator of the connection.
- A dotted line represents a protocol's outgoing bandwidth usage. This is the protocol's traffic that the ZyWALL sends out from the initiator of the connection.
- Different colors represent different protocols.

## 29.5.3 Application Patrol Statistics: Protocol Statistics

The bottom of the **AppPatrol > Statistics** screen displays statistics for each of the selected protocols.

**Figure 372** AppPatrol > Statistics: Protocol Statistics

Protocol Statistics

| Service | Forwarded Data(KB) | Dropped Data(KB) | Rejected Data(KB) | Matched Auto Connection | Matched Service Ports Connection |
|---|---|---|---|---|---|
| web-msn | 0 | 0 | 0 | 0 | 0 |
| irc | 0 | 0 | 0 | 0 | 0 |
| yahoo | 0 | 0 | 0 | 0 | 0 |
| aol-icq | 0 | 0 | 0 | 0 | 0 |
| qq | 0 | 0 | 0 | 0 | 0 |
| jabber/google talk | 0 | 0 | 0 | 0 | 0 |
| rediff | 0 | 0 | 0 | 0 | 0 |
| eDonkey | 0 | 0 | 0 | 0 | 0 |
| kad | 0 | 0 | 0 | 0 | 0 |
| bittorrent | 0 | 0 | 0 | 0 | 0 |
| ezpeer | 0 | 0 | 0 | 0 | 0 |
| kuro | 0 | 0 | 0 | 0 | 0 |
| gnutella | 0 | 0 | 0 | 0 | 0 |
| fasttrack | 0 | 0 | 0 | 0 | 0 |
| soulseek | 0 | 0 | 0 | 0 | 0 |
| poco | 0 | 0 | 0 | 0 | 0 |
| qqlive | 0 | 0 | 0 | 0 | 0 |
| pplive | 0 | 0 | 0 | 0 | 0 |
| thunder | 0 | 0 | 0 | 0 | 0 |
| http | 0 | 0 | 0 | 0 | 0 |
| ftp | 0 | 0 | 0 | 0 | 0 |
| pop3 | 0 | 0 | 0 | 0 | 0 |
| smtp | 0 | 0 | 0 | 0 | 0 |
| h323 | 0 | 0 | 0 | 0 | 0 |
| sip | 0 | 0 | 0 | 0 | 0 |
| rtsp | 0 | 0 | 0 | 0 | 0 |
| msn | 0 | 0 | 0 | 0 | 0 |
| other | 0 | 0 | 0 | n/a | 0 |

The following table describes the labels in this screen.

**Table 151** AppPatrol > Statistics: Protocol Statistics

| LABEL | DESCRIPTION |
|---|---|
| Service | This is the protocol. Click the expand icon (+) to display the statistics for each of a protocol's rules. Click the close icon (-) to hide the statistics for each of a protocol's rules. |
| Forwarded Data (KB) | This is how much of the application's traffic the ZyWALL has sent (in kilobytes). |
| Dropped Data (KB) | This is how much of the application's traffic the ZyWALL has discarded without notifying the client (in kilobytes). This traffic was dropped because it matched an application policy set to "drop". |
| Rejected Data (KB) | This is how much of the application's traffic the ZyWALL has discarded and notified the client that the traffic was rejected (in kilobytes). This traffic was rejected because it matched an application policy set to "reject". |
| Matched Auto Connection | This is how much of the application's traffic the ZyWALL identified by examining the IP payload. |
| Matched Service Ports Connection | This is how much of the application's traffic the ZyWALL identified by examining OSI level-3 information such as IP addresses and port numbers. |
| Rule | This is a protocol's rule. |

**Table 151** AppPatrol > Statistics: Protocol Statistics (continued)

| LABEL | DESCRIPTION |
|---|---|
| Inbound Kbps | This is the incoming bandwidth usage for traffic that matched this protocol rule, in kilobits per second. This is the protocol's traffic that the ZyWALL sends to the initiator of the connection. So for a connection initiated from the LAN to the WAN, the traffic sent from the WAN to the LAN is the inbound traffic. |
| Outbound Kbps | This is the outgoing bandwidth usage for traffic that matched this protocol rule, in kilobits per second. This is the protocol's traffic that the ZyWALL sends out from the initiator of the connection. So for a connection initiated from the LAN to the WAN, the traffic sent from the LAN to the WAN is the outbound traffic. |
| Forwarded Data (KB) | This is how much of the application's traffic the ZyWALL has sent (in kilobytes). |
| Dropped Data (KB) | This is how much of the application's traffic the ZyWALL has discarded without notifying the client (in kilobytes). This traffic was dropped because it matched a policy set to "drop". |
| Rejected Data (KB) | This is how much of the application's traffic the ZyWALL has discarded and notified the client that the traffic was rejected (in kilobytes). This traffic was rejected because it matched a policy set to "reject". |

# PART VI
# Anti-X

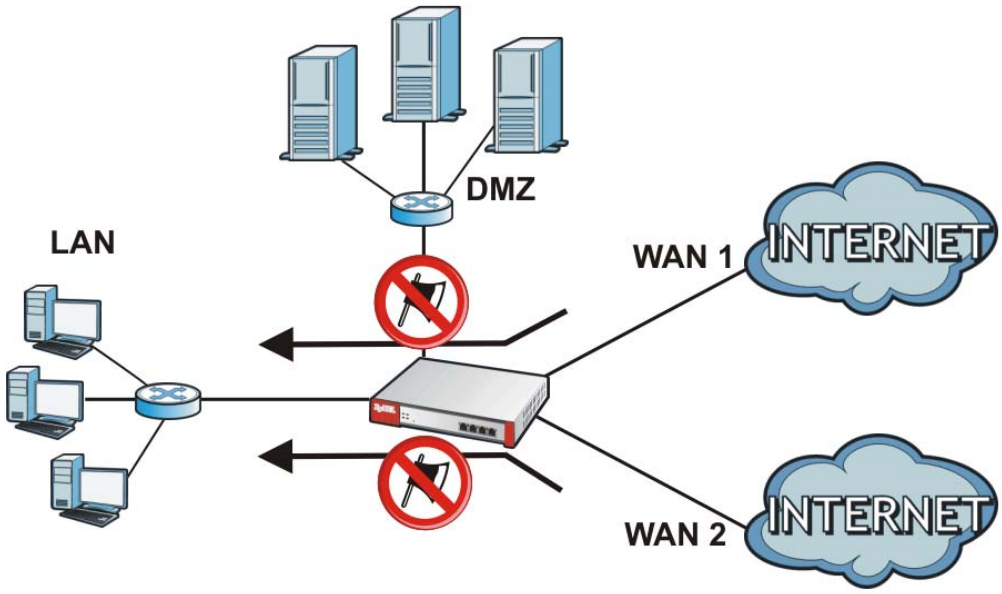
# 30

# Anti-Virus

## 30.1 Overview

Use the ZyWALL's anti-virus feature to protect your connected network from virus/spyware infection. The ZyWALL checks traffic going in the direction(s) you specify for signature matches. In the following figure the ZyWALL is set to check traffic coming from the WAN zone (which includes two interfaces) to the LAN zone.

**Figure 373** ZyWALL Anti-Virus Example




### 30.1.1 What You Can Do in the Anti-Virus Screens

- Use the **General** screens (Section 30.2 on page 508) to turn anti-virus on or off, set up anti-virus policies and check the anti-virus engine type and the anti-virus license and signature status.
- Use the **Black / White List** screen (Section 30.3 on page 513) to set up anti-virus black (blocked) and white (allowed) lists of virus file patterns.
- Use the **Signature** screen (Section 30.6 on page 517) to search signatures to get more information about signatures.

## 30.1.2 What You Need to Know About Anti-Virus

### Anti-Virus Engines

Subscribe to signature files for ZyXEL's anti-virus engine or one powered by Kaspersky. When using the trial, you can switch from one engine to the other in the **Registration** screen. After the trial expires, you need to purchase an iCard for the anti-virus engine you want to use and register it in the **Registration > Service** screen. You must use the ZyXEL anti-virus iCard for the ZyXEL anti-virus engine and the Kaspersky anti-virus iCard for the Kaspersky anti-virus engine. See Chapter 8 on page 165 for details.

### Virus and Worm

A computer virus is a small program designed to corrupt and/or alter the operation of other legitimate programs. A worm is a self-replicating virus that resides in active memory and duplicates itself. The effect of a virus attack varies from doing so little damage that you are unaware your computer is infected to wiping out the entire contents of a hard drive to rendering your computer inoperable.

### ZyWALL Anti-Virus Scanner

The ZyWALL has a built-in signature database. Setting up the ZyWALL between your local network and the Internet allows the ZyWALL to scan files transmitting through the enabled interfaces into your network. As a network-based anti-virus scanner, the ZyWALL helps stop threats at the network edge before they reach the local host computers.

You can set the ZyWALL to examine files received through the following protocols:

- FTP (File Transfer Protocol)
- HTTP (Hyper Text Transfer Protocol)
- SMTP (Simple Mail Transfer Protocol)
- POP3 (Post Office Protocol version 3)
- IMAP4 (Internet Message Access Protocol version 4)

### How the ZyWALL Anti-Virus Scanner Works

The following describes the virus scanning process on the ZyWALL.

1 The ZyWALL first identifies SMTP, POP3, IMAP4, HTTP and FTP packets through standard ports.

2 If the packets are not session connection setup packets (such as SYN, ACK and FIN), the ZyWALL records the sequence of the packets.

3 The scanning engine checks the contents of the packets for virus.

4 If a virus pattern is matched, the ZyWALL removes the infected portion of the file along with the rest of the file. The un-infected portion of the file before a virus pattern was matched still goes through.

5 If the send alert message function is enabled, the ZyWALL sends an alert to the file's intended destination computer(s).

Note: Since the ZyWALL erases the infected portion of the file before sending it, you may not be able to open the file.

### Notes About the ZyWALL Anti-Virus

The following lists important notes about the anti-virus scanner:

1 The ZyWALL anti-virus scanner can detect polymorphic viruses.

2 When a virus is detected, an alert message is displayed in Microsoft Windows computers. Refer to Appendix C on page 909 if your Windows computer does not display the alert messages.

3 Changes to the ZyWALL's anti-virus settings affect new sessions (not the sessions that already existed before you applied the changed settings).

4 The ZyWALL does not scan the following file/traffic types:

- Simultaneous downloads of a file using multiple connections. For example, when you use FlashGet to download sections of a file simultaneously.
- Encrypted traffic. This could be password-protected files or VPN traffic where the ZyWALL is not the endpoint (pass-through VPN traffic).
- Traffic through custom (non-standard) ports. The only exception is FTP traffic. The ZyWALL scans whatever port number is specified for FTP in the ALG screen.
- ZIP file(s) within a ZIP file.

### Finding Out More

- See Section 5.4.14 on page 92 for related information on these screens.
- See Section 30.7 on page 518 for anti-virus background information.

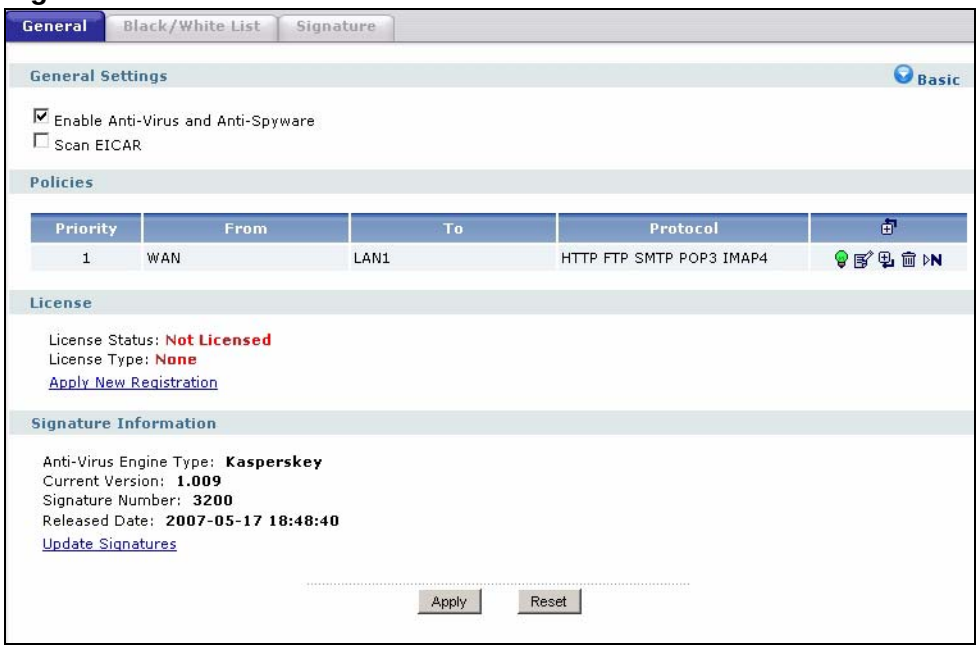
### 30.1.3 Before You Begin

- Before using anti-virus, see Chapter 8 on page 165 for how to register for the anti-virus service.
- You may need to customize the zones (in the **Network** > **Zone**) used for the anti-virus scanning direction.

## 30.2 Anti-Virus Summary Screen

Click **Anti-X** > **Anti-Virus** to display the configuration screen as shown next.

**Figure 374** Anti-X > Anti-Virus > General




The following table describes the labels in this screen.

**Table 152** Anti-X > Anti-Virus > General

| LABEL | DESCRIPTION |
|---|---|
| General Settings | Click **Advanced** to display more settings. Click **Basic** to display fewer settings. |
| Enable Anti-Virus and Anti-Spyware | Select this check box to check traffic for viruses and spyware. The following table lists policies that define which traffic the ZyWALL scans and the action it takes upon finding a virus. |

**Table 152** Anti-X > Anti-Virus > General (continued)

| LABEL | DESCRIPTION |
|---|---|
| Scan EICAR | Select this option to have the ZyWALL check for the EICAR test file and treat it in the same way as a real virus file. The EICAR test file is a standardized test file for signature based anti-virus scanners. When the virus scanner detects the EICAR file, it responds in the same way as if it found a real virus. Besides straightforward detection, the EICAR file can also be compressed to test whether the anti-virus software can detect it in a compressed file. The test string consists of the following human-readable ASCII characters.<br><br>X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H* |
| Priority | This is the position of an anti-virus policy in the list. The ordering of your anti-virus policies is important as the ZyWALL applies them in sequence. Once traffic matches an anti-virus policy, the ZyWALL applies that policy and does not check the traffic against any more policies. |
| From | The anti-virus policy has the ZyWALL scan traffic coming from this zone and going to the **To** zone. |
| To | The anti-virus policy has the ZyWALL scan traffic going to this zone from the **From** zone. |
| Protocol | These are the protocols of traffic to scan for viruses.<br><br>**FTP** applies to traffic using the TCP port number specified for FTP in the ALG screen.<br><br>**HTTP** applies to traffic using TCP ports 80, 8080 and 3128.<br><br>**SMTP** applies to traffic using TCP port 25.<br><br>**POP3** applies to traffic using TCP port 110.<br><br>**IMAP4** applies to traffic using TCP port 143. |
| Add icon | Click the **Add** icon in the heading row to add a new first entry.<br><br>The **Active** displays whether the entry is enabled or not. Click it to activate or deactivate the entry. Make sure you click **Apply** to save and apply the change.<br><br>Click the **Edit** icon to go to the screen where you can edit the entry on the ZyWALL.<br><br>Click the **Add** icon in an entry to add a policy below the current entry.<br><br>Click the **Remove** icon to delete an existing entry from the ZyWALL. A window displays asking you to confirm that you want to delete the entry. Note that subsequent entries move up by one when you take this action.<br><br>In a numbered list, click the **Move to N** icon to display a field to type an index number for where you want to put that entry and press [ENTER] to move the entry to the number that you typed. For example, if you type 6, the policy you are moving becomes number 6 and the previous policy 6 (if there is one) gets pushed up (or down) one.<br><br>The ordering of your policies is important as they are applied in order of their numbering. |

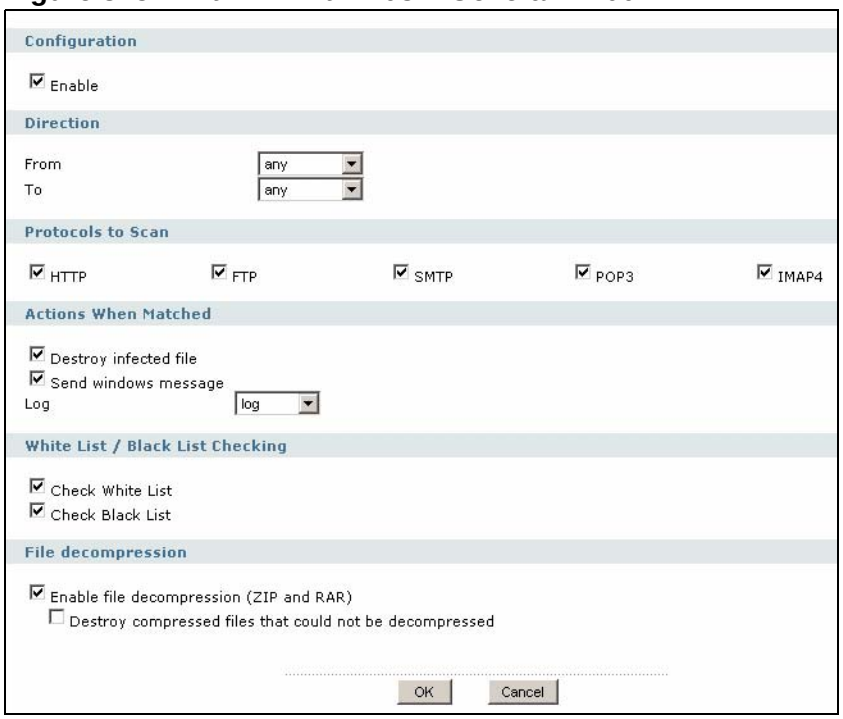
**Table 152** Anti-X > Anti-Virus > General (continued)

| LABEL | DESCRIPTION |
|---|---|
| License | The following fields display information about the current state of your subscription for virus signatures. |
| License Status | This field displays whether a service is activated (**Licensed**) or not (**Not Licensed**) or expired (**Expired**). |
| License Type | This field displays whether you applied for a trial application (**Trial**) or registered a service with your iCard's PIN number (**Standard**). **None** displays when the service is not activated. |
| Apply new Registration | This link appears if you have not registered for the service or only have the trial registration. Click this link to go to the screen where you can register for the service. |
| Signature Information | The following fields display information on the current signature set that the ZyWALL is using. |
| Anti-Virus Engine Type | This field displays whether the ZyWALL is set to use ZyXEL's anti-virus engine or the one powered by Kaspersky.<br><br>Upgrading the ZyWALL to firmware version 2.11 and updating the anti-virus signatures automatically upgrades the ZyXEL anti-virus engine to v2.0. v2.0 has more virus signatures and offers improved non-executable file scan throughput. |
| Current Version | This field displays the anti-virus signature set version number. This number gets larger as the set is enhanced. |
| Signature Number | This field displays the number of anti-virus signatures in this set. |
| Released Date | This field displays the date and time the set was released. |
| Update Signatures | Click this link to go to the screen you can use to download signatures from the update server. |
| Apply | Click **Apply** to save your changes. |
| Reset | Click **Reset** to start configuring this screen again. |

## 30.2.1 Anti-Virus Policy Add or Edit Screen

Click the **Add** or **Edit** icon in the **Anti-X** > **Anti-Virus > General** screen to display the configuration screen as shown next.

**Figure 375** Anti-X > Anti-Virus > General > Add




The following table describes the labels in this screen.

**Table 153** Anti-X > Anti-Virus > General > Add

| LABEL | DESCRIPTION |
|---|---|
| Enable | Select this check box to have the ZyWALL apply this anti-virus policy to check traffic for viruses. |
| From<br><br>To | Select source and destination zones for traffic to scan for viruses. The anti-virus policy has the ZyWALL scan traffic coming from the **From** zone and going to the **To** zone. |
| Protocols to Scan | Select which protocols of traffic to scan for viruses.<br><br>**HTTP** applies to traffic using TCP ports 80, 8080 and 3128.<br><br>**FTP** applies to traffic using the TCP port number specified for FTP in the ALG screen.<br><br>**SMTP** applies to traffic using TCP port 25.<br><br>**POP3** applies to traffic using TCP port 110.<br><br>**IMAP4** applies to traffic using TCP port 143. |
| Actions When Matched | |

**Table 153** Anti-X > Anti-Virus > General > Add (continued)

| LABEL | DESCRIPTION |
|---|---|
| Destroy infected file | When you select this check box, if a virus pattern is matched, the ZyWALL overwrites the infected portion of the file (and the rest of the file) with zeros. The un-infected portion of the file before a virus pattern was matched goes through unmodified. |
| Send Windows Message | Select this check box to set the ZyWALL to send a message alert to files' intended user(s) using Microsoft Windows computers connected to the to interface.<br><br>Refer to Appendix C on page 909 if your Windows computer does not display the alert messages. |
| Log | These are the log options:<br><br>**no**: Do not create a log when a packet matches a signature(s).<br><br>**log**: Create a log on the ZyWALL when a packet matches a signature(s).<br><br>**log alert**: An alert is an e-mailed log for more serious events that may need more immediate attention. Select this option to have the ZyWALL send an alert when a packet matches a signature(s). |
| White List / Black List Checking | |
| Check White List | Select this check box to check files against the white list. |
| Check Black List | Select this check box to check files against the black list. |
| File decompression | |
| Enable file decompression (ZIP and RAR) | Select this check box to have the ZyWALL scan a ZIP file (the file does not have to have a "zip" or "rar" file extension). The ZyWALL first decompresses the ZIP file and then scans the contents for viruses.<br><br>Note: The ZyWALL decompresses a ZIP file once. The ZyWALL does NOT decompress any ZIP file(s) within a ZIP file. |
| Destroy compressed files that could not be decompressed | Note: When you select this option, the ZyWALL deletes ZIP files that use password encryption.<br><br>Select this check box to have the ZyWALL delete any ZIP files that it is not able to unzip. The ZyWALL cannot unzip password protected ZIP files or a ZIP file within another ZIP file. There are also limits to the number of ZIP files that the ZyWALL can concurrently unzip.<br><br>Note: The ZyWALL's firmware package cannot go through the ZyWALL with this option enabled. The ZyWALL classifies the firmware package as not being able to be decompressed and deletes it.<br><br>You can upload the firmware package to the ZyWALL with the option enabled, so you only need to clear this option while you download the firmware package. |

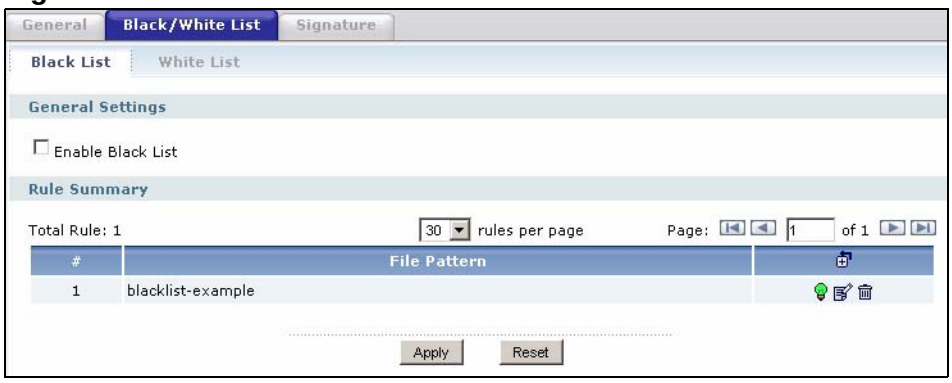
**Table 153** Anti-X > Anti-Virus > General > Add (continued)

| LABEL | DESCRIPTION |
|---|---|
| OK | Click **OK** to save your changes. |
| Cancel | Click **Cancel** to exit this screen without saving your changes. |

# 30.3 Anti-Virus Black List

Click **Anti-X** > **Anti-Virus > Black / White List** to display the screen shown next. Use the **Black List** screen to set up the Anti-Virus black (blocked) list of virus file patterns. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

**Figure 376** Anti-X > Anti-Virus > Black/White List > Black List




The following table describes the labels in this screen.

**Table 154** Anti-X > Anti-Virus > Black/White List > Black List

| LABEL | DESCRIPTION |
|---|---|
| Enable Black List | Select this check box to log and delete files with names that match the black list patterns. Use the black list to log and delete files with names that match the black list patterns. |
| Total Rule | This is the number of entries configured. |
| rules per page | Select how many entries you want to display on each page. |
| Page x of x | This is the number of the page of entries currently displayed and the total number of pages of entries. Type a page number to go to or use the arrows to navigate the pages of entries. |
| # | This is the entry's index number in the list. |
| File Pattern | This is the file name pattern. If a file's name that matches this pattern, the ZyWALL logs and deletes the file. |

**Table 154** Anti-X > Anti-Virus > Black/White List > Black List

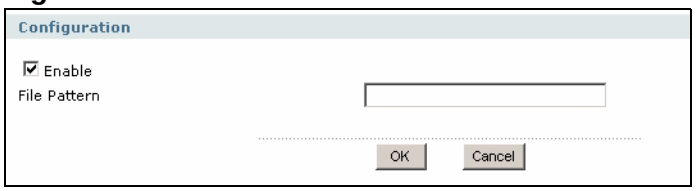
| LABEL | DESCRIPTION |
|---|---|
| Add icon | This column provides icons to add, activate / deactivate, edit, and remove entries.<br><br>To add an entry, click the **Add** icon at the top of the column.<br><br>Click an entry's **Active** icon to activate or deactivate the entry. Make sure you click **Apply** to save and apply the change.<br><br>Click an entry's **Edit** icon to edit the entry.<br><br>To delete an entry, click the entry's **Remove** icon. The Web Configurator confirms that you want to delete the entry. |
| Apply | Click **Apply** to save your changes. |
| Reset | Click **Reset** to start configuring this screen again. |

# 30.4 Anti-Virus Black List or White List Add/Edit

From the **Anti-X** > **Anti-Virus > Black / White List > Black List** (or **White List**) screen, click the **Add** icon or an **Edit** icon to display the following screen.

- For a black list entry, enter a file pattern that should cause the ZyWALL to log and delete a file.
- For a white list entry, enter a file pattern that should cause the ZyWALL to allow a file.

**Figure 377** Anti-X > Anti-Virus > Black/White List > Black List (or White List) > Add



The following table describes the labels in this screen.

**Table 155** Anti-X > Anti-Virus > Black/White List > Black List (or White List) > Add

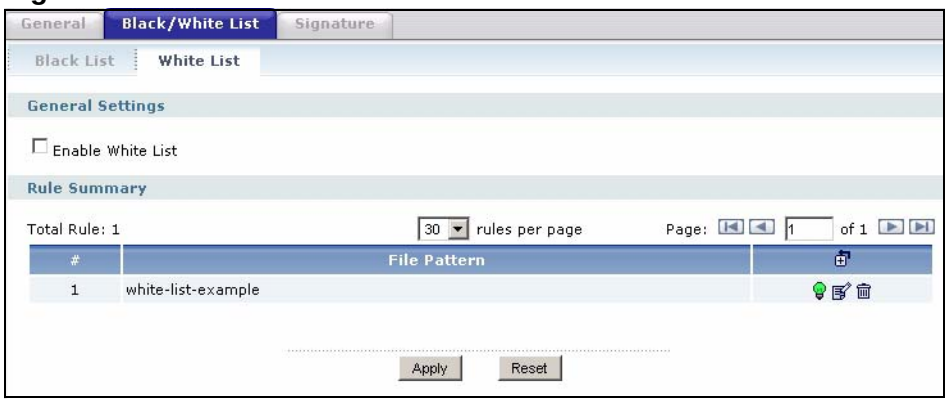
| LABEL | DESCRIPTION |
|---|---|
| Enable | If this is a black list entry, select this option to have the ZyWALL apply this entry when using the black list.<br>If this is a white list entry, select this option to have the ZyWALL apply this entry when using the white list. |
| File Pattern | For a black list entry, specify a pattern to identify the names of files that the ZyWALL should log and delete.<br>For a white list entry, specify a pattern to identify the names of files that the ZyWALL should not scan for viruses.<br>• Use up to 80 characters. Alphanumeric characters, underscores (_), dashes (-), question marks (?) and asterisks (*) are allowed.<br>• A question mark (?) lets a single character in the file name vary. For example, use “a?.zip” (without the quotation marks) to specify aa.zip, ab.zip and so on.<br>• Wildcards (*) let multiple files match the pattern. For example, use “*a.zip” (without the quotation marks) to specify any file that ends with “a.zip”. A file named “testa.zip would match. There could be any number (of any type) of characters in front of the “a.zip” at the end and the file name would still match. A file named “test.zipa” for example would not match.<br>• A * in the middle of a pattern has the ZyWALL check the beginning and end of the file name and ignore the middle. For example, with “abc*.zip”, any file starting with “abc” and ending in “.zip” matches, no matter how many characters are in between.<br>• The whole file name has to match if you do not use a question mark or asterisk.<br>• If you do not use a wildcard, the ZyWALL checks up to the first 80 characters of a file name. |
| OK | Click **OK** to save your changes. |
| Cancel | Click **Cancel** to exit this screen without saving your changes. |

# 30.5 Anti-Virus White List

Click **Anti-X** > **Anti-Virus > Black/White List > White List** to display the screen shown next. Use the **Black/White List** screen to set up Anti-Virus black (blocked) and white (allowed) lists of virus file patterns. Click a column’s heading

cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

**Figure 378** Anti-X > Anti-Virus > Black/White List > White List




The following table describes the labels in this screen.

**Table 156** Anti-X > Anti-Virus > Black/White List > White List

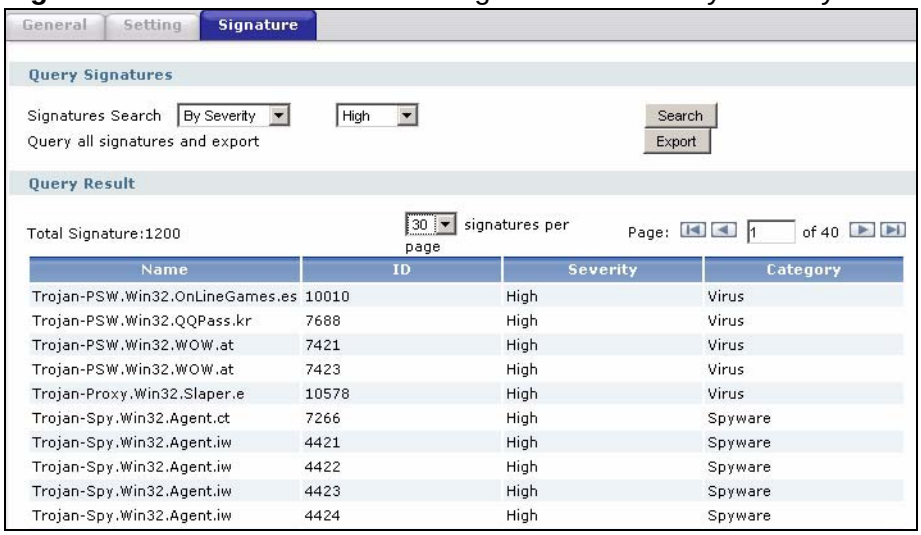
| LABEL | DESCRIPTION |
|---|---|
| Enable White List | Select this check box to have the ZyWALL not perform the anti-virus check on files with names that match the white list patterns.<br><br>Use the white list to have the ZyWALL not perform the anti-virus check on files with names that match the white list patterns. |
| Total Rule | This is the number of entries configured. |
| rules per page | Select how many entries you want to display on each page. |
| Page x of x | This is the number of the page of entries currently displayed and the total number of pages of entries. Type a page number to go to or use the arrows to navigate the pages of entries. |
| # | This is the entry's index number in the list. |
| File Pattern | This is the file name pattern. If a file's name matches this pattern, the ZyWALL does not check the file for viruses. |
| Add icon | This column provides icons to add, activate / deactivate, edit, and remove entries.<br><br>To add an entry, click the **Add** icon at the top of the column. See Section 30.4 on page 514 for details.<br><br>Click an entry's **Active** icon to activate or deactivate the entry. Make sure you click **Apply** to save and apply the change.<br><br>Click an entry's **Edit** icon to edit the entry. See Section 30.4 on page 514 for details.<br><br>To delete an entry, click the entry's **Remove** icon. The Web Configurator confirms that you want to delete the entry. |
| Apply | Click **Apply** to save your changes. |
| Reset | Click **Reset** to start configuring this screen again. |

# 30.6 Signature Searching

Click **Anti-X** > **Anti-Virus > Signature** to display this screen. Use this screen to locate signatures and display details about them.

If Internet Explorer opens a warning screen about a script making Internet Explorer run slowly and the computer maybe becoming unresponsive, just click **No** to continue. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

**Figure 379** Anti-X > Anti-Virus > Signature: Search by Severity




The following table describes the labels in this screen.

**Table 157** Anti-X > Anti-Virus > Signature

| LABEL | DESCRIPTION |
|---|---|
| Signatures Search | Select the criteria on which to perform the search.<br><br>Select **By Name** from the drop down list box and type the name or part of the name of the signature(s) you want to find. This search is not case-sensitive.<br><br>Select **By ID** from the drop down list box and type the ID or part of the ID of the signature you want to find.<br><br>Select **By Severity** from the drop down list box and select the severity level of the signatures you want to find.<br><br>Select **By Category** from the drop down list box and select whether you want to see virus signatures or spyware signatures.<br><br>Click **Search** to have the ZyWALL search the signatures based on your specified criteria. |
| Query all signatures and export | Click **Export** to have the ZyWALL save all of the anti-virus signatures to your computer in a .txt file. |
| Query Result | |

**Table 157** Anti-X > Anti-Virus > Signature (continued)

| LABEL | DESCRIPTION |
|---|---|
| Total Signature | This is the number of signatures that matched your search criteria. |
| signatures per page | Select how many entries you want to display on each page. |
| Page x of x | This is the number of the page of entries currently displayed and the total number of pages of entries. Type a page number to go to or use the arrows to navigate the pages of entries. |
| Name | This is the name of the anti-virus signature. Click the **Name** column heading to sort your search results in ascending or descending order according to the signature name.<br><br>Click a signature's name to see details about the virus. |
| ID | This is the IDentification number of the anti-virus signature. Click the ID column header to sort your search results in ascending or descending order according to the ID. |
| Severity | This is the severity level of the anti-virus signature. Click the severity column header to sort your search results by ascending or descending severity. |
| Category | This column displays whether the signature is for identifying a virus or spyware. Click the column heading to sort your search results by category. |

# 30.7 Anti-Virus Technical Reference

### Types of Computer Viruses

The following table describes some of the common computer viruses.

**Table 158** Common Computer Virus Types

| TYPE | DESCRIPTION |
|---|---|
| File Infector | This is a small program that embeds itself in a legitimate program. A file infector is able to copy and attach itself to other programs that are executed on an infected computer. |
| Boot Sector Virus | This type of virus infects the area of a hard drive that a computer reads and executes during startup. The virus causes computer crashes and to some extend renders the infected computer inoperable. |
| Macro Virus | Macro viruses or Macros are small programs that are created to perform repetitive actions. Macros run automatically when a file to which they are attached is opened. Macros spread more rapidly than other types of viruses as data files are often shared on a network. |

**Table 158** Common Computer Virus Types (continued)

| TYPE | DESCRIPTION |
|---|---|
| E-mail Virus | E-mail viruses are malicious programs that spread through e-mail. |
| Polymorphic Virus | A polymorphic virus (also known as a mutation virus) tries to evade detection by changing a portion of its code structure after each execution or self replication. This makes it harder for an anti-virus scanner to detect or intercept it.<br>A polymorphic virus can also belong to any of the virus types discussed above. |

### Computer Virus Infection and Prevention

The following describes a simple life cycle of a computer virus.

1. A computer gets a copy of a virus from a source such as the Internet, e-mail, file sharing or any removable storage media. The virus is harmless until the execution of an infected program.
2. The virus spreads to other files and programs on the computer.
3. The infected files are unintentionally sent to another computer thus starting the spread of the virus.
4. Once the virus is spread through the network, the number of infected networked computers can grow exponentially.

### Types of Anti-Virus Scanner

The section describes two types of anti-virus scanner: host-based and network-based.

A host-based anti-virus (HAV) scanner is often software installed on computers and/or servers in the network. It inspects files for virus patterns as they are moved in and out of the hard drive. However, host-based anti-virus scanners cannot eliminate all viruses for a number of reasons:

- HAV scanners are slow in stopping virus threats through real-time traffic (such as from the Internet).
- HAV scanners may reduce computing performance as they also share the resources (such as CPU time) on the computer for file inspection.
- You have to update the virus signatures and/or perform virus scans on all computers in the network regularly.

A network-based anti-virus (NAV) scanner is often deployed as a dedicated security device (such as your ZyWALL) on the network edge. NAV scanners inspect real-time data traffic (such as E-mail messages or web) that tends to bypass HAV scanners. The following lists some of the benefits of NAV scanners.

- NAV scanners stops virus threats at the network edge before they enter or exit a network.
- NAV scanners reduce computing loading on computers as the read-time data traffic inspection is done on a dedicated security device.

# 31

# IDP

## 31.1 Overview

This chapter introduces packet inspection IDP (Intrusion, Detection and Prevention), IDP profiles, binding an IDP profile to a traffic flow, custom signatures and updating signatures. An IDP system can detect malicious or suspicious packets and respond instantaneously. IDP on the ZyWALL protects against network-based intrusions.

### 31.1.1 What You Can Do Using the IDP Screens

- Use the **Anti-X > IDP > General** screen (Section 31.2 on page 523) to turn IDP on or off, bind IDP profiles to traffic directions, and view registration and signature information. Click the **Add** or **Edit** icon in this screen to bind an IDP profile to a traffic direction.
- Use the **Anti-X > IDP > Profile** screen (Section 31.3 on page 526) to add a new profile, edit an existing profile or delete an existing profile.
- Use the **Anti-X > IDP > Custom Signature** screens (Section 31.8 on page 540) to create a new signature, edit an existing signature, delete existing signatures or save signatures to your computer.

### 31.1.2 What You Need To Know About IDP

#### Packet Inspection Signatures

A signature identifies a malicious or suspicious packet and specifies an action to be taken. You can change the action in the profile screens. Packet inspection signatures examine OSI (Open System Interconnection) layer-4 to layer-7 packet contents for malicious data. Generally, packet inspection signatures are created for known attacks while anomaly detection looks for abnormal behavior (see Chapter 32 on page 555).

#### Zone

A zone is a combination of ZyWALL interfaces and VPN connections used for configuring security. See the zone chapter for details on zones and the interfaces chapter for details on interfaces.

### IDP Profiles

An IDP profile is a set of related IDP signatures that you can activate as a set and configure common log and action settings. You can apply IDP profiles to traffic flowing from one zone to another. For example, apply the default LAN_IDP profile to any traffic going to the LAN zone in order to protect your LAN computers.

Note: You can only apply one IDP profile to one traffic flow.

### Base IDP Profiles

Base IDP profiles are templates that you use to create new IDP profiles.The ZyWALL comes with several base profiles. See Table 161 on page 527 for details on base profiles.

### IDP Policies

An IDP policy refers to application of an IDP profile to a traffic flowing from one zone to another.

### Applying Your IDP Configuration

Changes to the ZyWALL's IDP settings affect new sessions (not the sessions that already existed before you applied the changed settings).

### Finding Out More

- See Section 5.4.15 on page 93 for IDP prerequisite information.
- See Chapter 32 on page 555 for anomaly detection and protection.
- See Section 31.9 on page 552 for more information on network-based intrusions
- See Section 31.6.2 on page 533 for a list of attacks that the ZyWALL can protect against.
- See Section 31.7 on page 538 for how to create your own custom IDP signatures.

## 31.1.3 Before You Begin

- Register for a trial IDP subscription in the **Registration** screen (see Section 8.2 on page 167). This gives you access to free signature updates. This is important as new signatures are created as new attacks evolve. When the trial subscription expires, purchase and enter a license key using the same screens to continue the subscription.
- Configure zones on the ZyWALL - see Chapter 14 on page 297 for more information.

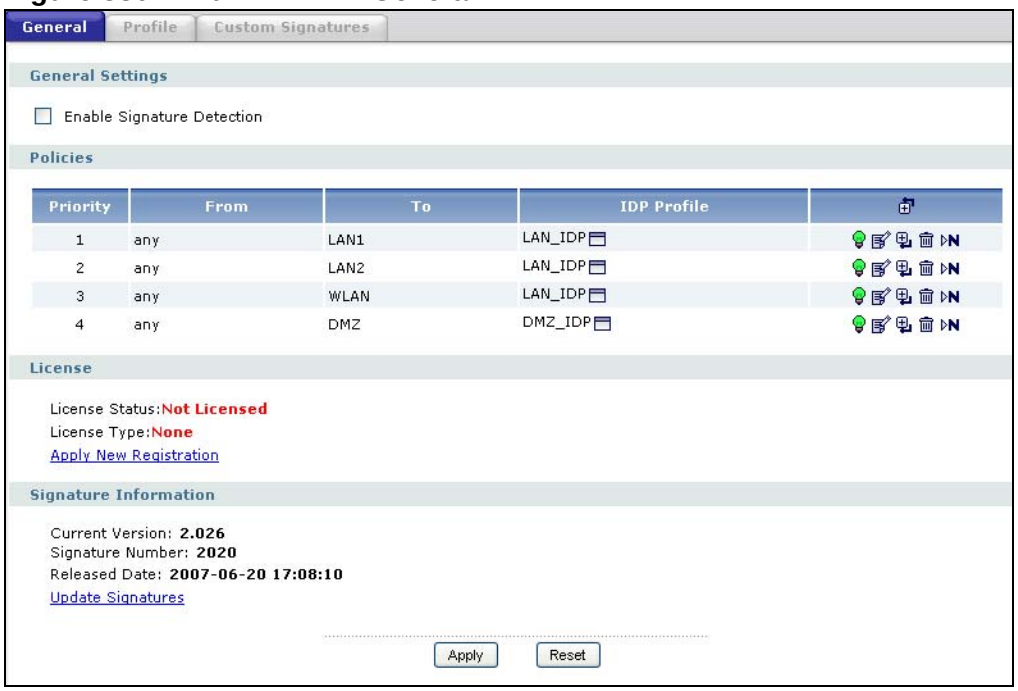
# 31.2 The IDP General Screen

Click **Anti-X > IDP > General** to open this screen. Use this screen to turn IDP on or off, bind IDP profiles to traffic directions, and view registration and signature information.

Note: You must register in order to use packet inspection signatures. See the **Registration** screens.

If you try to enable IDP when the IDP service has not yet been registered, a warning screen displays and IDP is not enabled.

**Figure 380** Anti-X > IDP > General




The following table describes the screens in this screen.

**Table 159** Anti-X > IDP > General

| LABEL | DESCRIPTION |
|---|---|
| General Settings | |
| Enable Signature Detection | You must register for IDP service in order to use packet inspection signatures. If you don't have a standard license, you can register for a once-off trial one. |
| Policies | Use this list to specify which IDP profile the ZyWALL uses for traffic flowing in a specific direction. |
| Priority | IDP policies are applied in order of priority. |

**Table 159** Anti-X > IDP > General (continued)

| LABEL | DESCRIPTION |
|---|---|
| From, To | This is the direction of travel of packets to which an IDP profile is bound.<br><br>Note: Depending on your network topology and traffic load, binding every packet direction to an IDP profile may affect the ZyWALL's performance.<br><br>**From LAN1 To LAN1** means packets traveling from a computer on one LAN1 subnet to a computer on another LAN subnet via the ZyWALL's LAN1 zone interfaces. The ZyWALL does not check packets traveling from a LAN1 computer to another LAN1 computer on the same subnet.<br><br>**From WAN To WAN** means packets that come in from the WAN zone and the ZyWALL routes back out through the WAN zone. |
| IDP Profile | This field shows which IDP profile is bound to which traffic direction. Click the **popup** icon to change to a different profile. |
| Add icon | Click the **Add** icon in the heading row to add a new first entry.<br><br>The **Active** icon displays whether the entry is enabled or not. Click it to activate or deactivate the entry. Make sure you click **Apply** to save and apply the change.<br><br>Click the **Edit** icon to go to the screen where you can edit the entry.<br><br>Click the **Add** icon in an entry to add an entry below the current entry.<br><br>Click the **Remove** icon to delete an existing entry from the ZyWALL. A window displays asking you to confirm that you want to delete the entry. Note that subsequent entries move up by one when you take this action.<br><br>In a numbered list, click the **Move to N** icon to display a field to type an index number for where you want to put that entry and press [ENTER] to move the entry to the number that you typed. For example, if you type 6, the entry you are moving becomes number 6 and the previous entry 6 (if there is one) gets pushed up (or down) one.<br><br>The ordering of your entries is important as they are applied in order of their numbering. |
| License | You need to create an account at myZyXEL.com, register your ZyWALL and then subscribe for IDP in order to be able to download new packet inspection signatures from myZyXEL.com. There's an initial free trial period for IDP after which you must pay to subscribe to the service. See the Registration chapter for details. |
| License Status | **Licensed**, **Not Licensed** or **Expired** indicates whether you have subscribed for IDP services or not or your registration has expired. |
| License Type | This field shows **Trial**, **Standard** or **None** depending on whether you subscribed to the IDP trial, bought an iCard for IDP service or neither. |

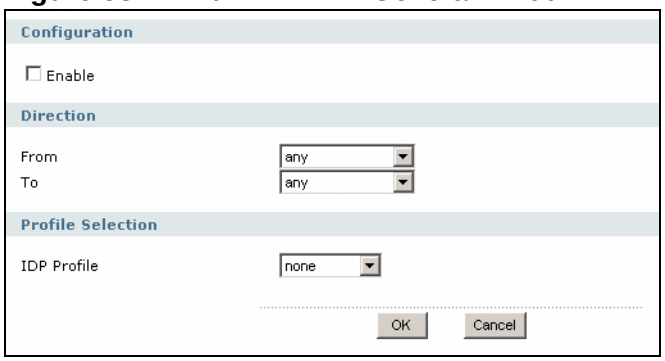
**Table 159** Anti-X > IDP > General (continued)

| LABEL | DESCRIPTION |
|---|---|
| Apply new Registration | This link appears if you have not registered for the service or only have the trial registration. Click this link to go to the screen where you can register for the service. |
| Signature Information | The following fields display information on the current signature set that the ZyWALL is using. |
| Current Version | This field displays the IDP signature set version number. This number gets larger as the set is enhanced. |
| Signature Number | This field displays the number of IDP signatures in this set. This number usually gets larger as the set is enhanced. Older signatures and rules may be removed if they are no longer applicable or have been supplanted by newer ones. |
| Released Date | This field displays the date and time the set was released. |
| Update Signatures | Click this link to go to the screen you can use to download signatures from the update server. |
| Apply | Click **Apply** to save your changes. |
| Reset | Click **Reset** to start configuring this screen again. |

## 31.2.1 Configuring IDP Policies

Click **Anti-X > IDP > General** and then an **Add** or **Edit** icon to display the following screen. Use this screen to apply an IDP profile to traffic flowing from one zone to another.

**Figure 381** Anti-X > IDP > General > Add




The following table describes the screens in this screen.

**Table 160** Anti-X > IDP > General > Add

| LABEL | DESCRIPTION |
|---|---|
| Enable | Select this check box to turn on this IDP profile to traffic direction binding. |
| From | Traffic direction is defined by the zone the traffic is coming from and the zone the traffic is going to.<br>Use the **From** field to specify the zone from which the traffic is coming. |

**Table 160** Anti-X > IDP > General > Add (continued)

| LABEL | DESCRIPTION |
|---|---|
| To | Use the **To** field to specify the zone to which the traffic is going. |
| IDP Profile | Select an IDP profile to apply to the entry's traffic direction. Configure the IDP profiles in the IDP profile screens. |
| OK | Click **OK** to save your changes. |
| Cancel | Click **Cancel** to exit this screen without saving your changes. |

# 31.3 Introducing IDP Profiles

An IDP profile is a set of packet inspection signatures.

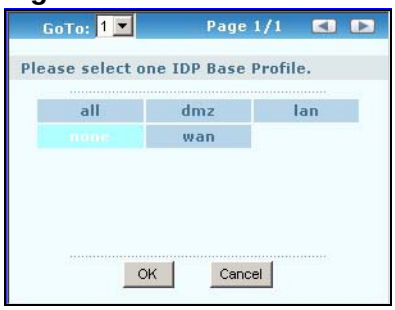
Packet inspection signatures examine packet content for malicious data. Packet inspection applies to OSI (Open System Interconnection) layer-4 to layer-7 contents. You need to subscribe for IDP service in order to be able to download new signatures.

In general, packet inspection signatures are created for known attacks while anomaly detection looks for abnormal behavior (see Chapter 32 on page 555 for information on anomaly detection).

## 31.3.1 Base Profiles

The ZyWALL comes with several base profiles. You use base profiles to create new profiles. In the **Anti-X > IDP > Profile** screen, click the **Add** icon to display the following screen.

**Figure 382** Base Profiles



The following table describes this screen.

**Table 161** Base Profiles

| BASE PROFILE | DESCRIPTION |
|---|---|
| all | All signatures are enabled. Signatures with a high or severe severity level (greater than three) generate log alerts and cause packets that trigger them to be dropped. Signatures with a very low, low or medium severity level (less than or equal to three) generate logs (not log alerts) and no action is taken on packets that trigger them. |
| dmz | This profile is most suitable for networks containing your servers. Signatures for common services such as DNS, FTP, HTTP, ICMP, IMAP, MISC, NETBIOS, POP3, RPC, RSERVICE, SMTP, SNMP, SQL, TELNET, Oracle, MySQL are enabled. Signatures with a high or severe severity level (greater than three) generate log alerts and cause packets that trigger them to be dropped. Signatures with a low or medium severity level (two or three) generate logs (not log alerts) and no action is taken on packets that trigger them. Signatures with a very low severity level (one) are disabled. |
| lan | This profile is most suitable for common LAN network services. Signatures for common services such as DNS, FTP, HTTP, ICMP, IM, IMAP, MISC, NETBIOS, P2P, POP3, RPC, RSERVICE, SMTP, SNMP, SQL, TELNET, TFTP, MySQL are enabled. Signatures with a high or severe severity level (greater than three) generate logs (not log alerts) and cause packets that trigger them to be dropped. Signatures with a low or medium severity level (two or three) generate logs (not log alerts) and no action is taken on packets that trigger them. Signatures with a very low severity level (one) are disabled. |
| none | All signatures are disabled. No logs are generated nor actions are taken. |
| wan | Signatures for all services are enabled. Signatures with a medium, high or severe severity level (greater than two) generate logs (not log alerts) and no action is taken on packets that trigger them. Signatures with a very low or low severity level (less than or equal to two) are disabled. |
| OK | Click **OK** to save your changes. |
| Cancel | Click **Cancel** to exit this screen without saving your changes. |

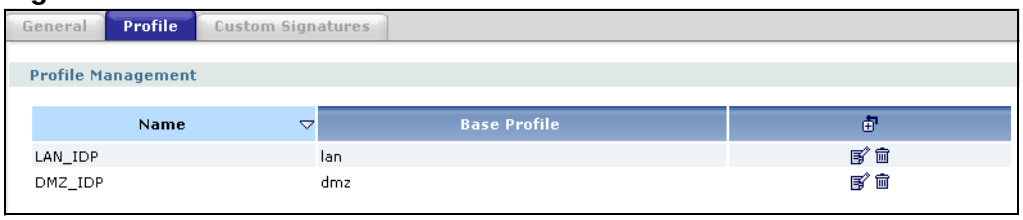
# 31.4 The Profile Summary Screen

Select **Anti-X > IDP > Profile**. Use this screen to:

- Add a new profile
- Edit an existing profile
- Delete an existing profile.

Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

**Figure 383** Anti-X > IDP > Profile




The following table describes the fields in this screen.

**Table 162** Anti-X > IDP > Profile

| LABEL | DESCRIPTION |
|---|---|
| Name | This is the name of the profile you created. |
| Base Profile | This is the base profile from which the profile was created. |
| Add icon | Click the **Add** icon in the column header to create a new profile. A pop-up screen displays requiring you to choose a base profile from which to create the new profile.<br><br>Click an **Edit** icon to edit an existing profile.<br><br>Click a **Remove** icon to delete an existing profile. |

# 31.5 Creating New Profiles

You may want to create a new profile if not all signatures in a base profile are applicable to your network. In this case you should disable non-applicable signatures so as to improve ZyWALL IDP processing efficiency.

You may also find that certain signatures are triggering too many false positives or false negatives. A false positive is when valid traffic is flagged as an attack. A false negative is when invalid traffic is wrongly allowed to pass through the ZyWALL. As each network is different, false positives and false negatives are common on initial IDP deployment.

You could create a new 'monitor profile' that creates logs but all actions are disabled. Observe the logs over time and try to eliminate the causes of the false alarms. When you're satisfied that they have been reduced to an acceptable level, you could then create an 'inline profile' whereby you configure appropriate actions to be taken when a packet matches a signature.

## 31.5.1 Procedure To Create a New Profile

To create a new profile:

1 Click the **Add** icon in the **Anti-X > IDP > Profile** screen to display a pop-up screen allowing you to choose a base profile.

2 Select a base profile (see Table 161 on page 527) and then click **OK** to go to the profile details screen.

Note: If Internet Explorer opens a warning screen about a script making Internet Explorer run slowly and the computer maybe becoming unresponsive, just click **No** to continue.

3 Type a new profile name

4 Enable or disable individual signatures.

5 Edit the default log options and actions.

## 31.6 Profiles: Packet Inspection

Select **Anti-X > IDP > Profile** and then add a new or edit an existing profile select. Packet inspection signatures examine the contents of a packet for malicious data. It operates at layer-4 to layer-7.

## 31.6.1 Profile > Group View Screen

**Figure 384** Anti-X > IDP > Profile > Edit : Group View

The following table describes the fields in this screen.

**Table 163** Anti-X > IDP > Profile > Group View

| LABEL | DESCRIPTION |
|---|---|
| Name | This is the name of the profile. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. These are valid, unique profile names:<br>MyProfile<br>mYProfile<br>Mymy12_3-4<br>These are invalid profile names:<br>1mYProfile<br>My Profile<br>MyProfile?<br>Whatalongprofilename123456789012 |
| Switch to query view | Click this button to go to a screen where you can search for signatures by criteria such as name, ID, severity, attack type, vulnerable attack platforms, service category, log options or actions. |
| Service | Click the + sign next to a service group to expand it. A service group is a group of related IDP signatures. |
| Message | This is the name of the signature. |
| SID | This is the signature ID (identification) number that uniquely identifies a ZyWALL signature. |
| Severity | These are the severities as defined in the ZyWALL. The number in brackets is the number you use if using commands.<br>**Severe** (5): These denote attacks that try to run arbitrary code or gain system privileges.<br>**High** (4): These denote known serious vulnerabilities or attacks that are probably not false alarms.<br>**Medium** (3): These denote medium threats, access control attacks or attacks that could be false alarms.<br>**Low** (2): These denote mild threats or attacks that could be false alarms.<br>**Very Low** (1): These denote possible attacks caused by traffic such as Ping, trace route, ICMP queries etc. |
| Policy Type | This is the attack type as defined on the ZyWALL. See Table 164 on page 533 for a description of each type. |
| Activation | Click the icon to enable or disable a signature or group of signatures. |

**Table 163** Anti-X > IDP > Profile > Group View (continued)

| LABEL | DESCRIPTION |
|---|---|
| Log | These are the log options:<br><br>**original setting**: Select this option to return each log option within a service group to its previously saved configuration.<br><br>**no**: Select this option on an individual signature or a complete service group to have the ZyWALL create no log when a packet matches a signature(s).<br><br>**log**: Select this option on an individual signature or a complete service group to have the ZyWALL create a log when a packet matches a signature(s).<br><br>**log alert**: An alert is an e-mailed log for more serious events that may need more immediate attention. Select this option to have the ZyWALL send an alert when a packet matches a signature(s). |
| Action | Select what action the ZyWALL should take when a packet matches a signature here.<br><br>**original setting**: Select this action to return each signature in a service group to its previously saved configuration.<br><br>**none**: Select this action on an individual signature or a complete service group to have the ZyWALL take no action when a packet matches the signature(s).<br><br>**drop**: Select this action on an individual signature or a complete service group to have the ZyWALL silently drop a packet that matches the signature(s). Neither sender nor receiver are notified.<br><br>**reject-sender**: Select this action on an individual signature or a complete service group to have the ZyWALL send a reset to the sender when a packet matches the signature. If it is a TCP attack packet, the ZyWALL will send a packet with a 'RST' flag. If it is an ICMP or UDP attack packet, the ZyWALL will send an ICMP unreachable packet.<br><br>**reject-receiver**: Select this action on an individual signature or a complete service group to have the ZyWALL send a reset to the receiver when a packet matches the signature. If it is a TCP attack packet, the ZyWALL will send a packet with an a 'RST' flag. If it is an ICMP or UDP attack packet, the ZyWALL will do nothing.<br><br>**reject-both**: Select this action on an individual signature or a complete service group to have the ZyWALL send a reset to both the sender and receiver when a packet matches the signature. If it is a TCP attack packet, the ZyWALL will send a packet with a 'RST' flag to the receiver and sender. If it is an ICMP or UDP attack packet, the ZyWALL will send an ICMP unreachable packet. |
| OK | A profile consists of three separate screens. If you want to configure just one screen for an IDP profile, click **OK** to save your settings to the ZyWALL, complete the profile and return to the profile summary page. |

**Table 163** Anti-X > IDP > Profile > Group View (continued)

| LABEL | DESCRIPTION |
|---|---|
| Cancel | Click **Cancel** to return to the profile summary page without saving any changes. |
| Save | If you want to configure more than one screen for an IDP profile, click **Save** to save the configuration to the ZyWALL, but remain in the same page. You may then go to another profile screen (tab) in order to complete the profile. Click **OK** in the final profile screen to complete the profile. |

## 31.6.2 Policy Types

This section describes IDP policy types, also known as attack types, as categorized in the ZyWALL. You may refer to these types when categorizing your own custom rules.

**Table 164** Policy Types

| POLICY TYPE | DESCRIPTION |
|---|---|
| P2P | Peer-to-peer (P2P) is where computing devices link directly to each other and can directly initiate communication with each other; they do not need an intermediary. A device can be both the client and the server. In the ZyWALL, P2P refers to peer-to-peer applications such as e-Mule, e-Donkey, BitTorrent, iMesh, etc. |
| IM | IM (Instant Messenger) refers to chat applications. Chat is real-time, text-based communication between two or more users via networks-connected computers. After you enter a chat (or chat room), any room member can type a message that will appear on the monitors of all the other participants. |
| SPAM | Spam is unsolicited “junk” e-mail sent to large numbers of people to promote products or services. |
| DoS/DDoS | The goal of Denial of Service (DoS) attacks is not to steal information, but to disable a device or network on the Internet.<br><br>A Distributed Denial of Service (DDoS) attack is one in which multiple compromised systems attack a single target, thereby causing denial of service for users of the targeted system. |
| Scan | A scan describes the action of searching a network for an exposed service. An attack may then occur once a vulnerability has been found. Scans occur on several network levels.<br><br>A network scan occurs at layer-3. For example, an attacker looks for network devices such as a router or server running in an IP network.<br><br>A scan on a protocol is commonly referred to as a layer-4 scan. For example, once an attacker has found a live end system, he looks for open ports.<br><br>A scan on a service is commonly referred to a layer-7 scan. For example, once an attacker has found an open port, say port 80 on a server, he determines that it is a HTTP service run by some web server application. He then uses a web vulnerability scanner (for example, Nikto) to look for documented vulnerabilities. |

**Table 164** Policy Types (continued)

| POLICY TYPE | DESCRIPTION |
|---|---|
| Buffer Overflow | A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. The excess information can overflow into adjacent buffers, corrupting or overwriting the valid data held in them.<br><br>Intruders could run codes in the overflow buffer region to obtain control of the system, install a backdoor or use the victim to launch attacks on other devices. |
| Virus/Worm | A computer virus is a small program designed to corrupt and/or alter the operation of other legitimate programs. A worm is a program that is designed to copy itself from one computer to another on a network. A worm's uncontrolled replication consumes system resources, thus slowing or stopping other tasks. |
| Backdoor/Trojan | A backdoor (also called a trapdoor) is hidden software or a hardware mechanism that can be triggered to gain access to a program, online service or an entire computer system. A Trojan horse is a harmful program that is hidden inside apparently harmless programs or data.<br><br>Although a virus, a worm and a Trojan are different types of attacks, they can be blended into one attack. For example, W32/Blaster and W32/Sasser are blended attacks that feature a combination of a worm and a Trojan. |
| Access Control | Access control refers to procedures and controls that limit or detect access. Access control attacks try to bypass validation checks in order to access network resources such as servers, directories, and files. |
| Web Attack | Web attacks refer to attacks on web servers such as IIS (Internet Information Services). |

## 31.6.3 IDP Service Groups

An IDP service group is a set of related packet inspection signatures.

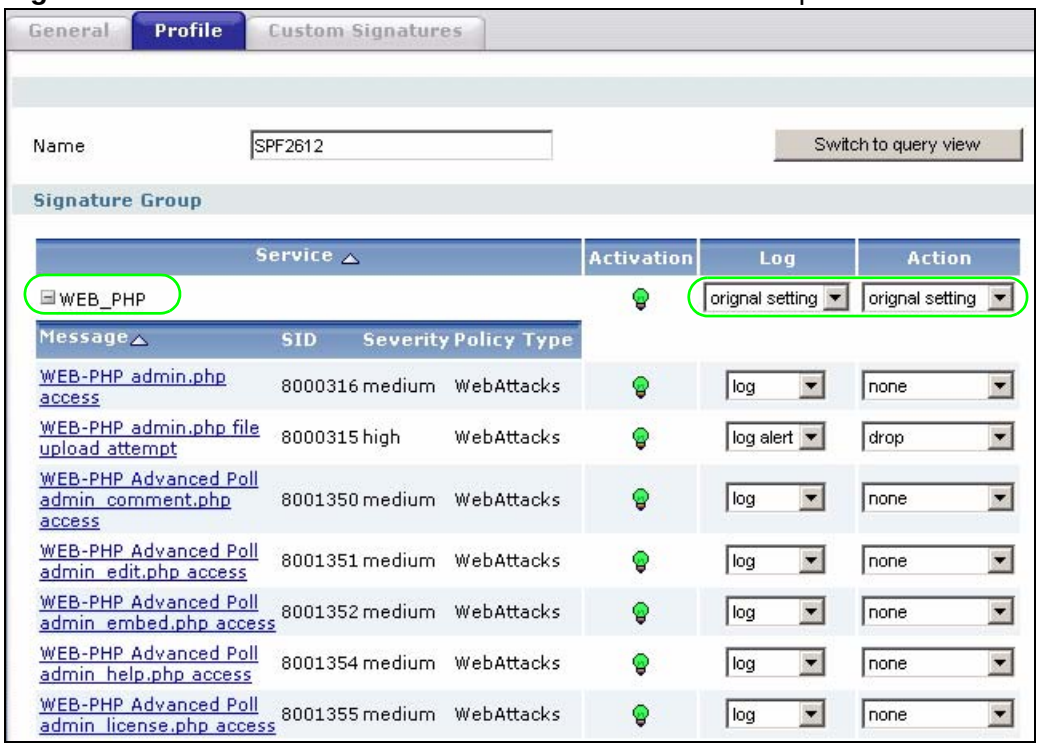
**Table 165** IDP Service Groups

| | | | |
|---|---|---|---|
| WEB_PHP | WEB_MISC | WEB_IIS | WEB_FRONTPAGE |
| WEB_CGI | WEB_ATTACKS | TFTP | TELNET |
| SQL | SNMP | SMTP | RSERVICES |
| RPC | POP3 | POP2 | P2P |
| ORACLE | NNTP | NETBIOS | MYSQL |
| MISC_EXPLOIT | MISC_DDOS | MISC_BACKDOOR | MISC |
| IMAP | IM | ICMP | FTP |
| FINGER | DNS | | |

The following figure shows the WEB_PHP service group that contains signatures related to attacks on web servers using PHP exploits. PHP (PHP: Hypertext Preprocessor) is a server-side HTML embedded scripting language that allows web developers to build dynamic websites.

Logs and actions applied to a service group apply to all signatures within that group. If you select **original setting** for service group logs and/or actions, all signatures within that group are returned to their last-saved settings.

**Figure 385** Anti-X > IDP > Profile > Edit > IDP Service Group

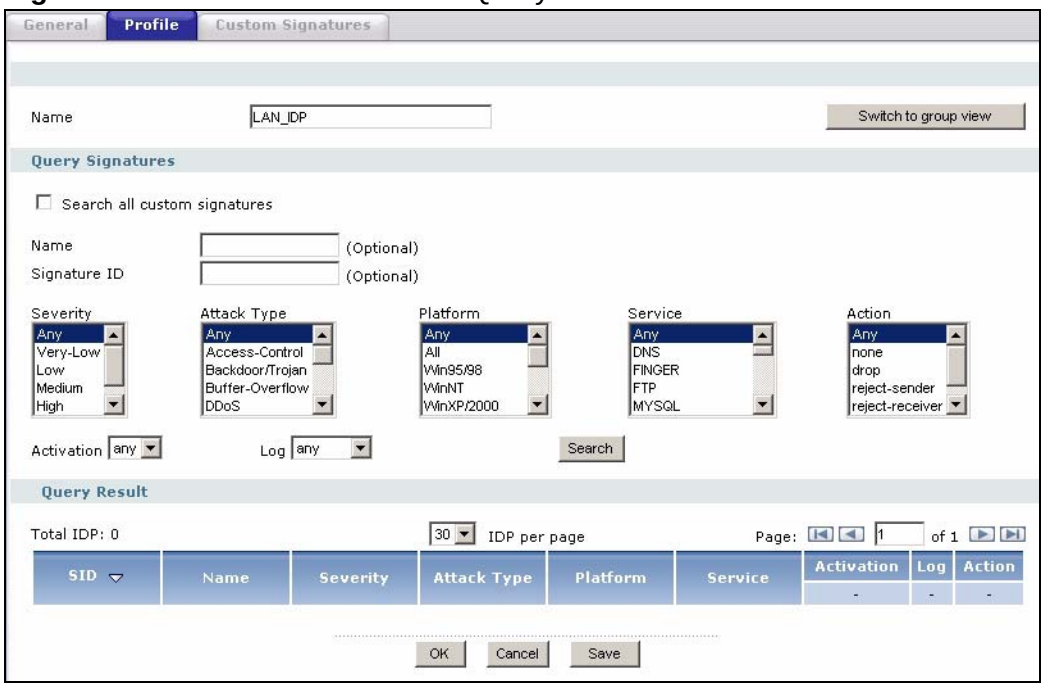



## 31.6.4 Profile > Query View Screen

Click **Switch to query view** in the screen as shown in Figure 384 on page 530 to go to a signature query screen. In the query view screen, you can search for

signatures by criteria such as name, ID, severity, attack type, vulnerable attack platforms, service category, log options or actions.

**Figure 386** Anti-X > IDP > Profile: Query View




The following table describes the fields in this screen.

**Table 166** Anti-X > IDP > Profile: Query View

| LABEL | DESCRIPTION |
|---|---|
| Name | This is the name of the profile that you created in the **IDP > Profiles > Group View** screen. |
| Switch to group view | Click this button to go to the IDP profile group view screen where IDP signatures are grouped by service and you can configure activation, logs and/or actions. |
| Query Signatures | Select the criteria on which to perform the search. |
| Search all custom signatures | Select this check box to search for signatures you created or imported in the **Custom Signatures** screen. You can search by name or ID. If the name and ID fields are left blank, then all custom signatures are displayed. |
| Name | Type the name or part of the name of the signature(s) you want to find. |
| Signature ID | Type the ID or part of the ID of the signature(s) you want to find. |
| Severity | Search for signatures by severity level(s) (see Table 163 on page 531). Hold down the [Ctrl] key if you want to make multiple selections. |
| Attack Type | Search for signatures by attack type(s) (see Table 164 on page 533). Attack types are known as policy types in the group view screen. Hold down the [Ctrl] key if you want to make multiple selections. |

**Table 166** Anti-X > IDP > Profile: Query View (continued)

| LABEL | DESCRIPTION |
|---|---|
| Platform | Search for signatures created to prevent intrusions targeting specific operating system(s). Hold down the [Ctrl] key if you want to make multiple selections. |
| Service | Search for signatures by IDP service group(s). See Table 165 on page 534 for group details. Hold down the [Ctrl] key if you want to make multiple selections. |
| Action | Search for signatures by the response the ZyWALL takes when a packet matches a signature. See Table 163 on page 531 for action details. Hold down the [Ctrl] key if you want to make multiple selections. |
| Activation | Search for enabled and/or disabled signatures here. |
| Log | Search for signatures by log option here. See Table 163 on page 531 for option details. |
| Search | Click this button to begin the search. The results display at the bottom of the screen. Results may be spread over several pages depending on how broad the search criteria selected were. The tighter the criteria selected, the fewer the signatures returned. |
| Query Result | The results are displayed in a table showing the **SID**, **Name**, **Severity**, **Attack Type**, **Platform**, **Service**, **Activation**, **Log**, and **Action** criteria as selected in the search. Click the **SID** column header to sort search results by signature ID. |
| Total IDP: | This displays the total number of signatures found in your search. |
| IDP per page | Select the number of signatures you want to appear per page here. |
| Page x of x | This is the number of the page of entries currently displayed and the total number of pages of entries. Type a page number to go to or use the arrows to navigate the pages of entries. |
| OK | Click **OK** to save your settings to the ZyWALL, complete the profile and return to the profile summary page. |
| Cancel | Click **Cancel** to return to the profile summary page without saving any changes. |
| Save | Click **Save** to save the configuration to the ZyWALL, but remain in the same page. You may then go to the another profile screen (tab) in order to complete the profile. Click **OK** in the final profile screen to complete the profile. |

## 31.6.5 Query Example

This example shows a search with these criteria:

- Severity: severe and high
- Attack Type: DDoS
- Platform: Windows 2000 and Windows XP computers
- Service: Any

- Actions: Any

**Figure 387** Query Example Search Criteria

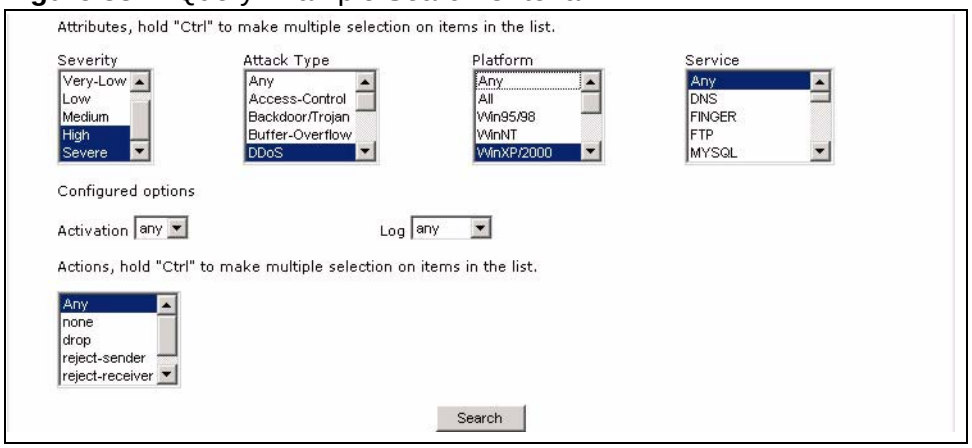
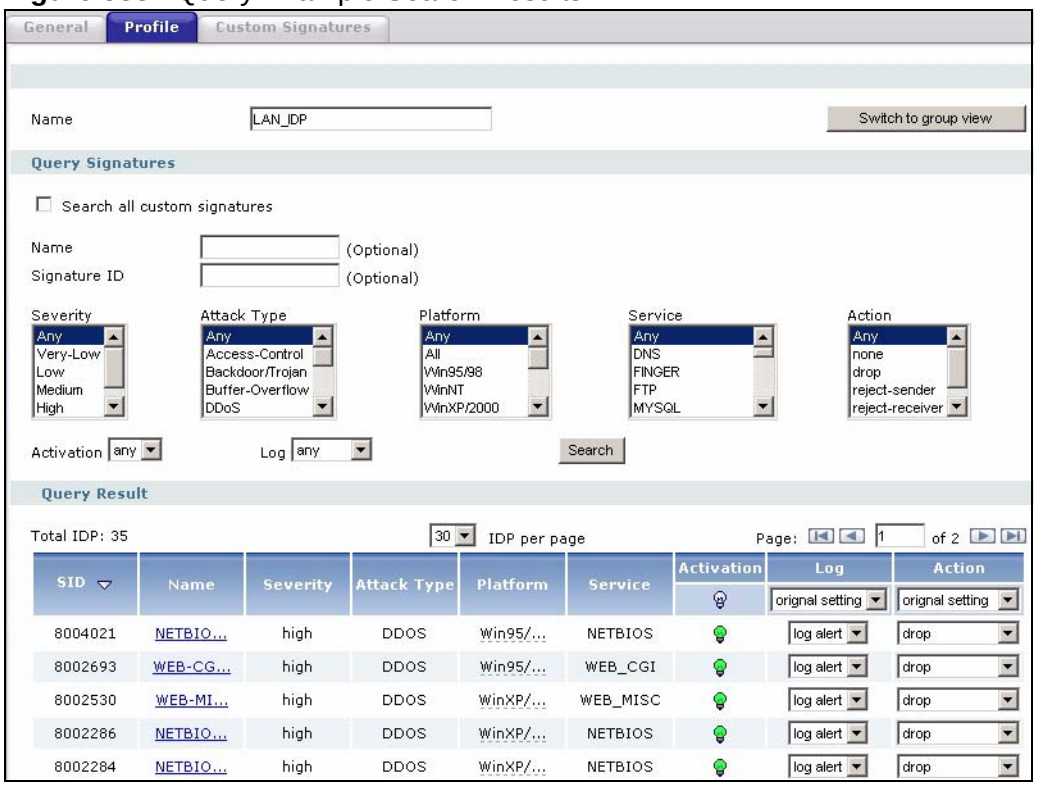



**Figure 388** Query Example Search Results




# 31.7 Introducing IDP Custom Signatures

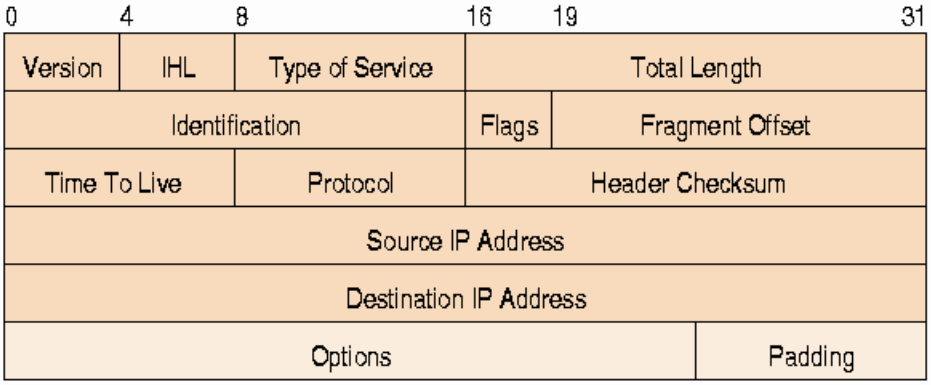
Create custom signatures for new attacks or attacks peculiar to your network. Custom signatures can also be saved to/from your computer so as to share with others.

You need some knowledge of packet headers and attack types to create your own custom signatures.

## 31.7.1 IP Packet Header

These are the fields in an Internet Protocol (IP) version 4 packet header.

**Figure 389** IP v4 Packet Headers




The header fields are discussed below:

**Table 167** IP v4 Packet Headers

| HEADER | DESCRIPTION |
|---|---|
| Version | The value 4 indicates IP version 4. |
| IHL | IP Header Length is the number of 32 bit words forming the total length of the header (usually five). |
| Type of Service | The Type of Service, (also known as Differentiated Services Code Point (DSCP)) is usually set to 0, but may indicate particular quality of service needs from the network. |
| Total Length | This is the size of the datagram in bytes. It is the combined length of the header and the data. |
| Identification | This is a 16-bit number, which together with the source address, uniquely identifies this packet. It is used during reassembly of fragmented datagrams. |
| Flags | Flags are used to control whether routers are allowed to fragment a packet and to indicate the parts of a packet to the receiver. |
| Fragment Offset | This is a byte count from the start of the original sent packet. |
| Time To Live | This is a counter that decrements every time it passes through a router. When it reaches zero, the datagram is discarded. It is used to prevent accidental routing loops. |
| Protocol | The protocol indicates the type of transport packet being carried, for example, 1 = ICMP; 2= IGMP; 6 = TCP; 17= UDP. |

**Table 167** IP v4 Packet Headers (continued)

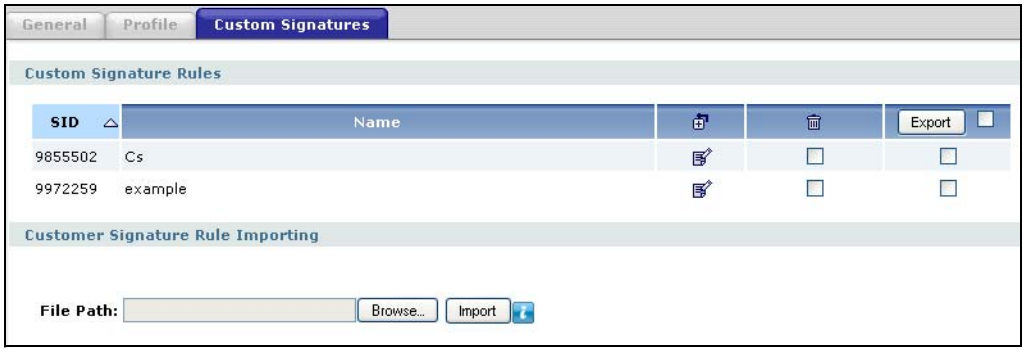
| HEADER | DESCRIPTION |
|---|---|
| Header Checksum | This is used to detect processing errors introduced into the packet inside a router or bridge where the packet is not protected by a link layer cyclic redundancy check. Packets with an invalid checksum are discarded by all nodes in an IP network. |
| Source IP Address | This is the IP address of the original sender of the packet. |
| Destination IP Address | This is the IP address of the final destination of the packet. |
| Options | IP options is a variable-length list of IP options for a datagram that define IP **Security Option, IP Stream Identifier**, (security and handling restrictions for the military), **Record Route** (have each router record its IP address), **Loose Source Routing** (specifies a list of IP addresses that must be traversed by the datagram), **Strict Source Routing** (specifies a list of IP addresses that must ONLY be traversed by the datagram), **Timestamp** (have each router record its IP address and time), **End of IP List** and **No IP Options**. |
| Padding | Padding is used as a filler to ensure that the IP packet is a multiple of 32 bits. |

# 31.8 Configuring Custom Signatures

Select **Anti-X > IDP > Custom Signature**s. The first screen shows a summary of all custom signatures created. Click the **SID** or **Name** heading to sort. Click the **Add** icon to create a new signature or click the **Edit** icon to edit an existing signature. You can also delete custom signatures here or save them to your computer.

Note: The ZyWALL checks all signatures and continues searching even after a match is found. If two or more rules have conflicting actions for the same packet, then the ZyWALL applies the more restrictive action (**reject-both, reject-receiver or reject-sender, drop, none** in this order). If a packet matches a rule for **reject-receiver** and it also matches a rule for **reject-sender**, then the ZyWALL will **reject-both**.

**Figure 390** Anti-X > IDP > Custom Signatures




The following table describes the fields in this screen.

**Table 168** Anti-X > IDP > Custom Signatures

| LABEL | DESCRIPTION |
|---|---|
| Custom Signature Rules | Use this part of the screen to create, edit, delete or export (save to your computer) custom signatures. |
| SID | SID is the signature ID that uniquely identifies a signature. Click the SID header to sort signatures in ascending or descending order. It is automatically created when you click the **Add** icon to create a new signature. You can edit the ID, but it cannot already exist and it must be in the 9000000 to 9999999 range. |
| Name | This is the name of your custom signature. Duplicate names can exist, but it is advisable to use unique signature names that give some hint as to intent of the signature and the type of attack it is supposed to prevent. |
| Add/Edit | Click the **Add** icon to create a new signature or click the **Edit** icon to edit an existing signature. |
| Delete | Use this column to delete signatures. Select (or clear) the check boxes next to individual signatures within the column. When you are certain that you have only selected signatures that you want to remove, click the **Delete** icon. Click **OK** in the confirm delete signature dialog box to delete the selected signature(s). |
| Export | Use this column to save signatures to your computer. Select (or clear) the check box in the header column to select (or clear) all check boxes in that column. You can also select (or clear) individual signatures within the column. When you are certain that you have only selected signatures that you want to save, click **Export**. Click **Save** in the file download dialog box and then select a location and name for the file.<br><br>Custom signatures must end with the 'rules' file name extension, for example, MySig.rules. |

**Table 168** Anti-X > IDP > Custom Signatures (continued)

| LABEL | DESCRIPTION |
|---|---|
| Customer Signature Rule Importing | Use this part of the screen to import custom signatures (previously saved to your computer) to the ZyWALL.<br><br>Note: The name of the complete custom signature file on the ZyWALL is 'custom.rules'. If you import a file named 'custom.rules', then all custom signatures on the ZyWALL are overwritten with the new file. If this is not your intention, make sure that the files you import are not named 'custom.rules'. |
| File Path | Type the file path and name of the custom signature file you want to import in the text box (or click **Browse** to find it on your computer) and then click **Import** to transfer the file to the ZyWALL.<br><br>New signatures then display in the ZyWALL **IDP > Custom Signatures** screen. |

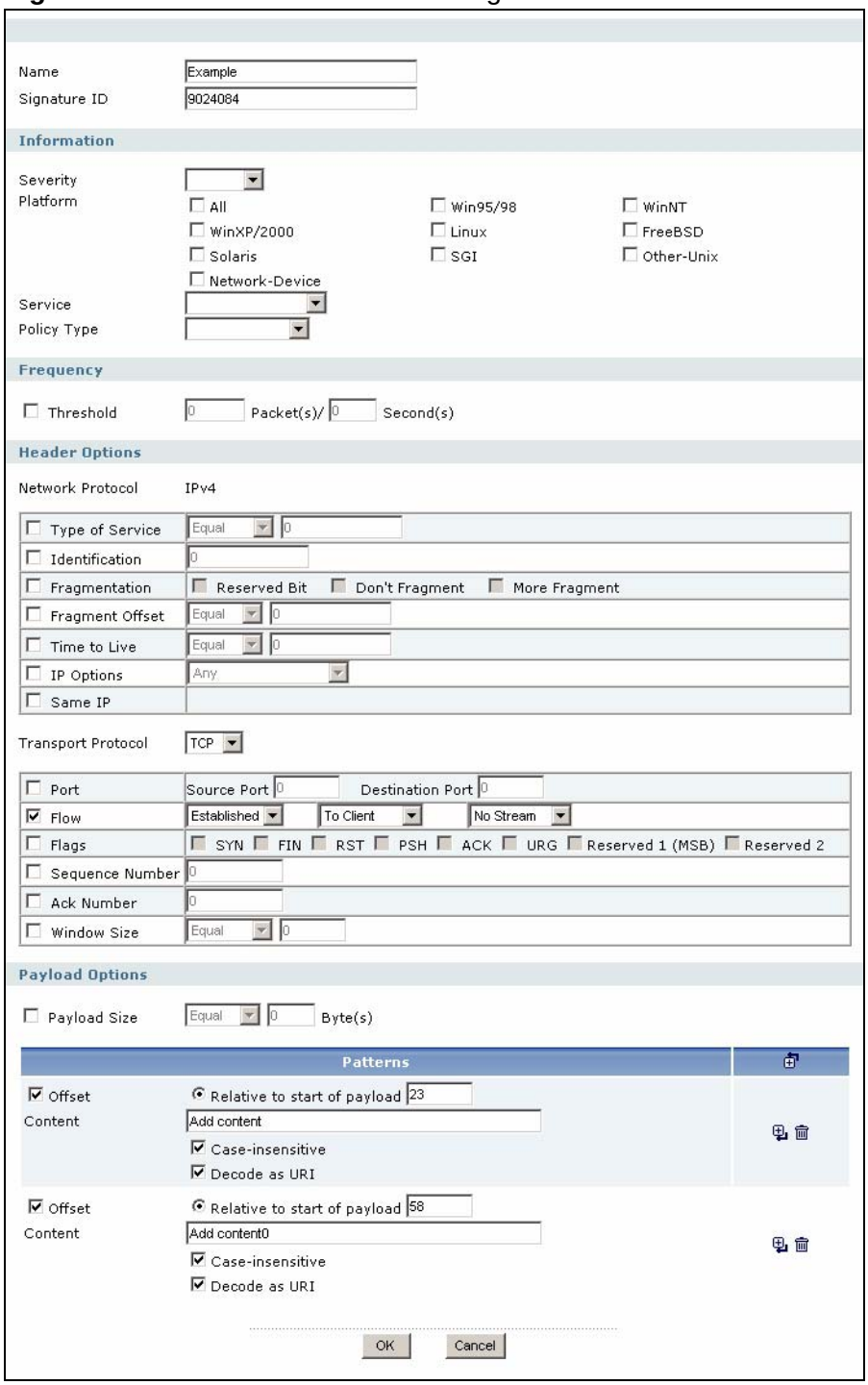
## 31.8.1 Creating or Editing a Custom Signature

Click the **Add** icon to create a new signature or click the **Edit** icon to edit an existing signature in the screen as shown in Figure 390 on page 541.

A packet must match all items you configure in this screen before it matches the signature. The more specific your signature (including packet contents), then the fewer false positives the signature will trigger.

Try to write signatures that target a vulnerability, for example a certain type of traffic on certain operating systems, instead of a specific exploit.

**Figure 391** Anti-X > IDP > Custom Signatures > Add/Edit



The following table describes the fields in this screen.

**Table 169** Anti-X > IDP > Custom Signatures > Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| Name | Type the name of your custom signature. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive.<br><br>Duplicate names can exist but it is advisable to use unique signature names that give some hint as to intent of the signature and the type of attack it is supposed to prevent. Refer to (but do not copy) the packet inspection signature names for hints on creating a naming convention. |
| Signature ID | A signature ID is automatically created when you click the **Add** icon to create a new signature. You can edit the ID to create a new one (in the 9000000 to 9999999 range), but you cannot use one that already exists. You may want to do that if you want to order custom signatures by SID. |
| Information | Use the following fields to set general information about the signature as denoted below. |
| Severity | The severity level denotes how serious the intrusion is. Categorize the seriousness of the intrusion here. See Table 163 on page 531 as a reference. |
| Platform | Some intrusions target specific operating systems only. Select the operating systems that the intrusion targets, that is, the operating systems you want to protect from this intrusion. SGI refers to Silicon Graphics Incorporated, who manufactures multi-user Unix workstations that run the IRIX operating system (SGI's version of UNIX). A router is an example of a network device. |
| Service | Select the IDP service group that the intrusion exploits or targets. See Table 165 on page 534 for a list of IDP service groups. The custom signature then appears in that group in the **IDP > Profile > Group View** screen. |
| Policy Type | Categorize the type of intrusion here. See Table 164 on page 533 as a reference. |
| Frequency | Recurring packets of the same type may indicate an attack. Use the following field to indicate how many packets per how many seconds constitute an intrusion |
| Threshold | Select **Threshold** and then type how many packets (that meet the criteria in this signature) per how many seconds constitute an intrusion. |
| Header Options | |
| Network Protocol | Configure signatures for IP version 4. |
| Type Of Service | Type of service in an IP header is used to specify levels of speed and/or reliability. Some intrusions use an invalid **Type Of Service** number. Select the check box, then select **Equal** or **Not-Equal** and then type in a number. |
| Identification | The identification field in a datagram uniquely identifies the datagram. If a datagram is fragmented, it contains a value that identifies the datagram to which the fragment belongs. Some intrusions use an invalid **Identification** number. Select the check box and then type in the invalid number that the intrusion uses. |

**Table 169** Anti-X > IDP > Custom Signatures > Add/Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Fragmentation | A fragmentation flag identifies whether the IP datagram should be fragmented, not fragmented or is a reserved bit. Some intrusions can be identified by this flag. Select the check box and then select the flag that the intrusion uses. |
| Fragmentation Offset | When an IP datagram is fragmented, it is reassembled at the final destination. The fragmentation offset identifies where the fragment belongs in a set of fragments. Some intrusions use an invalid **Fragmentation Offset** number. Select the check box, select **Equal**, **Smaller** or **Greater** and then type in a number |
| Time to Live | Time to Live is a counter that decrements every time it passes through a router. When it reaches zero, the datagram is discarded. Usually it's used to set an upper limit on the number of routers a datagram can pass through. Some intrusions can be identified by the number in this field. Select the check box, select **Equal**, **Smaller** or **Greater** and then type in a number. |
| IP Options | IP options is a variable-length list of IP options for a datagram that define IP **Security Option, IP Stream Identifier**, (security and handling restrictions for the military), **Record Route** (have each router record its IP address), **Loose Source Routing** (specifies a list of IP addresses that must be traversed by the datagram), **Strict Source Routing** (specifies a list of IP addresses that must ONLY be traversed by the datagram), **Timestamp** (have each router record its IP address and time), **End of IP List** and **No IP Options**. **IP Options** can help identify some intrusions. Select the check box, then select an item from the list box that the intrusion uses |
| Same IP | Select the check box for the signature to check for packets that have the same source and destination IP addresses. |
| Transport Protocol | The following fields vary depending on whether you choose **TCP**, **UDP** or **ICMP**. |
| Transport Protocol: TCP | |
| Port | Select the check box and then enter the source and destination TCP port numbers that will trigger this signature. |

**Table 169** Anti-X > IDP > Custom Signatures > Add/Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Flow | If selected, the signature only applies to certain directions of the traffic flow and only to clients or servers. Select **Flow** and then select the identifying options.<br>**Established**: The signature only checks for established TCP connections<br>**Stateless**: The signature is triggered regardless of the state of the stream processor (this is useful for packets that are designed to cause devices to crash)<br>**To Client**: The signature only checks for server responses from A to B.<br>**To Server**: The signature only checks for client requests from B to A.<br>**From Client**:.The signature only checks for client requests from B to A.<br>**From Servers**: The signature only checks for server responses from A to B.<br>**No Stream**: The signature does not check rebuilt stream packets.<br>**Only Stream**: The signature only checks rebuilt stream packets. |
| Flags | Select what TCP flag bits the signature should check. |
| Sequence Number | Use this field to check for a specific TCP sequence number. |
| Ack Number | Use this field to check for a specific TCP acknowledgement number. |
| Window Size | Use this field to check for a specific TCP window size. |
| Transport Protocol: UDP | |
| Port | Select the check box and then enter the source and destination UDP port numbers that will trigger this signature. |
| Transport Protocol: ICMP | |
| Type | Use this field to check for a specific ICMP type value. |
| Code | Use this field to check for a specific ICMP code value. |
| ID | Use this field to check for a specific ICMP ID value. This is useful for covert channel programs that use static ICMP fields when they communicate. |
| Sequence Number | Use this field to check for a specific ICMP sequence number. This is useful for covert channel programs that use static ICMP fields when they communicate. |
| Payload Options | The longer a payload option is, the more exact the match, the faster the signature processing. Therefore, if possible, it is recommended to have at least one payload option in your signature. |

**Table 169** Anti-X > IDP > Custom Signatures > Add/Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Payload Size | This field may be used to check for abnormally sized packets or for detecting buffer overflows.<br><br>Select the check box, then select **Equal**, **Smaller** or **Greater** and then type the payload size.<br><br>Stream rebuilt packets are not checked regardless of the size of the payload. |
| Offset | This field specifies where to start searching for a pattern within a packet. For example, an offset of 5 would start looking for the specified pattern after the first five bytes of the payload. |
| Content | Type the content that the signature should search for in the packet payload. Hexadecimal code entered between pipes is converted to ASCII. For example, you could represent the ampersand as either & or \|26\| (26 is the hexadecimal code for the ampersand). |
| Case-insensitive | Select this check box if content casing does NOT matter. |
| Decode as URI | A Uniform Resource Identifier (URI) is a string of characters for identifying an abstract or physical resource (RFC 2396). A resource can be anything that has identity, for example, an electronic document, an image, a service (“today's weather report for Taiwan”), a collection of other resources. An identifier is an object that can act as a reference to something that has identity. Example URIs are:<br><br>ftp://ftp.is.co.za/rfc/rfc1808.txt; ftp scheme for File Transfer Protocol services<br><br>http://www.math.uio.no/faq/compression-faq/part1.html; http scheme for Hypertext Transfer Protocol services<br><br>mailto:mduerst@ifi.unizh.ch; mailto scheme for electronic mail addresses<br><br>telnet://melvyl.ucop.edu/; telnet scheme for interactive services via the TELNET Protocol<br><br>Select this check box for the signature to search for normalized URI fields. This means that if you are writing signatures that includes normalized content, such as %2 for directory traversals, these signatures will not be triggered because the content is normalized out of the URI buffer.<br><br>For example, the URI:<br><br>/scripts/..%c0%af../winnt/system32/cmd.exe?/c+ver<br><br>will get normalized into:<br><br>/winnt/system32/cmd.exe?/c+ver |
| OK | Click this button to save your changes to the ZyWALL and return to the summary screen. |
| Cancel | Click this button to return to the summary screen without saving any changes. |

## 31.8.2 Custom Signature Example

Before creating a custom signature, you must first clearly understand the vulnerability.

### 31.8.2.1 Understand the Vulnerability

Check the ZyWALL logs when the attack occurs. Use web sites such as Google or Security Focus to get as much information about the attack as you can. The more specific your signature, the less chance it will cause false positives.

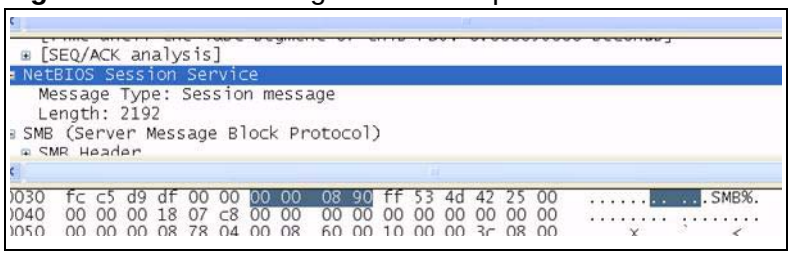
As an example, say you want to create a signature for the 'Microsoft Windows Plug-and-Play Service Remote Overflow (MS-05-39)' attack. Search the Security Focus web site and you will find it uses the NetBIOS service in established TCP connections to a server using port 445.

### 31.8.2.2 Analyze Packets

Then use a packet sniffer such as TCPdump or Ethereal to investigate some more.

From the NetBIOS header you see that the first byte '00' defines the message type. The next three bytes represent the length of data, so you can ignore it. Therefore enter **|00|** as the first pattern.

**Figure 392** Custom Signature Example Pattern 1



Next, check the content of the SMB header. Add **|FF|SMB%** and ‘TransactionNmPipe’ to the signature as the next patterns.

**Figure 393** Custom Signature Example Pattern 2

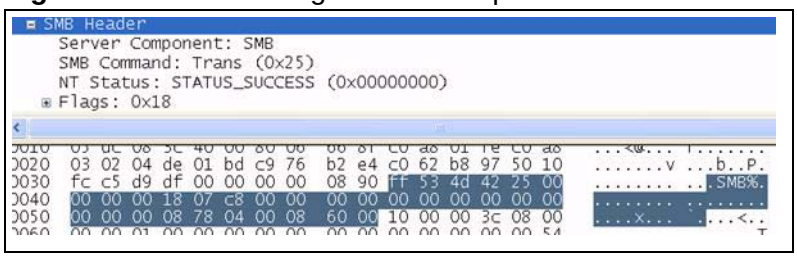
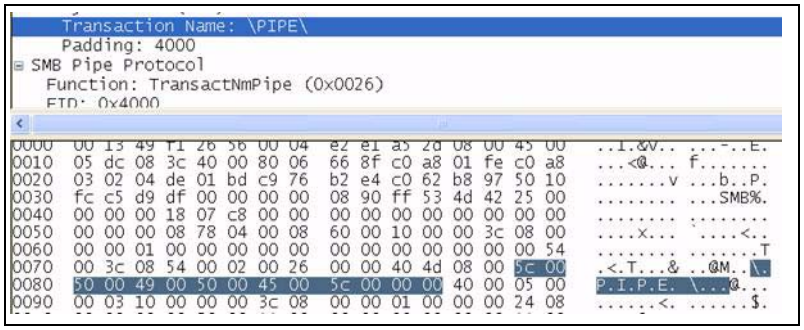


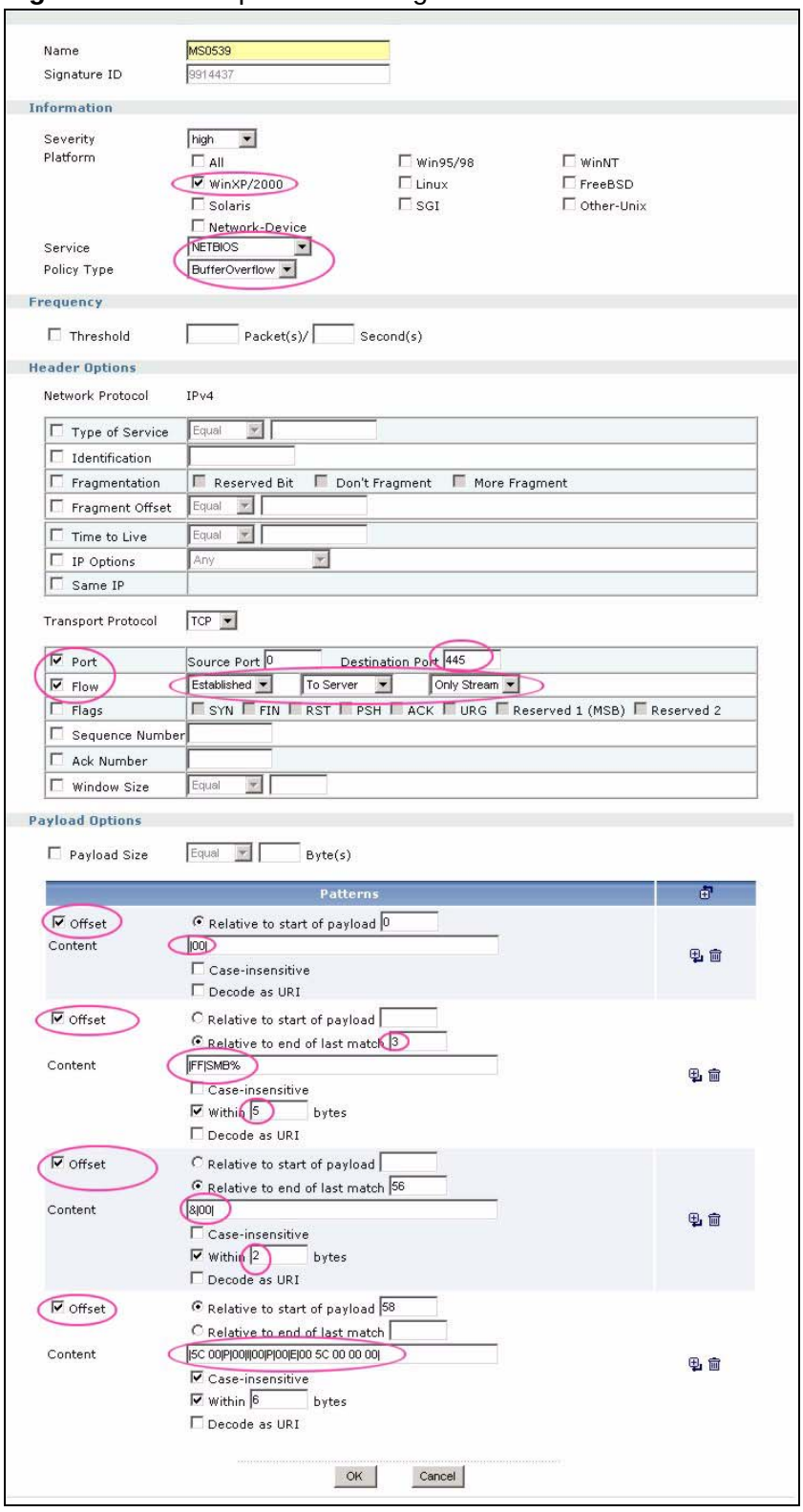

**Figure 394** Custom Signature Example Patterns 3 and 4




The final custom signature should look like as shown in the following figure.

If the attack occurs, check the logs for a log of your custom signature. This indicates the signature works correctly.

**Figure 395** Example Custom Signature

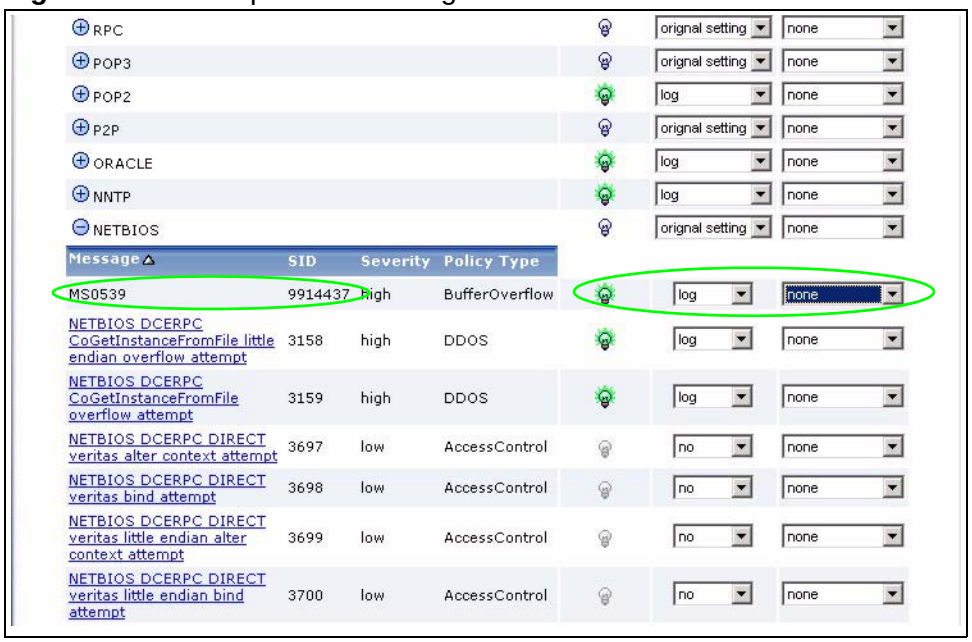


## 31.8.3 Applying Custom Signatures

After you create your custom signature, it becomes available in the IDP service group category in the **IDP > Profile > Packet Inspection** screen. Custom signatures have an SID from 9000000 to 9999999.

You can activate the signature, configure what action to take when a packet matches it and if it should generate a log or alert in a profile. Then bind the profile to a zone.

**Figure 396** Example: Custom Signature in IDP Profile



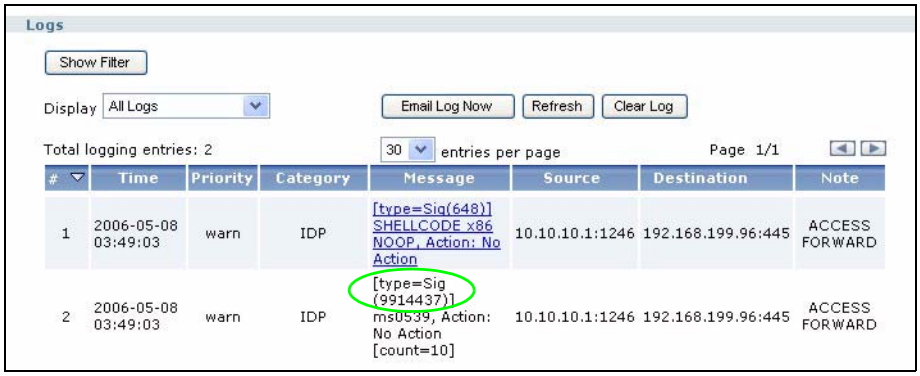

## 31.8.4 Verifying Custom Signatures

You should configure the signature to create a log when an 'attack packet' matches the signature. (You may also want to configure an alert if the attack is more serious and needs more immediate attention.) After you apply the signature to a zone, you can see if it works by checking the logs (**Maintenance > Logs > View Log**).

All IDP signatures come under the **IDP** category. The **Priority** column shows **warn** for signatures that are configured to generate a log only. It shows **critical** for signatures that are configured to generate a log and alert. **count** is the number of attacks that occurred at that time. The **Note** column displays **ACCESS FORWARD** when no action is configured for the signature. It displays **ACCESS**

**DENIED** if you configure the signature action to drop the packet. The destination port is the service port (NetBIOS in this case) that the attack tries to exploit.

**Figure 397** Custom Signature Log




# 31.9 IDP Technical Reference

This section contains some background information on IDP.

### Host Intrusions

The goal of host-based intrusions is to infiltrate files on an individual computer or server in with the goal of accessing confidential information or destroying information on a computer.

You must install a host IDP directly on the system being protected. It works closely with the operating system, monitoring and intercepting system calls to the kernel or APIs in order to prevent attacks as well as log them.

Disadvantages of host IDPs are that you have to install them on each device (that you want to protect) in your network and due to the necessarily tight integration with the host operating system, future operating system upgrades could cause problems.

### Network Intrusions

Network-based intrusions have the goal of bringing down a network or networks by attacking computer(s), switch(es), router(s) or modem(s). If a LAN switch is compromised for example, then the whole LAN is compromised. Host-based intrusions may be used to cause network-based intrusions when the goal of the host virus is to propagate attacks on the network, or attack computer/server operating system vulnerabilities with the goal of bringing down the computer/server. Typical “network-based intrusions” are SQL slammer, Blaster, Nimda MyDoom etc.

## Snort Signatures

You may want to refer to open source Snort signatures when creating custom ZyWALL ones. Most Snort rules are written in a single line. Snort rules are divided into two logical sections, the rule header and the rule options as shown in the following example:

```
alert tcp any any -> 192.168.1.0/24 111 (content:"|00 01 a5|";
msg:"mountd access";)
```

The text up to the first parenthesis is the rule header and the section enclosed in parenthesis contains the rule options. The words before the colons in the rule options section are the option keywords.

The rule header contains the rule's:

- Action
- Protocol
- Source and destination IP addresses and netmasks
- Source and destination ports information.

The rule option section contains alert messages and information on which parts of the packet should be inspected to determine if the rule action should be taken.

These are some equivalent Snort terms in the ZyWALL.

**Table 170** ZyWALL - Snort Equivalent Terms

| ZYWALL TERM | SNORT EQUIVALENT TERM |
|---|---|
| Type Of Service | tos |
| Identification | id |
| Fragmentation | fragbits |
| Fragmentation Offset | fragoffset |
| Time to Live | ttl |
| IP Options | ipopts |
| Same IP | sameip |
| Transport Protocol | |
| Transport Protocol: TCP | |
| Port | (In Snort rule header) |
| Flow | flow |
| Flags | flags |
| Sequence Number | seq |
| Ack Number | ack |
| Window Size | window |
| Transport Protocol: UDP | (In Snort rule header) |

**Table 170** ZyWALL - Snort Equivalent Terms (continued)

| ZYWALL TERM | SNORT EQUIVALENT TERM |
|---|---|
| Port | (In Snort rule header) |
| Transport Protocol: ICMP | |
| Type | itype |
| Code | icode |
| ID | icmp_id |
| Sequence Number | icmp_seq |
| Payload Options | (Snort rule options) |
| Payload Size | dsize |
| Offset (relative to start of payload) | offset |
| Relative to end of last match | distance |
| Content | content |
| Case-insensitive | nocase |
| Decode as URI | uricontent |

Note: Not all Snort functionality is supported in the ZyWALL.

# 32 ADP

## 32.1 Overview

This chapter introduces ADP (Anomaly Detection and Prevention), anomaly profiles and applying an ADP profile to a traffic direction. ADP protects against anomalies based on violations of protocol standards (RFCs – Requests for Comments) and abnormal flows such as port scans.

### 32.1.1 ADP and IDP Comparison

1 ADP anomaly detection is in general effective against abnormal behavior while IDP packet inspection signatures are in general effective for known attacks (see Chapter 31 on page 521 for information on packet inspection).

2 ADP traffic and anomaly rules are updated when you upload new firmware. This is different from the IDP packet inspection signatures and the system protect signatures you download from myZyXEL.com.

### 32.1.2 What You Can Do Using the ADP Screens

- Use **Anti-X > ADP > General** (Section 32.2 on page 557) to turn anomaly detection on or off and apply anomaly profiles to traffic directions.
- Use **Anti-X > ADP > Profile** (Section 32.3 on page 559) to add a new profile, edit an existing profile or delete an existing profile.

### 32.1.3 What You Need To Know About ADP

#### Traffic Anomalies

Traffic anomaly rules look for abnormal behavior or events such as port scanning, sweeping or network flooding. It operates at OSI layer-2 and layer-3. Traffic anomaly rules may be updated when you upload new firmware.

### Protocol Anomalies

Protocol anomalies are packets that do not comply with the relevant RFC (Request For Comments). Protocol anomaly detection includes HTTP Inspection, TCP Decoder, UDP Decoder and ICMP Decoder. Protocol anomaly rules may be updated when you upload new firmware.

### ADP Profile

An ADP profile is a set of traffic anomaly rules and protocol anomaly rules that you can activate as a set and configure common log and action settings. You can apply ADP profiles to traffic flowing from one zone to another.

### Base ADP Profiles

Base ADP profiles are templates that you use to create new ADP profiles.The ZyWALL comes with several base profiles. See Table 173 on page 560 for details on ADP base profiles.

### ADP Policy

An ADP policy refers to application of an ADP profile to a traffic flow.

### Finding Out More

- See Section 5.4.16 on page 93 for ADP prerequisites
- See Chapter 31 on page 521 for IDP information.
- See Section 31.1.2 on page 521 for IDP-related term definitions.
- See Section 32.4 on page 566 for background information on these screens.

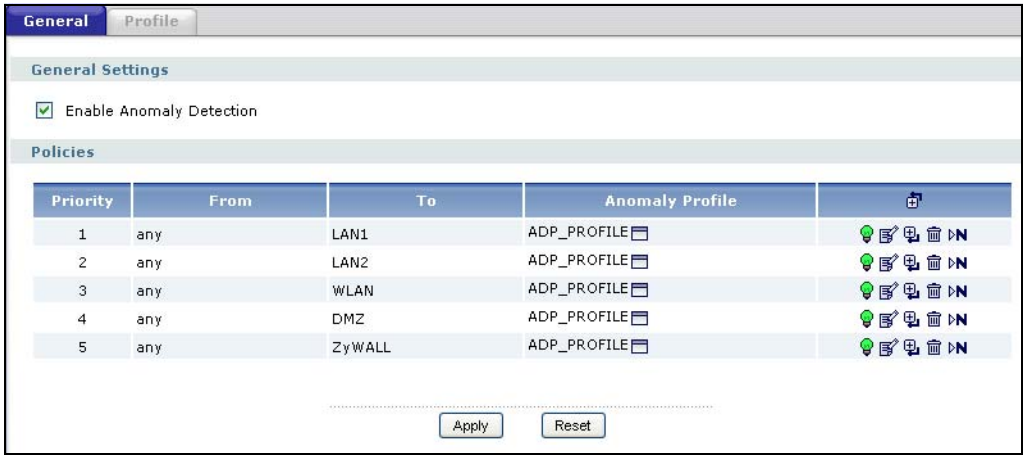
## 32.1.4 Before You Begin

Configure the ZyWALL's zones - see Chapter 14 on page 297 for more information.

# 32.2 The ADP General Screen

Click **Anti-X > ADP > General**. Use this screen to turn anomaly detection on or off and apply anomaly profiles to traffic directions.

**Figure 398** Anti-X > ADP > General




The following table describes the screens in this screen.

**Table 171** Anti-X > ADP > General

| LABEL | DESCRIPTION |
|---|---|
| General Settings | |
| Enable Anomaly Detection | Select this check box to enable traffic anomaly and protocol anomaly detection. |
| Policies | Use this list to specify which anomaly profile the ZyWALL uses for traffic flowing in a specific direction. |
| Priority | This is the rank in the list of anomaly profile policies. The list is applied in order of priority. |
| From, To | This is the direction of travel of packets to which an anomaly profile is bound.<br><br>Note: Depending on your network topology and traffic load, applying every packet direction to an anomaly profile may affect the ZyWALL's performance. |
| Anomaly Profile | An anomaly profile is a set of anomaly rules with configured activation, log and action settings. This field shows which anomaly profile is bound to which traffic direction. |

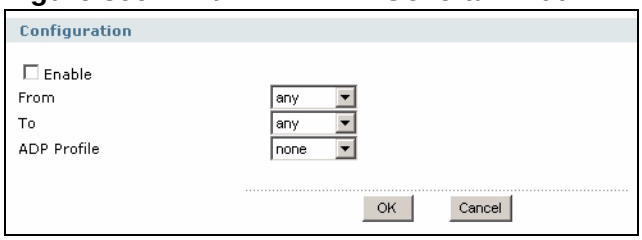
**Table 171** Anti-X > ADP > General (continued)

| LABEL | DESCRIPTION |
|---|---|
| Add icon | Click the **Add** icon in the heading row to add a new first entry.<br>The **Active** icon displays whether the entry is enabled or not. Click it to activate or deactivate the entry. Make sure you click **Apply** to save and apply the change.<br>Click the **Edit** icon to go to the screen where you can edit the entry.<br>Click the **Add** icon in an entry to add an entry below the current entry.<br>Click the **Remove** icon to delete an existing entry from the ZyWALL. A window displays asking you to confirm that you want to delete the entry. Note that subsequent entries move up by one when you take this action.<br>In a numbered list, click the **Move to N** icon to display a field to type an index number for where you want to put that entry and press [ENTER] to move the entry to the number that you typed. For example, if you type 6, the entry you are moving becomes number 6 and the previous entry 6 (if there is one) gets pushed up (or down) one.<br>The ordering of your entries is important as they are applied in order of their numbering. |
| Apply | Click **Apply** to save your changes. |
| Reset | Click **Reset** to start configuring this screen again. |

## 32.2.1 Configuring ADP Policies

Click **Anti-X > ADP > General** and then an **Add** or **Edit** icon to display the following screen. Use this screen to apply an ADP profile to a traffic direction.

**Figure 399** Anti-X > ADP > General > Add



The following table describes the screens in this screen.

**Table 172** Anti-X > ADP > General > Add

| LABEL | DESCRIPTION |
|---|---|
| Enable | Select this check box to turn on this anomaly profile to traffic direction policy. |
| From | Traffic direction is defined by the zone the traffic is coming from and the zone the traffic is going to.<br>Use the **From** field to specify the zone from which the traffic is coming.<br>Select **ZyWALL** to specify traffic coming from the ZyWALL itself. |
| To | Use the **To** field to specify the zone to which the traffic is going.<br>Select **ZyWALL** to specify traffic destined for the ZyWALL itself.<br>**From LAN1 To LAN1** means packets traveling from a computer on one LAN1 subnet to a computer on another LAN1 subnet via the ZyWALL's LAN1 zone interfaces. The ZyWALL does not check packets traveling from a LAN1 computer to another LAN1 computer on the same subnet.<br>**From WAN To WAN** means packets that come in from the WAN zone and the ZyWALL routes back out through the WAN zone. |
| ADP Profile | An ADP profile is a set of ADP rules with configured activation, log and action settings. Select an ADP profile to apply to the entry's traffic direction. Configure the ADP profiles in the ADP profile screens. |
| OK | Click **OK** to save your changes. |
| Cancel | Click **Cancel** to exit this screen without saving your changes. |

# 32.3 The Profile Summary Screen

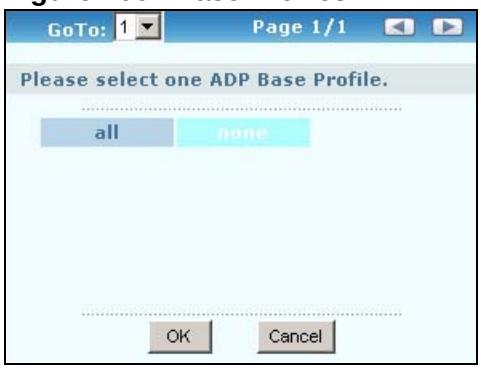
Use this screen to:

- Create a new profile using an existing base profile
- Edit an existing profile
- Delete an existing profile

## 32.3.1 Base Profiles

The ZyWALL comes with base profiles. You use base profiles to create new profiles.

**Figure 400** Base Profiles




These are the default base profiles at the time of writing.

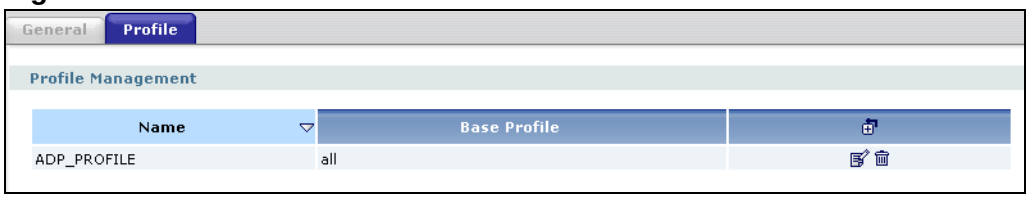
**Table 173** Base Profiles

| BASE PROFILE | DESCRIPTION |
|---|---|
| all | All traffic anomaly and protocol anomaly rules are enabled. Rules with a high or severe severity level (greater than three) generate log alerts and cause packets that trigger them to be dropped. Rules with a very low, low or medium severity level (less than or equal to three) generate logs (not log alerts) and no action is taken on packets that trigger them. |
| none | All traffic anomaly and protocol anomaly rules are disabled. No logs are generated nor actions are taken. |
| OK | Click **OK** to save your changes. |
| Cancel | Click **Cancel** to exit this screen without saving your changes. |

## 32.3.2 Configuring The ADP Profile Summary Screen

Select **Anti-X > ADP > Profile**.

**Figure 401** Anti-X > ADP > Profile



The following table describes the fields in this screen.

**Table 174** Anti-X > ADP > Profile

| LABEL | DESCRIPTION |
|---|---|
| Name | This is the name of the profile you created. |
| Base Profile | This is the base profile from which the profile was created. |
| Add icon | Click the **Add** icon in the column header to create a new profile. A pop-up screen displays requiring you to choose a base profile from which to create the new profile.<br>Click an **Edit** icon to edit an existing profile.<br>Click a **Remove** icon to delete an existing profile. |

## 32.3.3 Creating New ADP Profiles

You may want to create a new profile if not all rules in a base profile are applicable to your network. In this case you should disable non-applicable rules so as to improve ZyWALL ADP processing efficiency.

You may also find that certain rules are triggering too many false positives or false negatives. A false positive is when valid traffic is flagged as an attack. A false negative is when invalid traffic is wrongly allowed to pass through the ZyWALL. As each network is different, false positives and false negatives are common on initial ADP deployment.

You could create a new 'monitor profile' that creates logs but all actions are disabled. Observe the logs over time and try to eliminate the causes of the false alarms. When you're satisfied that they have been reduced to an acceptable level, you could then create an 'inline profile' whereby you configure appropriate actions to be taken when a packet matches a rule.

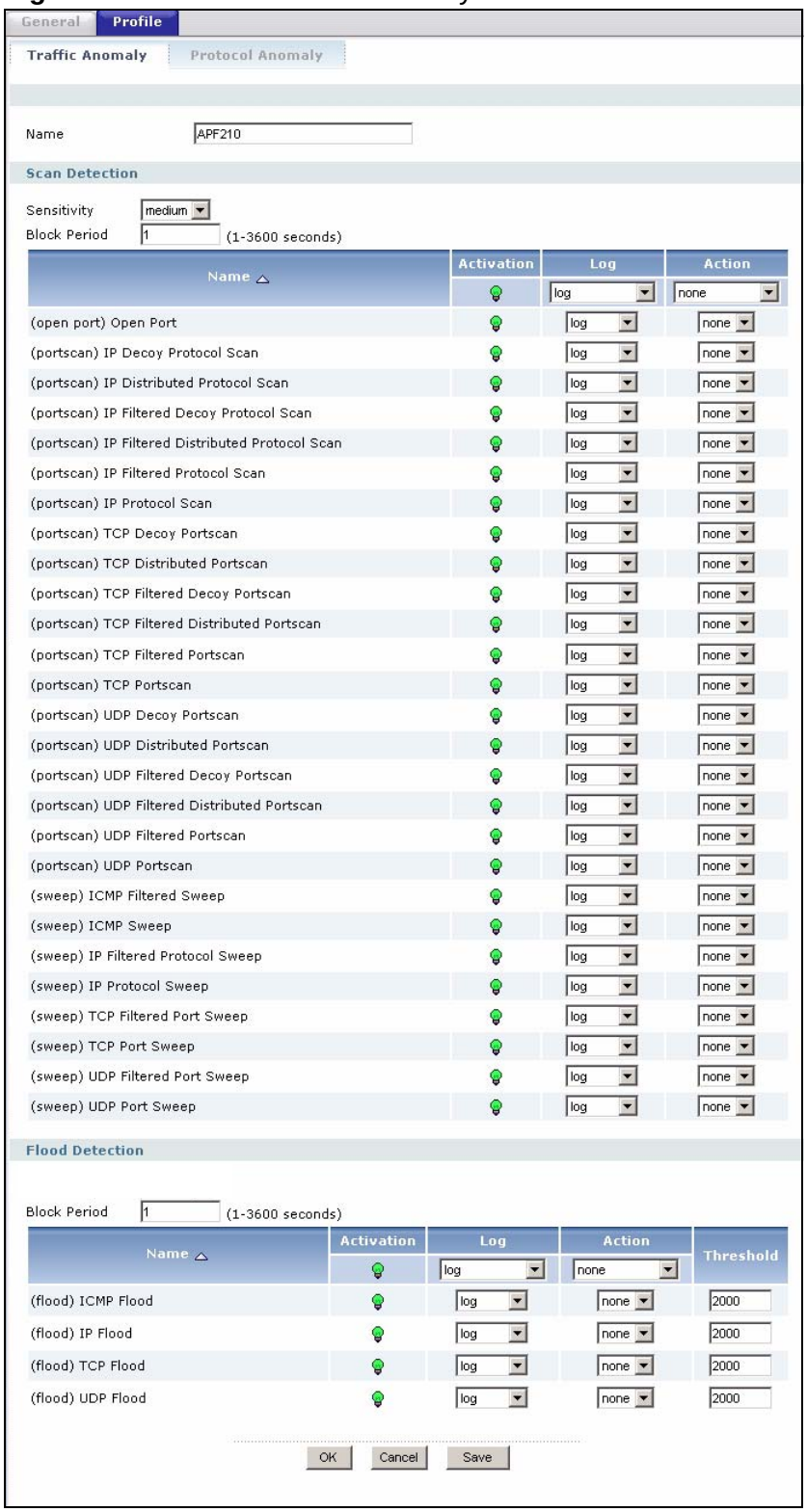
ADP profiles consist of traffic anomaly profiles and protocol anomaly profiles. To create a new profile, select a base profile (see Table 173 on page 560) and then click **OK** to go to the profile details screen. Type a new profile name, enable or disable individual rules and then edit the default log options and actions.

## 32.3.4 Traffic Anomaly Profiles

The traffic anomaly screen is the second screen in an ADP profile. Traffic anomaly detection looks for abnormal behavior such as scan or flooding attempts. In the **Anti-X > ADP > Profile** screen, click the **Edit** icon or click the **Add** icon and choose a base profile. If you made changes to other screens belonging to this

profile, make sure you have clicked **OK** or **Save** to save the changes before selecting the **Traffic Anomaly** tab.

**Figure 402** Profiles: Traffic Anomaly



The following table describes the fields in this screen.

**Table 175** ADP > Profile > Traffic Anomaly

| LABEL | DESCRIPTION |
|---|---|
| Name | This is the name of the ADP profile. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. These are valid, unique profile names:<br>MyProfile<br>mYProfile<br>Mymy12_3-4<br>These are invalid profile names:<br>1mYProfile<br>My Profile<br>MyProfile?<br>Whatalongprofilename123456789012 |
| Scan/Flood Detection | |
| Sensitivity | (Scan detection only.) Select a sensitivity level so as to reduce false positives in your network. If you choose low sensitivity, then scan thresholds and sample times are set low, so you will have fewer logs and false positives; however some traffic anomaly attacks may not be detected.<br>If you choose high sensitivity, then scan thresholds and sample times are set high, so most traffic anomaly attacks will be detected; however you will have more logs and false positives. |
| Block Period | Specify for how many seconds the ZyWALL blocks all packets from being sent to the victim (destination) of a detected anomaly attack. |
| Name | This is the name of the traffic anomaly rule. Click the **Name** column heading to sort in ascending or descending order according to the rule name. |
| Activation | Click the icon to enable or disable a rule or group of rules. |
| Log | Select whether to have the ZyWALL generate a log (**log**), log and alert (**log alert**) or neither (**no**) when traffic matches this anomaly rule. See Chapter 47 on page 793 for more on logs. |
| Action | Select what the ZyWALL should do when a packet matches a rule.<br>**none**: The ZyWALL takes no action when a packet matches the signature(s).<br>**block**: The ZyWALL silently drops packets that matches the rule. Neither sender nor receiver are notified. |
| Threshold | For flood detection you can set the number of detected flood packets per second that causes the ZyWALL to take the configured action. |
| OK | Click **OK** to save your settings to the ZyWALL, complete the profile and return to the profile summary page. |

**Table 175** ADP > Profile > Traffic Anomaly (continued)

| LABEL | DESCRIPTION |
|---|---|
| Cancel | Click **Cancel** to return to the profile summary page without saving any changes. |
| Save | Click **Save** to save the configuration to the ZyWALL but remain in the same page. You may then go to the another profile screen (tab) in order to complete the profile. Click **OK** in the final profile screen to complete the profile. |

## 32.3.5 Protocol Anomaly Profiles

Protocol anomaly is the third screen in an ADP profile. Protocol anomaly (PA) rules check for protocol compliance against the relevant RFC (Request for Comments).

Protocol anomaly detection includes HTTP Inspection, TCP Decoder, UDP Decoder, and ICMP Decoder where each category reflects the packet type inspected.

Protocol anomaly rules may be updated when you upload new firmware.

## 32.3.6 Protocol Anomaly Configuration

In the **Anti-X > ADP > Profile** screen, click the **Edit** icon or click the **Add** icon and choose a base profile, then select the **Protocol Anomaly** tab. If you made changes to other screens belonging to this profile, make sure you have clicked **OK** or **Save** to save the changes before selecting the **Protocol Anomaly** tab.

**Figure 403** Profiles: Protocol Anomaly

The following table describes the fields in this screen.

**Table 176** ADP > Profile > Protocol Anomaly

| LABEL | DESCRIPTION |
|---|---|
| Name | This is the name of the profile. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. These are valid, unique profile names:<br>MyProfile<br>mYProfile<br>Mymy12_3-4<br>These are invalid profile names:<br>1mYProfile<br>My Profile<br>MyProfile?<br>Whatalongprofilename123456789012 |
| HTTP Inspection/TCP Decoder/UDP Decoder/ICMP Decoder | |
| Name | This is the name of the protocol anomaly rule. Click the **Name** column heading to sort in ascending or descending order according to the protocol anomaly rule name. |
| Activation | Click the icon to enable or disable a rule or group of rules. |
| Log | Select whether to have the ZyWALL generate a log (**log**), log and alert (**log alert**) or neither (**no**) when traffic matches this anomaly rule. See Chapter 47 on page 793 for more on logs. |
| Action | Select what the ZyWALL should do when a packet matches a rule.<br>**none**: The ZyWALL takes no action when a packet matches the signature(s).<br>**block**: The ZyWALL silently drops packets that matches the rule. Neither sender nor receiver are notified. |
| OK | Click **OK** to save your settings to the ZyWALL, complete the profile and return to the profile summary page. |
| Cancel | Click **Cancel** to return to the profile summary page without saving any changes. |
| Save | Click **Save** to save the configuration to the ZyWALL but remain in the same page. You may then go to the another profile screen (tab) in order to complete the profile. Click **OK** in the final profile screen to complete the profile. |

# 32.4 ADP Technical Reference

This section is divided into traffic anomaly background information and protocol anomaly background information.

# Traffic Anomaly Background Information

The following sections may help you configure the traffic anomaly profile screen (Section 32.3.4 on page 561)

## Port Scanning

An attacker scans device(s) to determine what types of network protocols or services a device supports. One of the most common port scanning tools in use today is Nmap.

Many connection attempts to different ports (services) may indicate a port scan. These are some port scan types:

- TCP Portscan
- UDP Portscan
- IP Portscan

An IP port scan searches not only for TCP, UDP and ICMP protocols in use by the remote computer, but also additional IP protocols such as EGP (Exterior Gateway Protocol) or IGP (Interior Gateway Protocol). Determining these additional protocols can help reveal if the destination device is a workstation, a printer, or a router.

### Decoy Port Scans

Decoy port scans are scans where the attacker has spoofed the source address. These are some decoy scan types:

- TCP Decoy Portscan
- UDP Decoy Portscan
- IP Decoy Portscan

### Distributed Port Scans

Distributed port scans are many-to-one port scans. Distributed port scans occur when multiple hosts query one host for open services. This may be used to evade intrusion detection. These are distributed port scan types:

- TCP Distributed Portscan
- UDP Distributed Portscan
- IP Distributed Portscan

### Port Sweeps

Many different connection attempts to the same port (service) may indicate a port sweep, that is, they are one-to-many port scans. One host scans a single port on multiple hosts. This may occur when a new exploit comes out and the attacker is looking for a specific service. These are some port sweep types:

- TCP Portsweep
- UDP Portsweep
- IP Portsweep
- ICMP Portsweep

### Filtered Port Scans

A filtered port scan may indicate that there were no network errors (ICMP unreachables or TCP RSTs) or responses on closed ports have been suppressed. Active network devices, such as NAT routers, may trigger these alerts if they send out many connection attempts within a very small amount of time. These are some filtered port scan examples.

- TCP Filtered Portscan
- UDP Filtered Portscan
- IP Filtered Portscan
- TCP Filtered Decoy Portscan
- UDP Filtered Decoy Portscan
- IP Filtered Decoy Portscan
- TCP Filtered Portsweep
- UDP Filtered Portsweep
- IP Filtered Portsweep
- ICMP Filtered Portsweep
- TCP Filtered Distributed Portscan
- UDP Filtered Distributed Portscan
- IP Filtered Distributed Portscan

## Flood Detection

Flood attacks saturate a network with useless data, use up all available bandwidth, and therefore make communications in the network impossible.

### ICMP Flood Attack

An ICMP flood is broadcasting many pings or UDP packets so that so much data is sent to the system, that it slows it down or locks it up.

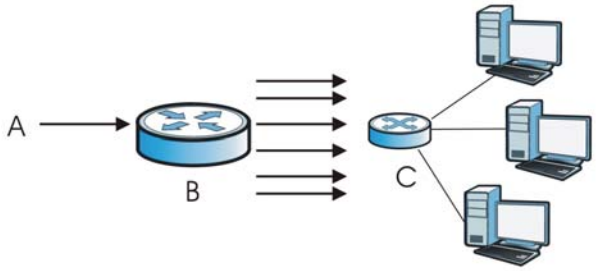
### Smurf

A smurf attacker (A) floods a router (B) with Internet Control Message Protocol (ICMP) echo request packets (pings) with the destination IP address of each packet as the broadcast address of the network. The router will broadcast the

ICMP echo request packet to all hosts on the network. If there are numerous hosts, this will create a large amount of ICMP echo request and response traffic.

If an attacker (A) spoofs the source IP address of the ICMP echo request packet, the resulting ICMP traffic will not only saturate the receiving network (B), but the network of the spoofed source IP address (C).

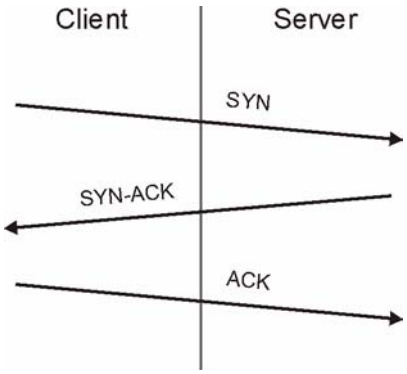
**Figure 404** Smurf Attack




## TCP SYN Flood Attack

Usually a client starts a session by sending a SYN (synchronize) packet to a server. The receiver returns an ACK (acknowledgment) packet and its own SYN, and then the initiator responds with an ACK (acknowledgment). After this handshake, a connection is established.

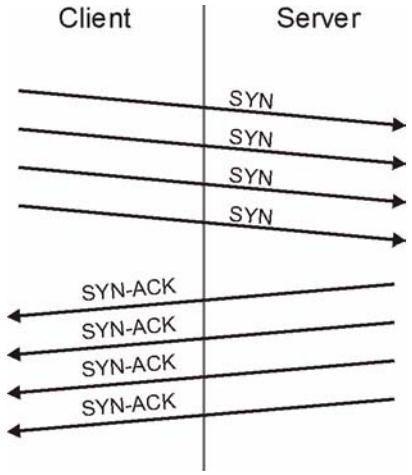
**Figure 405** TCP Three-Way Handshake




A SYN flood attack is when an attacker sends a series of SYN packets. Each packet causes the receiver to reply with a SYN-ACK response. The receiver then waits for the ACK that follows the SYN-ACK, and stores all outstanding SYN-ACK responses on a backlog queue. SYN-ACKs are only moved off the queue when an ACK comes back or when an internal timer ends the three-way handshake. Once the queue is

full, the system will ignore all incoming SYN requests, making the system unavailable for other users.

**Figure 406** SYN Flood




### LAND Attack

In a LAND attack, hackers flood SYN packets into a network with a spoofed source IP address of the network itself. This makes it appear as if the computers in the network sent the packets to themselves, so the network is unavailable while they try to respond to themselves.

### UDP Flood Attack

UDP is a connection-less protocol and it does not require any connection setup procedure to transfer data. A UDP flood attack is possible when an attacker sends a UDP packet to a random port on the victim system. When the victim system receives a UDP packet, it will determine what application is waiting on the destination port. When it realizes that there is no application that is waiting on the port, it will generate an ICMP packet of destination unreachable to the forged source address. If enough UDP packets are delivered to ports on victim, the system will go down.

## Protocol Anomaly Background Information

The following sections may help you configure the protocol anomaly profile screen (see Section 32.3.5 on page 564)

## HTTP Inspection and TCP/UDP/ICMP Decoders

The following table gives some information on the HTTP inspection, TCP decoder, UDP decoder and ICMP decoder ZyWALL protocol anomaly rules.

**Table 177** HTTP Inspection and TCP/UDP/ICMP Decoders

| LABEL | DESCRIPTION |
|---|---|
| HTTP Inspection | |
| APACHE-WHITESPACE ATTACK | This rule deals with non-RFC standard of tab for a space delimiter. Apache uses this, so if you have an Apache server, you need to enable this option. |
| ASCII-ENCODING ATTACK | This rule can detect attacks where malicious attackers use ASCII-encoding to encode attack strings. Attackers may use this method to bypass system parameter checks in order to get information or privileges from a web server. |
| BARE-BYTE-UNICODING-ENCODING ATTACK | Bare byte encoding uses non-ASCII characters as valid values in decoding UTF-8 values. This is NOT in the HTTP standard, as all non-ASCII values have to be encoded with a %. Bare byte encoding allows the user to emulate an IIS server and interpret non-standard encodings correctly. |
| BASE36-ENCODING ATTACK | This is a rule to decode base36-encoded characters. This rule can detect attacks where malicious attackers use base36-encoding to encode attack strings. Attackers may use this method to bypass system parameter checks in order to get information or privileges from a web server. |
| DIRECTORY-TRAVERSAL ATTACK | This rule normalizes directory traversals and self-referential directories. So, “/abc/this_is_not_a_real_dir/../xyz” get normalized to “/abc/xyz”. Also, “/abc/./xyz” gets normalized to “/abc/xyz”. If a user wants to configure an alert, then specify “yes”, otherwise “no”. This alert may give false positives since some web sites refer to files using directory traversals. |
| DOUBLE-ENCODING ATTACK | This rule is IIS specific. IIS does two passes through the request URI, doing decodes in each one. In the first pass, IIS encoding (UTF-8 unicode, ASCII, bare byte, and %u) is done. In the second pass ASCII, bare byte, and %u encodings are done. |
| IIS-BACKSLASH-EVASION ATTACK | This is an IIS emulation rule that normalizes backslashes to slashes. Therefore, a request-URI of “/abc\xyz” gets normalized to “/abc/xyz”. |
| IIS-UNICODE-CODEPOINT-ENCODING ATTACK | This rule can detect attacks which send attack strings containing non-ASCII characters encoded by IIS Unicode. IIS Unicode encoding references the unicode.map file. Attackers may use this method to bypass system parameter checks in order to get information or privileges from a web server. |
| MULTI-SLASH-ENCODING ATTACK | This rule normalizes multiple slashes in a row, so something like: “abc////////xyz” get normalized to “abc/xyz”. |
| NON-RFC-DEFINED-CHAR ATTACK | This rule lets you receive a log or alert if certain non-RFC characters are used in a request URI. For instance, you may want to know if there are NULL bytes in the request-URI. |

**Table 177** HTTP Inspection and TCP/UDP/ICMP Decoders (continued)

| LABEL | DESCRIPTION |
|---|---|
| NON-RFC-HTTP-DELIMITER ATTACK | This is when a newline "\n" character is detected as a delimiter. This is non-standard but is accepted by both Apache and IIS web servers. |
| OVERSIZE-CHUNK-ENCODING ATTACK | This rule is an anomaly detector for abnormally large chunk sizes. This picks up the apache chunk encoding exploits and may also be triggered on HTTP tunneling that uses chunk encoding. |
| OVERSIZE-REQUEST-URI-DIRECTORY ATTACK | This rule takes a non-zero positive integer as an argument. The argument specifies the max character directory length for URL directory. If a URL directory is larger than this argument size, an alert is generated. A good argument value is 300 characters. This should limit the alerts to IDS evasion type attacks, like whisker. |
| SELF-DIRECTORY-TRAVERSAL ATTACK | This rule normalizes self-referential directories. So, "/abc/./xyz" gets normalized to "/abc/xyz". |
| U-ENCODING ATTACK | This rule emulates the IIS %u encoding scheme. The %u encoding scheme starts with a %u followed by 4 characters, like %uXXXX. The XXXX is a hex encoded value that correlates to an IIS unicode codepoint. This is an ASCII value. An ASCII character is encoded like, %u002f = /, %u002e = ., etc. |
| UTF-8-ENCODING ATTACK | The UTF-8 decode rule decodes standard UTF-8 unicode sequences that are in the URI. This abides by the unicode standard and only uses % encoding. Apache uses this standard, so for any Apache servers, make sure you have this option turned on. When this rule is enabled, ASCII decoding is also enabled to enforce correct functioning. |
| WEBROOT-DIRECTORY-TRAVERSAL ATTACK | This is when a directory traversal traverses past the web server root directory. This generates much fewer false positives than the directory option, because it doesn't alert on directory traversals that stay within the web server directory structure. It only alerts when the directory traversals go past the web server root directory, which is associated with certain web attacks. |
| TCP Decoder | |
| BAD-LENGTH-OPTIONS ATTACK | This is when a TCP packet is sent where the TCP option length field is not the same as what it actually is or is 0. This may cause some applications to crash. |
| EXPERIMENTAL-OPTIONS ATTACK | This is when a TCP packet is sent which contains non-RFC-complaint options. This may cause some applications to crash. |
| OBSOLETE-OPTIONS ATTACK | This is when a TCP packet is sent which contains obsolete RFC options. |
| OVERSIZE-OFFSET ATTACK | This is when a TCP packet is sent where the TCP data offset is larger than the payload. |
| TRUNCATED-OPTIONS ATTACK | This is when a TCP packet is sent which doesn't have enough data to read. This could mean the packet was truncated. |

**Table 177** HTTP Inspection and TCP/UDP/ICMP Decoders (continued)

| LABEL | DESCRIPTION |
|---|---|
| TTCP-DETECTED ATTACK | T/TCP provides a way of bypassing the standard three-way handshake found in TCP, thus speeding up transactions. However, this could lead to unauthorized access to the system by spoofing connections. |
| UNDERSIZE-LEN ATTACK | This is when a TCP packet is sent which has a TCP datagram length of less than 20 bytes. This may cause some applications to crash. |
| UNDERSIZE-OFFSET ATTACK | This is when a TCP packet is sent which has a TCP header length of less than 20 bytes.This may cause some applications to crash. |
| UDP Decoder | |
| OVERSIZE-LEN ATTACK | This is when a UDP packet is sent which has a UDP length field of greater than the actual packet length. This may cause some applications to crash. |
| TRUNCATED-HEADER ATTACK | This is when a UDP packet is sent which has a UDP datagram length of less the UDP header length. This may cause some applications to crash. |
| UNDERSIZE-LEN ATTACK | This is when a UDP packet is sent which has a UDP length field of less than 8 bytes. This may cause some applications to crash. |
| ICMP Decoder | |
| TRUNCATED-ADDRESS-HEADER ATTACK | This is when an ICMP packet is sent which has an ICMP datagram length of less than the ICMP address header length. This may cause some applications to crash. |
| TRUNCATED-HEADER ATTACK | This is when an ICMP packet is sent which has an ICMP datagram length of less than the ICMP header length. This may cause some applications to crash. |
| TRUNCATED-TIMESTAMP-HEADER ATTACK | This is when an ICMP packet is sent which has an ICMP datagram length of less than the ICMP Time Stamp header length. This may cause some applications to crash. |

# 33

# Content Filtering

## 33.1 Overview

Use the content filtering feature to control access to specific web sites or web content.

### 33.1.1 What You Can Do in the Content Filter Screens

- Use the **General** screens (Section 33.2 on page 577) to configure global content filtering settings, configure content filtering policies, and check the content filtering license status.
- Use the **Filter Profile** screens (Section 33.4 on page 582) to set up content filtering profiles.
- Use the **Cache** screen (Section 33.7 on page 596) to view and configure your ZyWALL's URL caching.

### 33.1.2 What You Need to Know About Content Filtering

#### Content Filtering

Content filtering allows you to block certain web features, such as cookies, and/or block access to specific web sites. It can also block access to specific categories of web site content. You can create different content filter policies for different addresses, schedules, users or groups and content filter profiles. For example, you can configure one policy that blocks John Doe's access to arts and entertainment web pages during the workday and another policy that lets him access them after work.

#### Content Filtering Policies

A content filtering policy allows you to do the following.

- Use schedule objects to define when to apply a content filter profile.
- Use address and/or user/group objects to define to whose web access to apply the content filter profile.
- Apply a content filter profile that you have custom-tailored.

## Content Filtering Profiles

A content filtering profile conveniently stores your custom settings for the following features.

- Category-based Blocking

  The ZyWALL can block access to particular categories of web site content, such as pornography or racial intolerance.

- Restrict Web Features

  The ZyWALL can disable web proxies and block web features such as ActiveX controls, Java applets and cookies.

- Customize Web Site Access

  You can specify URLs to which the ZyWALL blocks access. You can alternatively block access to all URLs except ones that you specify. You can also have the ZyWALL block access to URLs that contain particular keywords.

## Content Filtering Configuration Guidelines

When the ZyWALL receives an HTTP request, the content filter searches for a policy that matches the source address and time (schedule). The content filter checks the policies in order (based on the policy numbers). When a matching policy is found, the content filter allows or blocks the request depending on the settings of the filtering profile specified by the policy. Some requests may not match any policy. The ZyWALL allows the request if the default policy is not set to block. The ZyWALL blocks the request if the default policy is set to block.

## External Web Filtering Service

When you register for and enable the external web filtering service, your ZyWALL accesses an external database that has millions of web sites categorized based on content. You can have the ZyWALL block, block and/or log access to web sites based on these categories.

## Keyword Blocking URL Checking

The ZyWALL checks the URL's domain name (or IP address) and file path separately when performing keyword blocking.

The URL's domain name or IP address is the characters that come before the first slash in the URL. For example, with the URL www.zyxel.com.tw/news/pressroom.php, the domain name is www.zyxel.com.tw.

The file path is the characters that come after the first slash in the URL. For example, with the URL www.zyxel.com.tw/news/pressroom.php, the file path is news/pressroom.php.

Since the ZyWALL checks the URL's domain name (or IP address) and file path separately, it will not find items that go across the two. For example, with the URL www.zyxel.com.tw/news/pressroom.php, the ZyWALL would find "tw" in the domain name (www.zyxel.com.tw). It would also find "news" in the file path (news/pressroom.php) but it would not find "tw/news".

### Finding Out More

- See Section 5.4.17 on page 93 for related information on these screens.
- See Section 33.8 on page 598 for content filtering background/technical information.

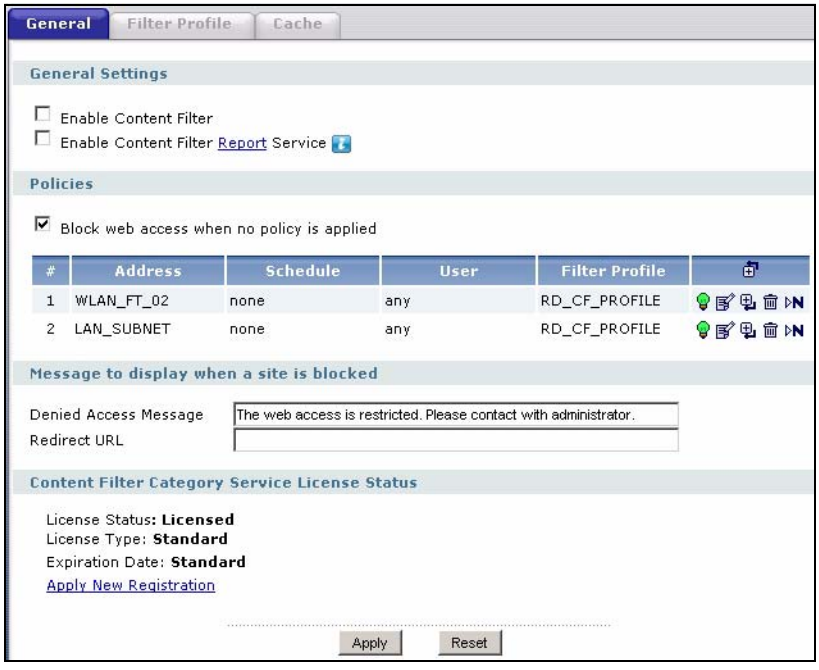
## 33.1.3 Before You Begin

- You must configure an address object, a schedule object and a filtering profile before you can set up a content filter policy.
- You must subscribe to use the external database content filtering (see the **Licensing** > **Registration** screens).

# 33.2 Content Filter General Screen

Click **Anti-X > Content Filter > General** to open the **Content Filter General** screen. Use this screen to enable content filtering, view and order your list of content filter policies, create a denial of access message or specify a redirect URL and check your external web filtering service registration status.

**Figure 407** Anti-X > Content Filter > General



The following table describes the labels in this screen.

**Table 178** Anti-X > Content Filter > General

| LABEL | DESCRIPTION |
|---|---|
| General Settings | |
| Enable Content Filter | Select this check box to enable the content filter. |
| Enable Content Filter Report Service | Select this check box to have the ZyWALL collect category-based content filtering statistics. |
| Policies | This is a list of the configured content filter policies. |
| Block web access when no policy is applied | Select this check box to stop users from accessing the Internet by default when their attempted access does not match a content filter policy. |
| # | This column lists the index numbers of the content filter policies. |
| Address | A content filter policy applies to web access from the IP addresses listed here. **any** means the content filter policy applies to all of the web access requests that the ZyWALL receives from any IP address. |
| Schedule | This column displays the name of the schedule for each content filter policy. You can define different policies for different time periods. **none** means the content filter policy applies all of the time. |
| User | This column displays the individual or group to which this policy applies. **any** means the content filter policy applies to all of the web access requests that the ZyWALL receives from any user. |
| Filter Profile | This column displays the name of the content filter profile that each content filter policy uses. The content filter profile defines to which web services, web sites or web site categories access is to be allowed or denied. |

**Table 178** Anti-X > Content Filter > General (continued)

| LABEL | DESCRIPTION |
|---|---|
| Add icon | Click the **Add** icon at the top of the column to create a new content filter policy at the top of the list.<br><br>The **Active** icon shows the entry is enabled. Click this icon to disable the entry.<br><br>The **Inactive** icon shows the entry is disabled. Click this icon to enable the entry.<br><br>Click the **Edit** icon to go to a screen where you can change the configuration settings of an entry.<br><br>Click the **Remove** icon to delete an entry from the list.<br><br>Click the **Move to N** icon, type a number in the move entry dialog box and press [ENTER] to move the entry to the numbered location.<br><br>Click a content filter policy's **Add** icon to create a new content filter policy above the current line. All other entries below the new entry are pushed down.<br><br>The ordering of the content filter policies is important as they are used in the order they are listed. The ZyWALL checks requests for Web sessions against the list of content filter policies (starting from the first in the list). The ZyWALL's content filter feature blocks or allows the Web session according to the first matching content filter policy and does not check any other content filter policies. The ZyWALL does not perform content filter on Web session requests that do not match any of the content filter policies. |
| Denied Access Message | Enter a message to be displayed when content filter blocks access to a web page. Use up to 255 characters (0-9a-zA-Z;/?:@&=+$\.-_!~*'()%,"). For example, "Access to this web page is not allowed. Please contact the network administrator". |
| Redirect URL | Enter the URL of the web page to which you want to send users when their web access is blocked by content filter. The web page you specify here opens in a new frame below the denied access message.<br><br>Use "http://" or "https://" followed by up to 255 characters (0-9a-zA-Z;/?:@&=+$\.-_!~*'()%). For example, http://192.168.1.17/ blocked access. |

**Table 178** Anti-X > Content Filter > General (continued)

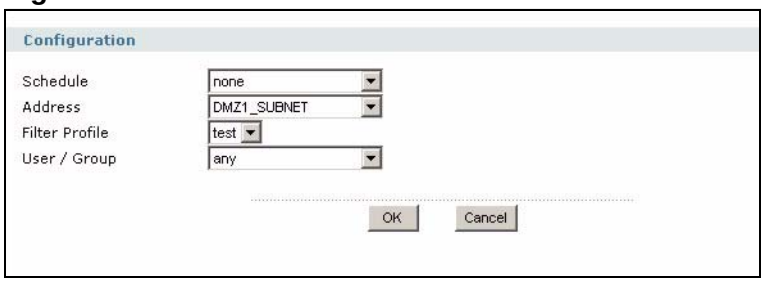
| LABEL | DESCRIPTION |
|---|---|
| License Status | This read-only field displays the status of your content-filtering database service registration.<br><br>**Not Licensed** displays if you have not successfully registered and activated the service.<br><br>**Expired** displays if your subscription to the service has expired.<br><br>**Licensed** displays if you have successfully registered the ZyWALL and activated the service.<br><br>After you register for content filter, you can see Chapter 33 on page 582 for how to use the **Test Against Web Filtering Server** button. When the content filter is active, you should see the web page's category. The query fails if the content filter is not active.<br><br>You can view content filter reports after you register the ZyWALL and activate the subscription service in the **Registration** screen (see Chapter 34 on page 601). |
| License Type | This read-only field displays what kind of service registration you have for the content-filtering database.<br><br>**None** displays if you have not successfully registered and activated the service.<br><br>**Standard** displays if you have successfully registered the ZyWALL and activated the service.<br><br>**Trial** displays if you have successfully registered the ZyWALL and activated the trial service subscription. |
| Apply new Registration | This link appears if you have not registered for the service or only have the trial registration. Click this link to go to the screen where you can register for the service. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# 33.3 Content Filter Policy Add or Edit Screen

Click **Anti-X > Content Filter > General > Add or Edit** to open the **Content Filter Policy** screen. Use this screen to configure a content filter policy. A content

filter policy defines which content filter profile should be applied, when it should be applied, and to whose web access it should be applied.

**Figure 408** Anti-X > Content Filter > General > Add l




The following table describes the labels in this screen.

**Table 179** Anti-X > Content Filter > General > Add

| LABEL | DESCRIPTION |
|---|---|
| Schedule | Select a schedule to define when to apply this content filter policy. You can define different policies for different time periods. For example, you could have one policy that blocks access to certain categories of web sites during working hours and another policy that allows access to certain categories after the work day is over.<br><br>Select **Create Object** to configure a new schedule (see Chapter 40 on page 677 for details).<br><br>Select **none** to have the content filter policy apply all of the time. |
| Address | Select the address or address group for which you want to use this policy.<br><br>Select **Create Object** to configure a new address or address group.<br><br>Select **any** to have the content filter policy apply to all of the web access requests that the ZyWALL receives from any IP address. |
| Filter Profile | Use the drop-down list box to select the content filter profile that you want to use for this policy. The content filter profile defines to which web services, web sites or web site categories access is to be allowed or denied. Use the content filter **Filter Profile** screens to configure the profiles. |
| User/Group | Use the drop-down list box to select the individual or group for which you want to use this policy.<br><br>Select **Create Object** to configure a new user account (see Section 37.2.1 on page 652 for details).<br><br>Select **any** to have the content filter policy apply to all of the web access requests that the ZyWALL receives from any user. |
| OK | Click **OK** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving your changes. |

# 33.4 Content Filter Profile Screen

Click **Anti-X > Content Filter > Filter Profile** to open the **Filter Profile** screen. A content filter profile defines to which web services, web sites or web site categories access is to be allowed or denied.

**Figure 409** Anti-X > Content Filter > Filter Profile


The following table describes the labels in this screen.

**Table 180** Anti-X > Content Filter > Filter Profile

| LABEL | DESCRIPTION |
|---|---|
| # | This column lists the index numbers of the content filter profiles. |
| Filtering Profile Name | This column lists the names of the content filter profiles. |
| Add | Click the **Add** icon at the top of the column to create a new content filter profile at the end of the list.<br>Click a content filter policy's **Add** icon at the to create a new content filter policy below the current line. All other entries below the new entry are pushed down. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

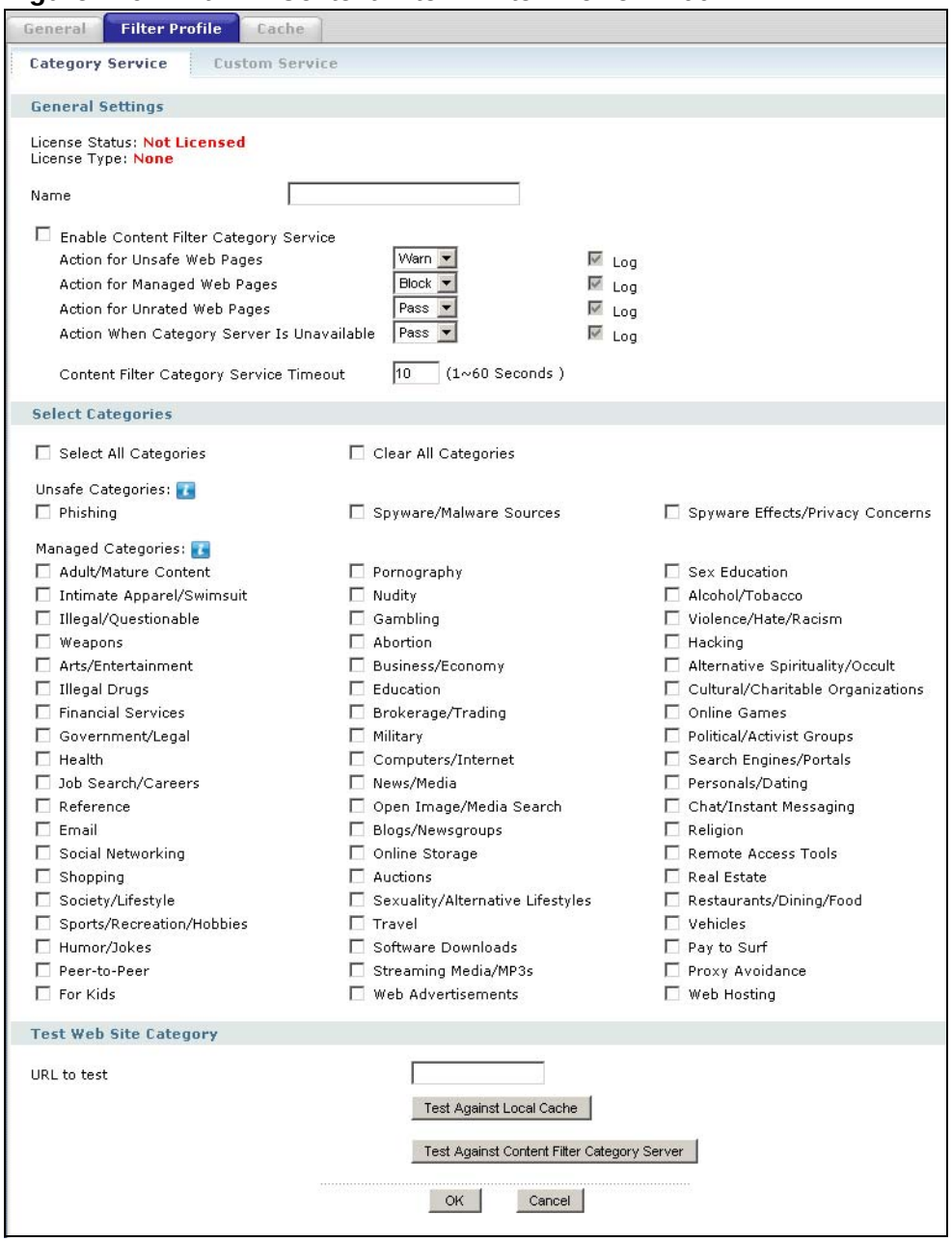
# 33.5 Content Filter Categories Screen

Click **Anti-X > Content Filter > Filter Profile > Add or Edit** to open the **Categories** screen. Use this screen to enable external database content filtering and select which web site categories to block and/or log.

Note: You must register for external content filtering before you can use it. See Section 8.2 on page 167 for how to register.

See Chapter 34 on page 601 for how to view content filtering reports.

**Figure 410** Anti-X > Content Filter > Filter Profile > Add



The following table describes the labels in this screen.

**Table 181** Anti-X > Content Filter > Filter Profile > Add

| LABEL | DESCRIPTION |
|---|---|
| License Status | This read-only field displays the status of your content-filtering database service registration.<br><br>**Not Licensed** displays if you have not successfully registered and activated the service.<br><br>**Expired** displays if your subscription to the service has expired.<br><br>**Licensed** displays if you have successfully registered the ZyWALL and activated the service.<br><br>After you register for content filter, you can see Chapter 33 on page 582 for how to use the **Test Against Web Filtering Server** button. When the content filter is active, you should see the web page's category. The query fails if the content filter is not active.<br><br>You can view content filter reports after you register the ZyWALL and activate the subscription service in the **Registration** screen (see Chapter 34 on page 601). |
| License Type | This read-only field displays what kind of service registration you have for the content-filtering database.<br><br>**None** displays if you have not successfully registered and activated the service.<br><br>**Standard** displays if you have successfully registered the ZyWALL and activated the standard content filtering service.<br><br>**Trial** displays if you have successfully registered the ZyWALL and activated the trial service subscription. |
| Name | Enter a descriptive name for this content filtering profile name. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| Enable Content Filter Category Service | Enable external database content filtering to have the ZyWALL check an external database to find to which category a requested web page belongs. The ZyWALL then blocks or forwards access to the web page depending on the configuration of the rest of this page. |

**Table 181** Anti-X > Content Filter > Filter Profile > Add (continued)

| LABEL | DESCRIPTION |
|---|---|
| Action for Unsafe Web Pages | Select **Pass** to allow users to access web pages that match the unsafe categories that you select below.<br><br>Select **Block** to prevent users from accessing web pages that match the unsafe categories that you select below. When external database content filtering blocks access to a web page, it displays the denied access message that you configured in the **Content Filter General** screen along with the category of the blocked web page.<br><br>Select **Warn** to display a warning message before allowing users to access web pages that match the unsafe categories that you select below.<br><br>Select **Log** to record attempts to access web pages that match the unsafe categories that you select below. |
| Action for Managed Web Pages | Select **Pass** to allow users to access web pages that match the other categories that you select below.<br><br>Select **Block** to prevent users from accessing web pages that match the other categories that you select below. When external database content filtering blocks access to a web page, it displays the denied access message that you configured in the **Content Filter General** screen along with the category of the blocked web page.<br><br>Select **Log** to record attempts to access web pages that match the other categories that you select below. |
| Action for Unrated Web Pages | Select **Pass** to allow users to access web pages that the external web filtering service has not categorized.<br><br>Select **Block** to prevent users from accessing web pages that the external web filtering service has not categorized. When the external database content filtering blocks access to a web page, it displays the denied access message that you configured in the **Content Filter General** screen along with the category of the blocked web page.<br><br>Select **Warn** to display a warning message before allowing users to access web pages that the external web filtering service has not categorized.<br><br>Select **Log** to record attempts to access web pages that are not categorized. |

**Table 181** Anti-X > Content Filter > Filter Profile > Add (continued)

| LABEL | DESCRIPTION |
|---|---|
| Action When Category Server Is Unavailable | Select **Pass** to allow users to access any requested web page if the external content filtering database is unavailable.<br><br>Select **Block** to block access to any requested web page if the external content filtering database is unavailable.<br><br>Select **Warn** to display a warning message before allowing users to access any requested web page if the external content filtering database is unavailable.<br><br>The following are possible causes for the external content filtering server not being available:<br><br>• There is no response from the external content filtering server within the time period specified in the **Content Filter Server Unavailable Timeout** field.<br>• The ZyWALL is not able to resolve the domain name of the external content filtering database.<br>• There is an error response from the external content filtering database. This can be caused by an expired content filtering registration (External content filtering's license key is invalid").<br><br>Select **Log** to record attempts to access web pages that occur when the external content filtering database is unavailable. |
| Content Filter Category Service Timeout | Specify a number of seconds (1 to 60) for the ZyWALL to wait for a response from the external content filtering server. If there is still no response by the time this period expires, the ZyWALL blocks or allows access to the requested web page based on the setting in the **Block When Content Filter Server Is Unavailable** field.<br><br>This setting applies to all of your content filtering profiles. |
| Select Categories | |
| Select All Categories | Select this check box to restrict access to all site categories listed below. |
| Clear All Categories | Select this check box to clear the selected categories below. |
| Unsafe Categories | These are categories of web pages that are known to pose a threat to users or their computers. |
| Phishing | This category includes pages that are designed to appear as a legitimate bank or retailer with the intent to fraudulently capture sensitive data (i.e. credit card numbers, pin numbers). |

**Table 181** Anti-X > Content Filter > Filter Profile > Add (continued)

| LABEL | DESCRIPTION |
|---|---|
| Spyware/Malware Sources | This category includes pages which distribute spyware and other malware. Spyware is defined as software which takes control of your computer, modifies computer settings, collects or reports personal information, or misrepresents itself by tricking users to install, download, or enter personal information. This includes drive-by downloads; browser hijackers; dialers; intrusive advertising; any program which modifies your homepage, bookmarks, or security settings; and keyloggers. It also includes any software which bundles spyware (as defined above) as part of its offering. Information collected or reported is "personal" if it contains uniquely identifying data, such as e-mail addresses, name, social security number, IP address, etc. A site is not classified as spyware if the user is reasonably notified that the software will perform these actions (that is, it alerts that it will send personal information, be installed, or that it will log keystrokes). Note: Sites rated as spyware should have a second category assigned with them. |
| Spyware Effects/ Privacy Concerns | This category includes pages to which spyware (as defined in the Spyware/Malware Sources category) reports its findings or from which it alone downloads advertisements. Also includes sites that contain serious privacy issues, such as “phone home” sites to which software can connect and send user info; sites that make extensive use of tracking cookies without a posted privacy statement; and sites to which browser hijackers redirect users. Usually does not include sites that can be marked as Spyware/Malware. Note: Sites rated as spyware effects typically have a second category assigned with them. |
| Managed Categories | These are categories of web pages based on their content. Select categories in this section to control access to specific types of Internet content.<br><br>You must have the standard content filtering license to filter these categories. |
| Adult/Mature Content | This category includes pages that contain material of adult nature that does not necessarily contain excessive violence, sexual content, or nudity. These pages include very profane or vulgar content and pages that are not appropriate for children. |
| Pornography | This category includes pages that contain sexually explicit material for the purpose of arousing a sexual or prurient interest. |
| Sex Education | This category includes pages that provide graphic information (sometimes graphic) on reproduction, sexual development, safe sex practices, sexuality, birth control, and sexual development. It also includes pages that offer tips for better sex as well as products used for sexual enhancement. |
| Intimate Apparel/ Swimsuit | This category includes pages that contain images or offer the sale of swimsuits or intimate apparel or other types of suggestive clothing. It does not include pages selling undergarments as a subsection of other products offered. |

**Table 181** Anti-X > Content Filter > Filter Profile > Add (continued)

| LABEL | DESCRIPTION |
|---|---|
| Nudity | This category includes pages containing nude or seminude depictions of the human body. These depictions are not necessarily sexual in intent or effect, but may include pages containing nude paintings or photo galleries of artistic nature. This category also includes nudist or naturist pages that contain pictures of nude individuals. |
| Alcohol/Tobacco | This category includes pages that promote or offer the sale alcohol/tobacco products, or provide the means to create them. It also includes pages that glorify, tout, or otherwise encourage the consumption of alcohol/tobacco. It does not include pages that sell alcohol or tobacco as a subset of other products. |
| Illegal/Questionable | This category includes pages that advocate or give advice on performing illegal acts such as service theft, evading law enforcement, fraud, burglary techniques and plagiarism. It also includes pages that provide or sell questionable educational materials, such as term papers.<br><br>Note: This category includes sites identified as being malicious in any way (such as having viruses, spyware and etc.). |
| Gambling | This category includes pages where a user can place a bet or participate in a betting pool (including lotteries) online. It also includes pages that provide information, assistance, recommendations, or training on placing bets or participating in games of chance. It does not include pages that sell gambling related products or machines. It also does not include pages for offline casinos and hotels (as long as those pages do not meet one of the above requirements). |
| Violence/Hate/Racism | This category includes pages that depict extreme physical harm to people or property, or that advocate or provide instructions on how to cause such harm. It also includes pages that advocate, depict hostility or aggression toward, or denigrate an individual or group on the basis of race, religion, gender, nationality, ethnic origin, or other characteristics. |
| Weapons | This category includes pages that sell, review, or describe weapons such as guns, knives or martial arts devices, or provide information on their use, accessories, or other modifications. It does not include pages that promote collecting weapons, or groups that either support or oppose weapons use. |
| Abortion | This category includes pages that provide information or arguments in favor of or against abortion, describe abortion procedures, offer help in obtaining or avoiding abortion, or provide information on the effects, or lack thereof, of abortion. |
| Hacking | This category includes pages that distribute, promote, or provide hacking tools and/or information which may help gain unauthorized access to computer systems and/or computerized communication systems. Hacking encompasses instructions on illegal or questionable tactics, such as creating viruses, distributing cracked or pirated software, or distributing other protected intellectual property. |

**Table 181** Anti-X > Content Filter > Filter Profile > Add (continued)

| LABEL | DESCRIPTION |
|---|---|
| Arts/Entertainment | This category includes pages that promote and provide information about motion pictures, videos, television, music and programming guides, books, comics, movie theatres, galleries, artists or reviews on entertainment. |
| Business/Economy | This category includes pages devoted to business firms, business information, economics, marketing, business management and entrepreneurship. This does not include pages that perform services that are defined in another category (such as Information Technology companies, or companies that sell travel services). |
| Alternative Spirituality/ Occult | This category includes pages that promote and provide information on religions such as Wicca, Witchcraft or Satanism. Occult practices, atheistic views, voodoo rituals or any other form of mysticism are represented here. Includes sites that endorse or offer methods, means of instruction, or other resources to affect or influence real events through the use of spells, incantations, curses and magic powers. This category includes sites which discuss or deal with paranormal or unexplained events. |
| Illegal Drugs | This category includes pages that promote, offer, sell, supply, encourage or otherwise advocate the illegal use, cultivation, manufacture, or distribution of drugs, pharmaceuticals, intoxicating plants or chemicals and their related paraphernalia. |
| Education | This category includes pages that offer educational information, distance learning and trade school information or programs. It also includes pages that are sponsored by schools, educational facilities, faculty, or alumni groups. |
| Cultural/Charitable Organization | This category includes pages that nurture cultural understanding and foster volunteerism such as 4H, the Lions and Rotary Clubs. Also encompasses non-profit associations that cultivate philanthropic or relief efforts. Sites that provide a learning environment or cultural refinement/awareness outside of the strictures of formalized education such as museums and planetariums are included under this heading. |
| Financial Services | This category includes pages that provide or advertise banking services (online or offline) or other types of financial information, such as loans. It does not include pages that offer market information, brokerage or trading services. |
| Brokerage/Trading | This category includes pages that provide or advertise trading of securities and management of investment assets (online or offline). It also includes insurance pages, as well as pages that offer financial investment strategies, quotes, and news. |
| Online Games | This category includes pages that provide information and support game playing or downloading, video games, computer games, electronic games, tips, and advice on games or how to obtain cheat codes. It also includes pages dedicated to selling board games as well as journals and magazines dedicated to game playing. It includes pages that support or host online sweepstakes and giveaways. |

**Table 181** Anti-X > Content Filter > Filter Profile > Add (continued)

| LABEL | DESCRIPTION |
|---|---|
| Government/Legal | This category includes pages sponsored by or which provide information on government, government agencies and government services such as taxation and emergency services. It also includes pages that discuss or explain laws of various governmental entities. |
| Military | This category includes pages that promote or provide information on military branches or armed services. |
| Political/Activist Groups | This category includes pages sponsored by or which provide information on political parties, special interest groups, or any organization that promotes change or reform in public policy, public opinion, social practice, or economic activities. |
| Health | This category includes pages that provide advice and information on general health such as fitness and well-being, personal health or medical services, drugs, alternative and complimentary therapies, medical information about ailments, dentistry, optometry, general psychiatry, self-help, and support organizations dedicated to a disease or condition. |
| Computers/Internet | This category includes pages that sponsor or provide information on computers, technology, the Internet and technology-related organizations and companies. |
| Search Engines/Portals | This category includes pages that support searching the Internet, indices, and directories. |
| Job Search/Careers | This category includes pages that provide assistance in finding employment, and tools for locating prospective employers. |
| News/Media | This category includes pages that primarily report information or comments on current events or contemporary issues of the day. It also includes radio stations and magazines. It does not include pages that can be rated in other categories. |
| Personals/Dating | This category includes pages that promote interpersonal relationships. |
| Reference | This category includes pages containing personal, professional, or educational reference, including online dictionaries, maps, census, almanacs, library catalogues, genealogy-related pages and scientific information. |
| Open Image/Media Search | This category includes pages with image or video search capabilities which return graphical results (i.e. thumbnail pictures) that include potentially pornographic content along with non-pornographic content (as defined in the Pornography category). Sites that explicitly exclude offensive content are not included in this category. |
| Chat/Instant Messaging | This category includes pages that provide chat or instant messaging capabilities or client downloads. |
| Email | This category includes pages offering web-based email services, such as online email reading, e-cards, and mailing list services. |
| Blogs/Newsgroups | This category includes pages that offer access to Usenet news groups or other messaging or bulletin board systems. Also, blog specific sites or an individual with his own blog. This does not include social networking communities with blogs. |

**Table 181** Anti-X > Content Filter > Filter Profile > Add (continued)

| LABEL | DESCRIPTION |
|---|---|
| Religion | This category includes pages that promote and provide information on conventional or unconventional religious or quasi-religious subjects, as well as churches, synagogues, or other houses of worship. It does not include pages containing alternative religions such as Wicca or witchcraft or atheist beliefs (Alternative Spirituality/Occult). |
| Social Networking | This category includes pages that enable people to connect with others to form an online community. Typically members describe themselves in personal web page profiles and form interactive networks, linking them with other members based on common interests or acquaintances. Instant messaging, file sharing and web logs (blogs) are common features of Social Networking sites. Note: These sites may contain offensive material in the community-created content. Sites in this category are also referred to as "virtual communities" or "online communities". This category does not include more narrowly focused sites, like those that specifically match descriptions for Personals/Dating sites or Business sites. |
| Online Storage | This category includes pages that provide a secure, encrypted, off-site backup and restoration of personal data. These online repositories are typically used to store, organize and share videos, music, movies, photos, documents and other electronically formatted information. Sites that fit this criteria essentially act as your personal hard drive on the Internet. |
| Remote Access Tools | This category includes pages that primarily focus on providing information about and/or methods that enables authorized access to and use of a desktop computer or private network remotely. |
| Shopping | This category includes pages that provide or advertise the means to obtain goods or services. It does not include pages that can be classified in other categories (such as vehicles or weapons). |
| Auctions | This category includes pages that support the offering and purchasing of goods between individuals. This does not include classified advertisements. |
| Real Estate | This category includes pages that provide information on renting, buying, or selling real estate or properties. |
| Society/Lifestyle | This category includes pages providing information on matters of daily life. This does not include pages relating to entertainment, sports, jobs, sex or pages promoting alternative lifestyles such as homosexuality. Personal homepages fall within this category if they cannot be classified in another category. |
| Sexuality/Alternative Lifestyles | This category includes pages that provide information, promote, or cater to gays, lesbians, swingers, other sexual orientations or practices, or a particular fetish. This category does not include sites that are sexually gratuitous in nature which would typically fall under the Pornography category. |
| Restaurants/Dining/ Food | This category includes pages that list, review, discuss, advertise and promote food, catering, dining services, cooking and recipes. |

**Table 181** Anti-X > Content Filter > Filter Profile > Add (continued)

| LABEL | DESCRIPTION |
|---|---|
| Sports/Recreation/ Hobbies | This category includes pages that promote or provide information about spectator sports, recreational activities, or hobbies. This includes pages that discuss or promote camping, gardening, and collecting. |
| Travel | This category includes pages that promote or provide opportunity for travel planning, including finding and making travel reservations, vehicle rentals, descriptions of travel destinations, or promotions for hotels or casinos. |
| Vehicles | This category includes pages that provide information on or promote vehicles, boats, or aircraft, including pages that support online purchase of vehicles or parts. |
| Humor/Jokes | This category includes pages that primarily focus on comedy, jokes, fun, etc. This may include pages containing jokes of adult or mature nature. Pages containing humorous Adult/ Mature content also have an Adult/Mature category rating. |
| Software Downloads | This category includes pages that are dedicated to the electronic download of software packages, whether for payment or at no charge. |
| Pay to Surf | This category includes pages that pay users in the form of cash or prizes, for clicking on or reading specific links, email, or web pages. |
| Peer-to-Peer | This category includes pages that distribute software to facilitate the direct exchange of files between users, including software that enables file search and sharing across a network without dependence on a central server. |
| Streaming Media/MP3s | This category includes pages that sell, deliver, or stream music or video content in any format, including sites that provide downloads for such viewers. |
| Proxy Avoidance | This category includes pages that provide information on how to bypass proxy server/appliance features or gain access to URLs in any way that bypasses the proxy server/appliance. It also includes any service that will allow a person to bypass the content filtering feature, such as anonymous surfing services. |
| For Kids | This category includes pages designed specifically for children. |
| Web Advertisements | This category includes pages that provide online advertisements or banners. This does not include advertising servers that serve adult-oriented advertisements. |
| Web Hosting | This category includes pages of organizations that provide top-level domain pages, as well as web communities or hosting services. |
| Test Web Site Category | |
| URL to test | You can check which category a web page belongs to. Enter a web site URL in the text box. |
| Test Against Local Cache | Click this button to see the category recorded in the ZyWALL's content filtering database for the web page you specified (if the database has an entry for it). |
| Test Against Content Filter Server | Click this button to see the category recorded in the external content filter server's database for the web page you specified. |

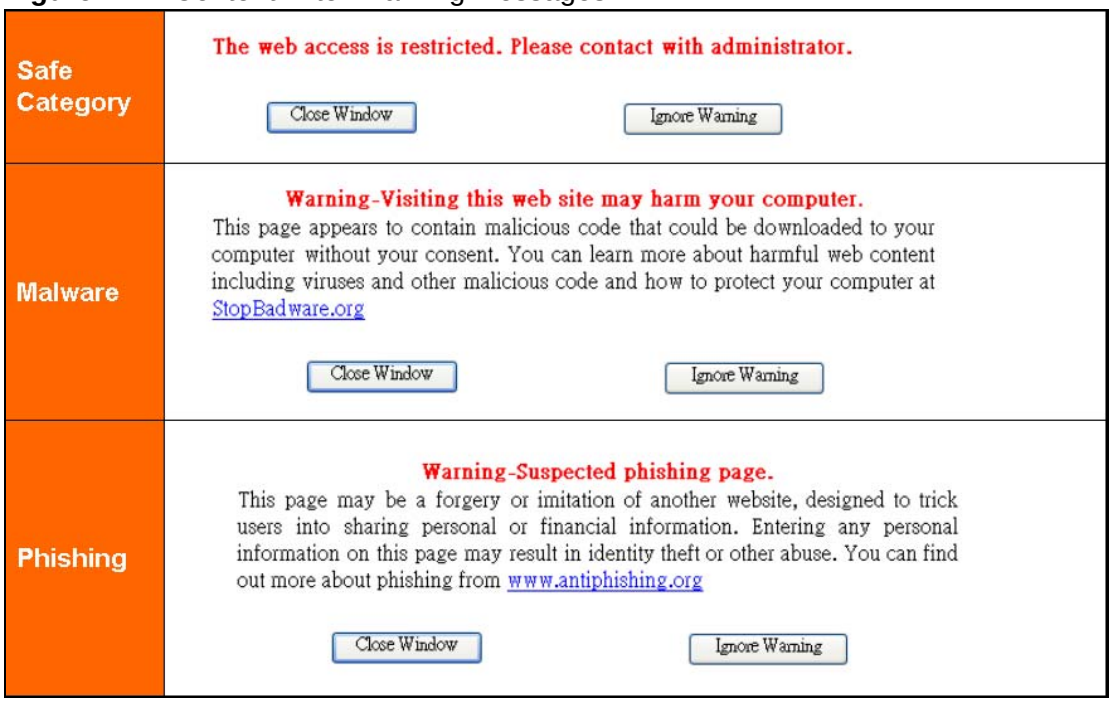
**Table 181** Anti-X > Content Filter > Filter Profile > Add (continued)

| LABEL | DESCRIPTION |
|---|---|
| OK | Click **OK** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving your changes. |

### 33.5.1 Content Filter Blocked and Warning Messages

These are the content filtering warning messages. The messages for blocked access are the same but do not include the buttons.

**Figure 411** Content Filter Warning Messages

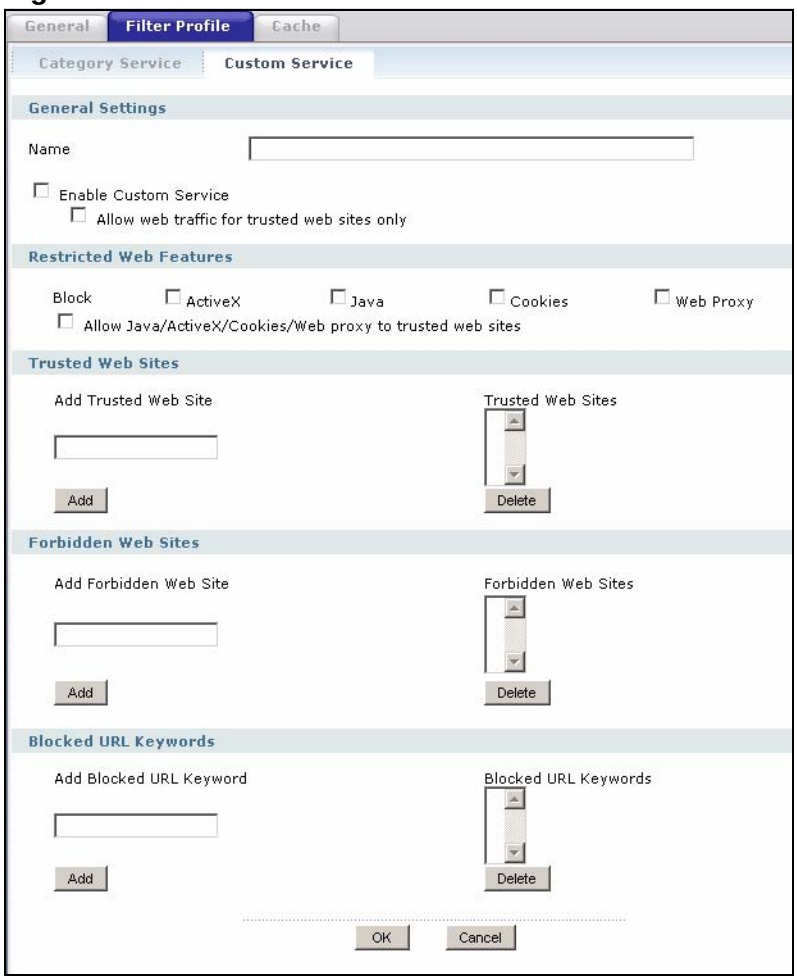



## 33.6 Content Filter Customization Screen

Click **Anti-X > Content Filter > Filter Profile > Add or Edit > Customization** to open the **Customization** screen. You can create a list of good (allowed) web site addresses and a list of bad (blocked) web site addresses. You can also block

web sites based on whether the web site's address contains a keyword. Use this screen to add or remove specific sites or keywords from the filter list.

**Figure 412** Anti-X > Content Filter > Filter Profile > Customization




The following table describes the labels in this screen.

**Table 182** Anti-X > Content Filter > Filter Profile > Customization

| LABEL | DESCRIPTION |
|---|---|
| Name | Enter a descriptive name for this content filtering profile name. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| Enable Custom Service | Select this check box to allow trusted web sites and block forbidden web sites. Content filter list customization may be enabled and disabled without re-entering these site names. |
| Allow Web traffic for trusted web sites only | When this box is selected, the ZyWALL blocks Web access to sites that are not on the **Trusted Web Sites** list. If they are chosen carefully, this is the most effective way to block objectionable material. |

**Table 182** Anti-X > Content Filter > Filter Profile > Customization (continued)

| LABEL | DESCRIPTION |
|---|---|
| Restricted Web Features | Select the check box(es) to restrict a feature. When you download a page containing a restricted feature, that part of the web page will appear blank or grayed out. |
| Block<br>ActiveX | ActiveX is a tool for building dynamic and active web pages and distributed object applications. When you visit an ActiveX web site, ActiveX controls are downloaded to your browser, where they remain in case you visit the site again. |
| Java | Java is a programming language and development environment for building downloadable Web components or Internet and intranet business applications of all kinds. |
| Cookies | Cookies are files stored on a computer's hard drive. Some web servers use them to track usage and provide service based on ID. |
| Web Proxy | A server that acts as an intermediary between a user and the Internet to provide security, administrative control, and caching service. When a proxy server is located on the WAN it is possible for LAN users to circumvent content filtering by pointing to this proxy server. |
| Allow Java/ActiveX/ Cookies/Web proxy to trusted web sites | When this box is selected, the ZyWALL will permit Java, ActiveX and Cookies from sites on the **Trusted Web Sites** list to the LAN. In certain cases, it may be desirable to allow Java, ActiveX or Cookies from sites that are known and trusted. |
| Trusted Web Sites | These are sites that you want to allow access to, regardless of their content rating, can be allowed by adding them to this list. |
| Add Trusted Web Site | Enter host names such as www.good-site.com into this text field. Do not enter the complete URL of the site – that is, do not include "http://". All subdomains are allowed. For example, entering "zyxel.com" also allows "www.zyxel.com", "partner.zyxel.com", "press.zyxel.com", and so on. You can also enter just a top level domain. For example, enter .com to allow all .com domains.<br><br>Use up to 63 characters (0-9a-z-). The casing does not matter. |
| Trusted Web Sites | This list displays the trusted web sites already added. |
| Add | Click this button when you have finished adding the host name in the text field above. |
| Delete | Select a web site name from the **Trusted Web Sites** list, and then click this button to delete it from that list. |
| Forbidden Web Site List | Sites that you want to block access to, regardless of their content rating, can be allowed by adding them to this list. |

**Table 182** Anti-X > Content Filter > Filter Profile > Customization (continued)

| LABEL | DESCRIPTION |
|---|---|
| Add Forbidden Web Site | Enter host names such as www.bad-site.com into this text field. Do not enter the complete URL of the site – that is, do not include “http://”. All subdomains are also blocked. For example, entering “bad-site.com” also blocks “www.bad-site.com”, “partner.bad-site.com”, “press.bad-site.com”, and do on. You can also enter just a top level domain. For example, enter .com to block all .com domains.<br><br>Use up to 63 characters (0-9a-z-). The casing does not matter. |
| Forbidden Web Sites | This list displays the forbidden web sites already added. |
| Add | Click this button when you have finished adding the host name in the text field above. |
| Delete | Select a web site name from the **Forbidden Web Sites** list, and then click this button to delete it from that list. |
| Blocked URL Keywords | This section allows you to block Web sites with URLs that contain certain keywords in the domain name or IP address. |
| Add Blocked URL Keyword | Enter a keyword or a numerical IP address to block. You can also enter a numerical IP address.<br><br>Use up to 63 case-insensitive characters (0-9a-zA-Z;/ ?:@&=+$\.-_!~*'()%,). For example enter Bad_Site to block access to any web page that includes the exact phrase Bad_Site. This does not block access to web pages that only include part of the phrase (such as Bad for example). |
| Blocked URL Keywords | This list displays the keywords already added. |
| Add | Click this button when you have finished adding the key words field above. |
| Delete | Select a keyword from the **Blocked URL Keywords** list, and then click this button to delete it from that list. |
| OK | Click **OK** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving your changes. |

# 33.7 Content Filter Cache Screen

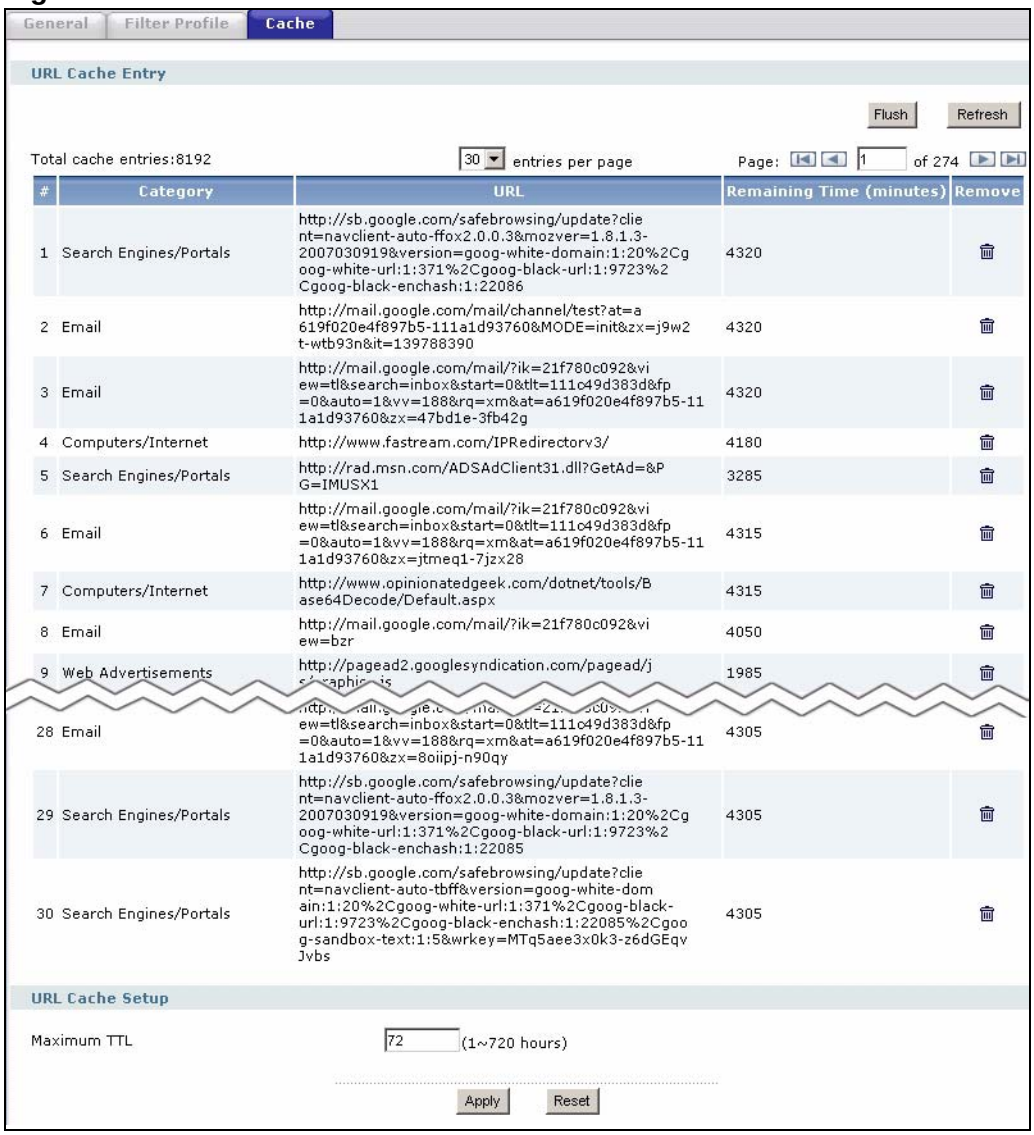
Click **Anti-X > Content Filter > Cache** to display the **Content Filter Cache** screen. Use this screen to view and configure your ZyWALL’s URL caching. You can also configure how long a categorized web site address remains in the cache as well as view those web site addresses to which access has been allowed or blocked based on the responses from the external content filtering server. The ZyWALL only queries the external content filtering database for sites not found in the cache.

You can remove individual entries from the cache. When you do this, the ZyWALL queries the external content filtering database the next time someone tries to

access that web site. This allows you to check whether a web site's category has been changed.

Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

**Figure 413** Anti-X > Content Filter > Cache




The following table describes the labels in this screen.

**Table 183** Anti-X > Content Filter > Cache

| LABEL | DESCRIPTION |
|---|---|
| URL Cache Entry | |
| Flush | Click this button to clear all web site addresses from the cache manually. |

**Table 183** Anti-X > Content Filter > Cache (continued)

| LABEL | DESCRIPTION |
|---|---|
| Refresh | Click this button to reload the list of content filter cache entries. |
| Total cache entries | This is the number of web site addresses in the content filter cache. |
| entries per page | Select how many web site addresses to display per page in the screen. |
| Page x of x | This is the number of the page of entries currently displayed and the total number of pages of entries. Type a page number to go to or use the arrows to navigate the pages of entries. |
| # | This is the index number of a categorized web site address record. |
| Category | This field shows whether access to the web site's URL was blocked or allowed.<br><br>Click the column heading to sort the entries. Point the triangle up to display the blocked URLs before the URLs to which access was allowed. Point the triangle down to display the URLs to which access was allowed before the blocked URLs. |
| URL | This is a web site's address that the ZyWALL previously checked with the external content filtering database. |
| Remaining Time (minutes) | This is the number of minutes left before the URL entry is discarded from the cache. |
| Remove | Click the **Delete** icon to remove the URL entry from the cache. |
| URL Cache Setup | |
| Maximum TTL | Type the maximum time to live (TTL) (1 to 720 hours). This sets how long the ZyWALL is to keep an entry in the URL cache before discarding it.<br><br>The external content filtering database frequently adds previously uncategorized web sites and sometimes changes a web site's category. Setting this limit higher will speed up the processing of web access requests but will also make it take longer for the ZyWALL to reflect changes in the external content filtering database. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

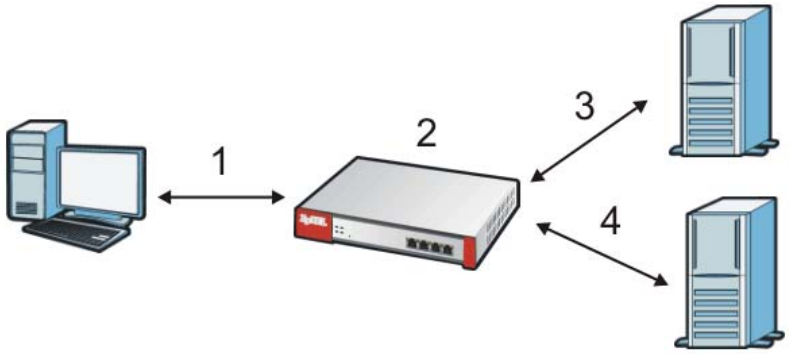
# 33.8 Content Filter Technical Reference

This section provides content filtering background information.

# External Content Filter Server Lookup Procedure

The content filter lookup process is described below.

**Figure 414** Content Filter Lookup Procedure




1. A computer behind the ZyWALL tries to access a web site.
2. The ZyWALL looks up the web site in its cache. If an attempt to access the web site was made in the past, a record of that web site's category will be in the ZyWALL's cache. The ZyWALL blocks, blocks and logs or just logs the request based on your configuration.
3. Use the **Content Filter Cache** screen to configure how long a web site address remains in the cache as well as view those web site addresses (see Section 33.7 on page 596). All of the web site address records are also cleared from the local cache when the ZyWALL restarts.
4. If the ZyWALL has no record of the web site, it queries the external content filter database and simultaneously sends the request to the web server.
5. The external content filter server sends the category information back to the ZyWALL, which then blocks and/or logs access to the web site based on the settings in the content filter profile. The web site's address and category are then stored in the ZyWALL's content filter cache.

# 34

# Content Filter Reports

## 34.1 Overview

You can view content filtering reports after you have activated the category-based content filtering subscription service.

See Chapter 8 on page 165 on how to create a myZyXEL.com account, register your device and activate the subscription services.

## 34.2 Viewing Content Filter Reports

Content filtering reports are generated statistics and charts of access attempts to web sites belonging to the categories you selected in your device content filter screen.

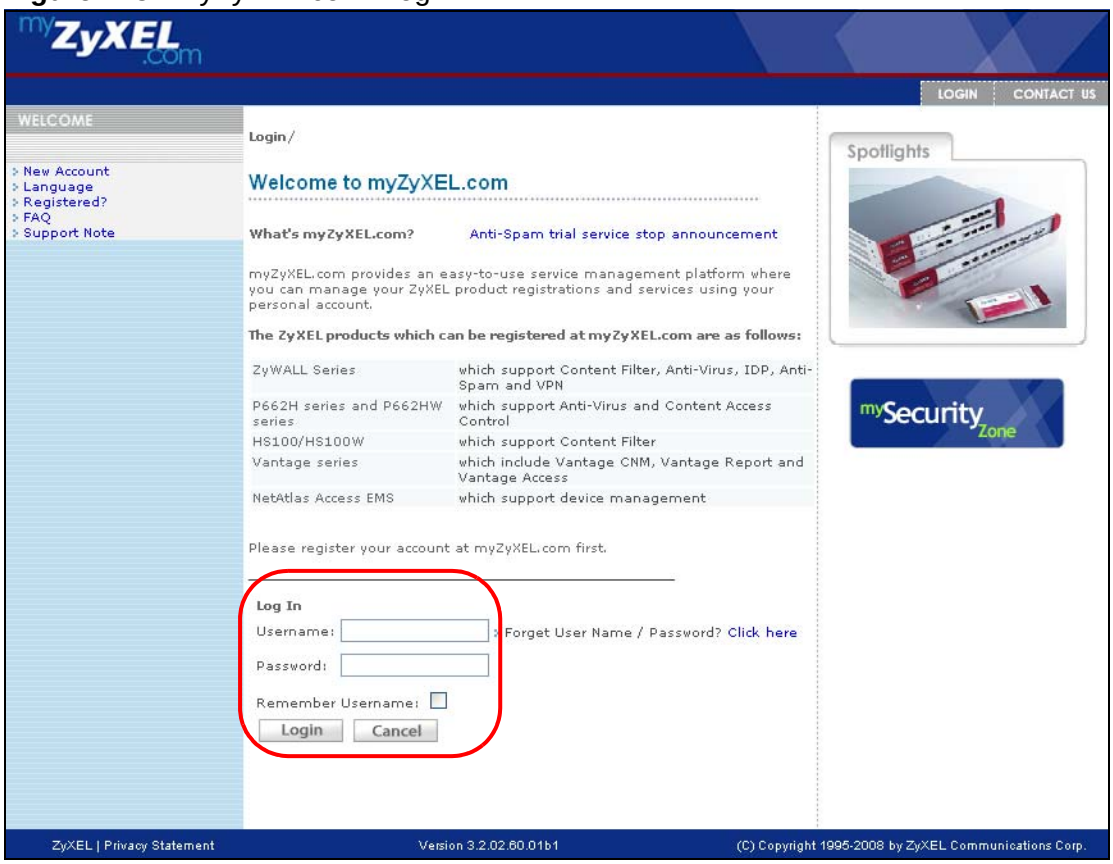
You need to register your iCard before you can view content filtering reports.

Alternatively, you can also view content filtering reports during the free trial (up to 30 days).

1 Go to http://www.myZyXEL.com.

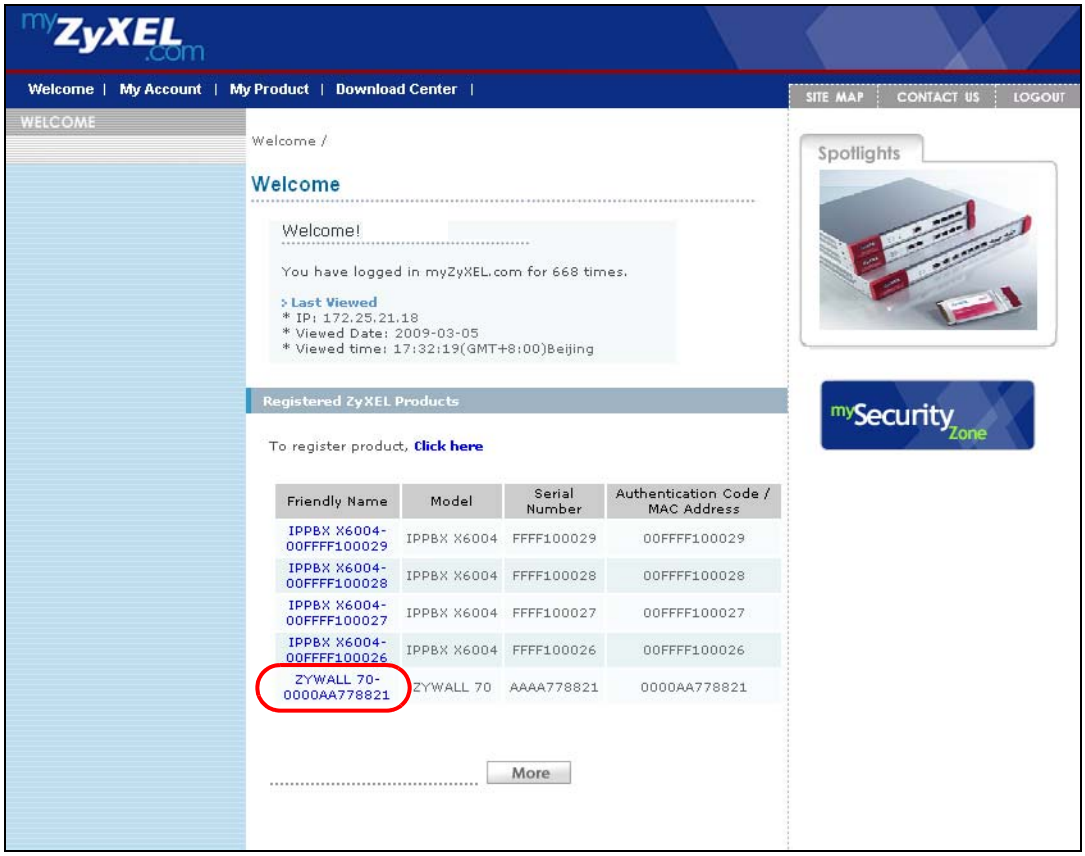
2 Fill in your myZyXEL.com account information and click **Login**.

**Figure 415** myZyXEL.com: Login



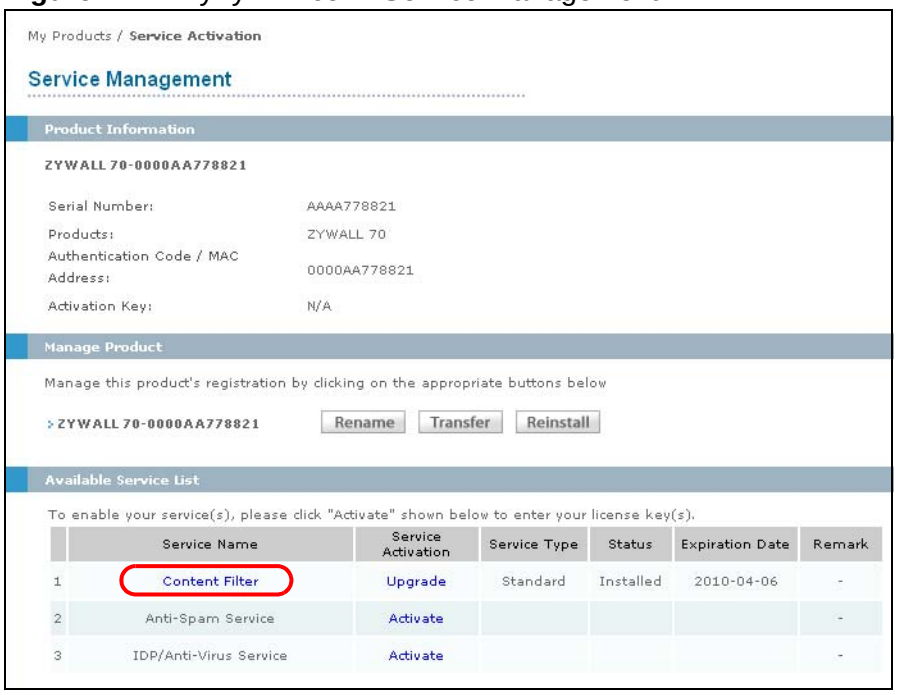
3 A welcome screen displays. Click your ZyWALL's model name and/or MAC address under **Registered ZyXEL Products** (the ZyWALL 70 is shown as an example here). You can change the descriptive name for your ZyWALL using the **Rename** button in the **Service Management** screen (see Figure 417 on page 604).

**Figure 416** myZyXEL.com: Welcome



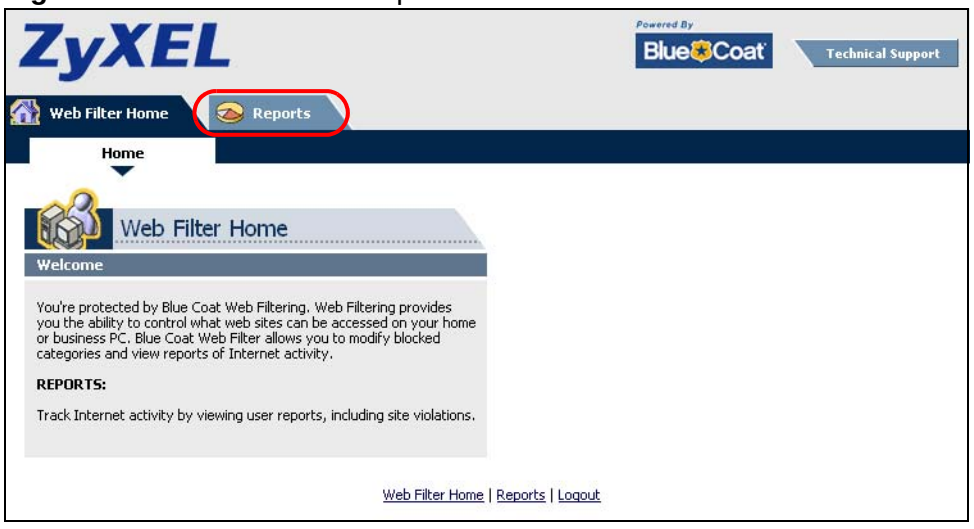
4 In the **Service Management** screen click **Content Filter** in the **Service Name** column to open the content filter reports screens.

**Figure 417** myZyXEL.com: Service Management



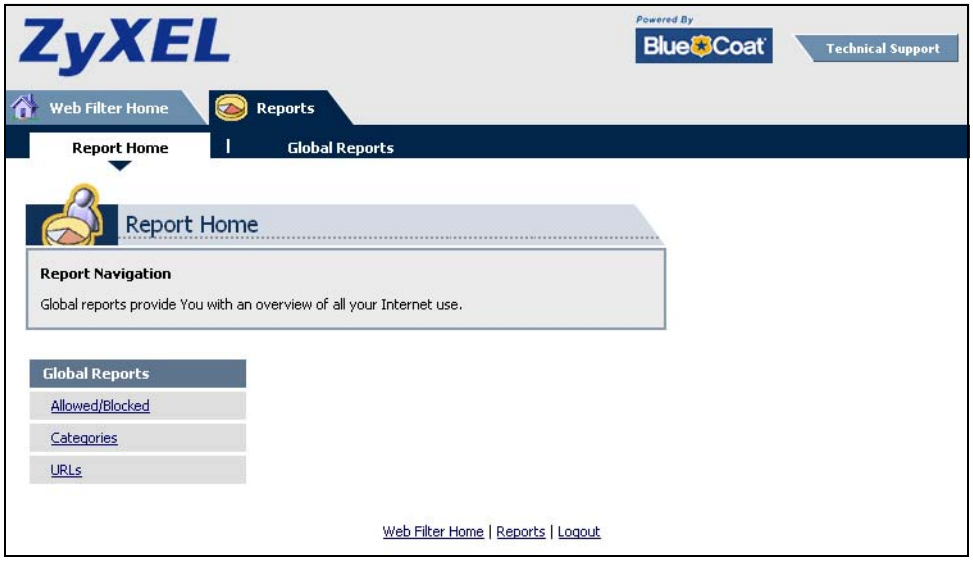

5 In the **Web Filter Home** screen, click the **Reports** tab.

**Figure 418** Content Filter Reports Main Screen



6 Select items under **Global Reports** to view the corresponding reports.

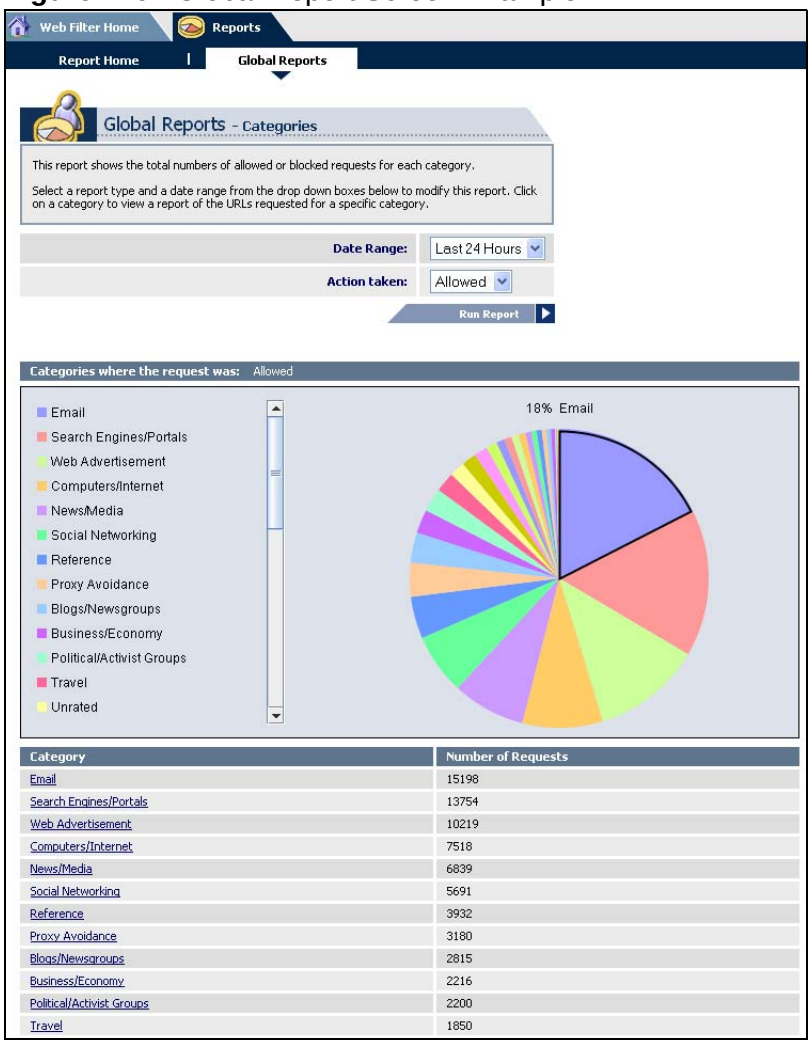
**Figure 419** Content Filter Reports: Report Home




7 Select a time period in the **Date Range** field, either **Allowed** or **Blocked** in the **Action Taken** field and a category (or enter the user name if you want to view single user reports) and click **Run Report**.The screens vary according to the report type you selected in the **Report Home** screen.

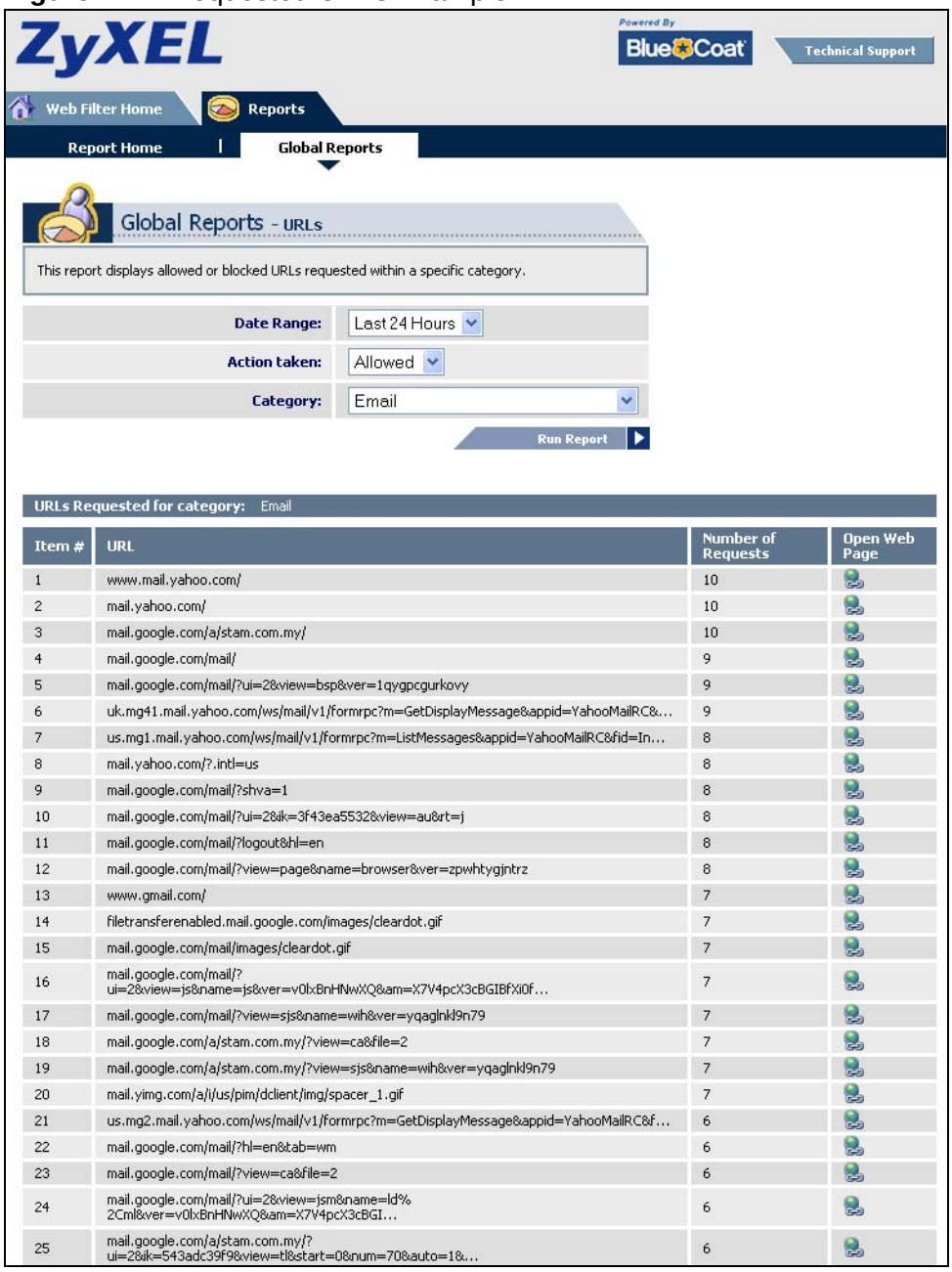
8 A chart and/or list of requested web site categories display in the lower half of the screen.

**Figure 420** Global Report Screen Example



9 You can click a category in the **Categories** report or click **URLs** in the **Report Home** screen to see the URLs that were requested.

**Figure 421** Requested URLs Example




| Item # | URL | Number of Requests | Open Web Page |
|---|---|---|---|
| 1 | www.mail.yahoo.com/ | 10 | |
| 2 | mail.yahoo.com/ | 10 | |
| 3 | mail.google.com/a/stam.com.my/ | 10 | |
| 4 | mail.google.com/mail/ | 9 | |
| 5 | mail.google.com/mail/?ui=2&view=bsp&ver=1qygpcgurkovy | 9 | |
| 6 | uk.mg41.mail.yahoo.com/ws/mail/v1/formrpc?m=GetDisplayMessage&appid=YahooMailRC&... | 9 | |
| 7 | us.mg1.mail.yahoo.com/ws/mail/v1/formrpc?m=ListMessages&appid=YahooMailRC&fid=In... | 8 | |
| 8 | mail.yahoo.com/?.intl=us | 8 | |
| 9 | mail.google.com/mail/?shva=1 | 8 | |
| 10 | mail.google.com/mail/?ui=2&ik=3f43ea5532&view=au&rt=j | 8 | |
| 11 | mail.google.com/mail/?logout&hl=en | 8 | |
| 12 | mail.google.com/mail/?view=page&name=browser&ver=zpwhtygjntrz | 8 | |
| 13 | www.gmail.com/ | 7 | |
| 14 | filetransferenabled.mail.google.com/images/cleardot.gif | 7 | |
| 15 | mail.google.com/mail/images/cleardot.gif | 7 | |
| 16 | mail.google.com/mail/?ui=2&view=js&name=js&ver=v0lxBnHNwXQ&am=X7V4pcX3cBGIBfXi0f... | 7 | |
| 17 | mail.google.com/mail/?view=sjs&name=wih&ver=yqaglnkl9n79 | 7 | |
| 18 | mail.google.com/a/stam.com.my/?view=ca&file=2 | 7 | |
| 19 | mail.google.com/a/stam.com.my/?view=sjs&name=wih&ver=yqaglnkl9n79 | 7 | |
| 20 | mail.yimg.com/a/i/us/pim/dclient/img/spacer_1.gif | 7 | |
| 21 | us.mg2.mail.yahoo.com/ws/mail/v1/formrpc?m=GetDisplayMessage&appid=YahooMailRC&f... | 6 | |
| 22 | mail.google.com/mail/?hl=en&tab=wm | 6 | |
| 23 | mail.google.com/mail/?view=ca&file=2 | 6 | |
| 24 | mail.google.com/mail/?ui=2&view=jsm&name=ld%2Cml&ver=v0lxBnHNwXQ&am=X7V4pcX3cBGI... | 6 | |
| 25 | mail.google.com/a/stam.com.my/?ui=2&ik=543adc39f9&view=tl&start=0&num=70&auto=1&... | 6 | |

# 35

# Anti-Spam

## 35.1 Overview

The anti-spam feature can mark or discard spam (unsolicited commercial or junk e-mail). Use the white list to identify legitimate e-mail. Use the black list to identify spam e-mail. The ZyWALL can also check e-mail against a DNS black list (DNSBL) of IP addresses of servers that are suspected of being used by spammers.

### 35.1.1 What You Can Do in the Anti-Spam Screens

- Use the **General** screens (Section 35.3 on page 611) to turn anti-spam on or off and manage anti-spam policies.
- Use the **Black / White List** screens (Section 35.4 on page 615) to set up a black list to identify spam and a white list to identify legitimate e-mail.
- Use the **DNSBL** screens (Section 35.6 on page 620) to have the ZyWALL check e-mail against DNS Black Lists.
- Use the **Status** screen (Section 35.6 on page 620) to see how many mail sessions the ZyWALL is currently checking and DNSBL statistics.

### 35.1.2 What You Need to Know About Anti-Spam

#### White list

Configure white list entries to identify legitimate e-mail. The white list entries have the ZyWALL classify any e-mail that is from a specified sender or uses a specified header field and header value as being legitimate (see E-mail Headers on page 610 for more on mail headers). The anti-spam feature checks an e-mail against the white list entries before doing any other anti-spam checking. If the e-mail matches a white list entry, the ZyWALL classifies the e-mail as legitimate and does not perform any more anti-spam checking on that individual e-mail. A properly configured white list helps keep important e-mail from being incorrectly classified as spam. The white list can also increases the ZyWALL's anti-spam speed and efficiency by not having the ZyWALL perform the full anti-spam checking process on legitimate e-mail.

### Black List

Configure black list entries to identify spam. The black list entries have the ZyWALL classify any e-mail that is from or forwarded by a specified IP address or uses a specified header field and header value as being spam. If an e-mail does not match any of the white list entries, the ZyWALL checks it against the black list entries. The ZyWALL classifies an e-mail that matches a black list entry as spam and immediately takes the configured action for dealing with spam. If an e-mail matches a blacklist entry, the ZyWALL does not perform any more anti-spam checking on that individual e-mail. A properly configured black list helps catch spam e-mail and increases the ZyWALL's anti-spam speed and efficiency.

### SMTP and POP3

Simple Mail Transfer Protocol (SMTP) is the Internet's message transport standard. It controls the sending of e-mail messages between servers. E-mail clients (also called e-mail applications) then use mail server protocols such as POP (Post Office Protocol) or IMAP (Internet Message Access Protocol) to retrieve e-mail. E-mail clients also generally use SMTP to send messages to a mail server. The older POP2 requires SMTP for sending messages while the newer POP3 can be used with or without it. This is why many e-mail applications require you to specify both the SMTP server and the POP or IMAP server (even though they may actually be the same server).

The ZyWALL's anti-spam feature checks SMTP (TCP port 25) and POP3 (TCP port 110) e-mails. The anti-spam feature does not check (or act upon) e-mails that use other protocols (such as IMAP) or other port numbers.

### E-mail Headers

Every email has a header and a body. The header is structured into fields and includes the addresses of the recipient and sender, the subject, and other information about the e-mail and its journey. The body is the actual message text and any attachments. You can have the ZyWALL check for specific header fields with specific values.

E-mail programs usually only show you the To:, From:, Subject:, and Date: header fields but there are others such as Received: and Content-Type:. To see all of an e-mail's header, you can select an e-mail in your e-mail program and look at its properties or details. For example, in Microsoft's Outlook Express, select a mail and click **File > Properties > Details**. This displays the e-mail's header. Click **Message Source** to see the source for the entire mail including both the header and the body.

### E-mail Header Buffer Size

The ZyWALL has a 5 K buffer for an individual e-mail header. If an e-mail's header is longer than 5 K, the ZyWALL only checks up to the first 5 K.

### DNSBL

A DNS Black List (DNSBL) is a server that hosts a list of IP addresses known or suspected of having sent or forwarded spam. A DNSBL is also known as a DNS spam blocking list. The ZyWALL can check the routing addresses of e-mail against DNSBLs and classify an e-mail as spam if it was sent or forwarded by a computer with an IP address in the DNSBL.

### Finding Out More

See Section 35.8 on page 623 for more background information on anti-spam.

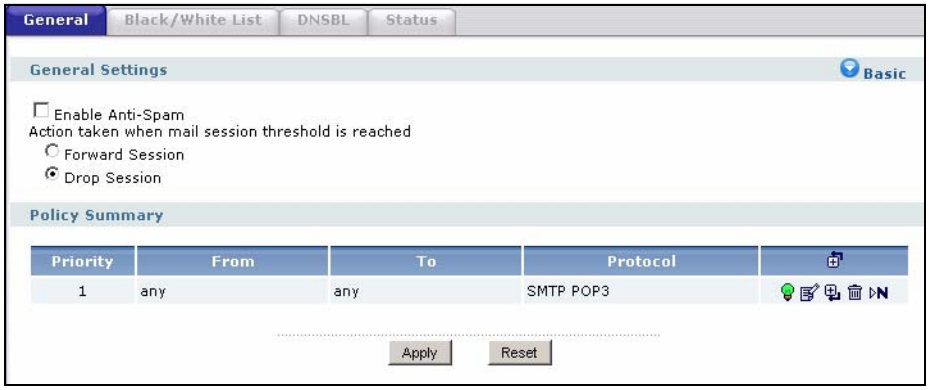
## 35.2 Before You Begin

Configure your zones before you configure anti-spam.

## 35.3 The Anti-Spam General Screen

Click **Anti-X** > **Anti-Spam** to open the **Anti-Spam General** screen. Use this screen to turn the anti-spam feature on or off and manage anti-spam policies. You can also select the action the ZyWALL takes when the mail sessions threshold is reached.

**Figure 422** Anti-X > Anti-Spam > General



The following table describes the labels in this screen.

**Table 184** Anti-X > Anti-Spam > General

| LABEL | DESCRIPTION |
|---|---|
| General Settings | Click **Advanced** to display more settings. Click **Basic** to display fewer settings. |
| Enable Anti-Spam | Select this check box to check SMTP (TCP port 25) and POP3 (TCP port 110) traffic for spam e-mail. |
| Action taken when mail sessions threshold is reached | An e-mail session is when an e-mail client and e-mail server (or two e-mail servers) connect through the ZyWALL. Select how to handle concurrent e-mail sessions that exceed the maximum number of concurrent e-mail sessions that the anti-spam feature can handle. See the chapter of product specifications for the threshold.<br>Select **Forward Session** to have the ZyWALL allow the excess e-mail sessions without any spam filtering.<br>Select **Drop** to have the ZyWALL drop mail connections to stop the excess e-mail sessions. The e-mail client or server will have to re-attempt to send or receive e-mail later when the number of e-mail sessions is under the threshold. |
| Policy Summary | |
| Priority | This is the position of an anti-spam policy in the list. The ordering of your anti-spam policies is important as the ZyWALL applies them in sequence. Once traffic matches an anti-spam policy, the ZyWALL applies that policy and does not check the traffic against any more policies. |
| From | The anti-spam policy has the ZyWALL scan e-mail traffic that is coming from this zone and going to the **To** zone. |
| To | The anti-spam policy has the ZyWALL scan e-mail traffic that is going to this zone from the **From** zone. |
| Protocol | These are the protocols of traffic to scan for spam.<br>**SMTP** applies to traffic using TCP port 25.<br>**POP3** applies to traffic using TCP port 110. |

**Table 184** Anti-X > Anti-Spam > General

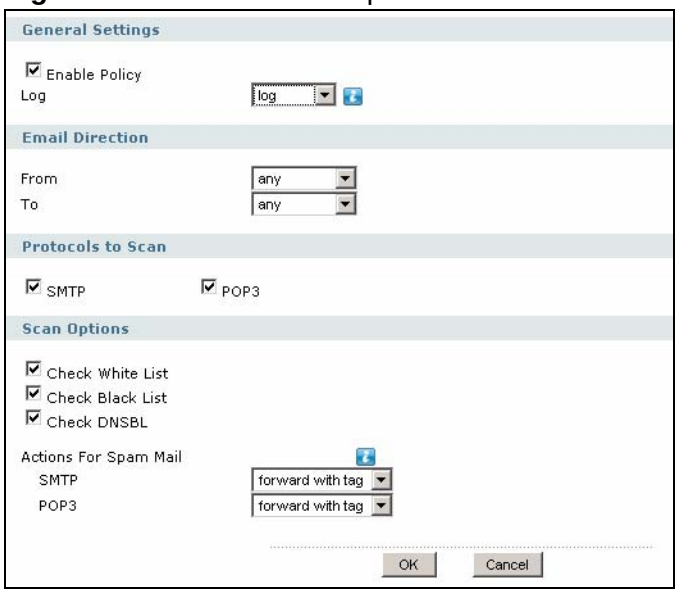
| LABEL | DESCRIPTION |
|---|---|
| Add icon | Click the **Add** icon in the heading row to add a new first entry.<br><br>The **Active** displays whether the entry is enabled or not. Click it to activate or deactivate the entry. Make sure you click **Apply** to save and apply the change.<br><br>Click the **Edit** icon to go to the screen where you can edit the entry on the ZyWALL.<br><br>Click the **Add** icon in an entry to add an entry below the current entry.<br><br>Click the **Remove** icon to delete an existing entry from the ZyWALL. A window displays asking you to confirm that you want to delete the entry. Note that subsequent entries move up by one when you take this action.<br><br>In a numbered list, click the **Move to N** icon to display a field to type an index number for where you want to put that entry and press [ENTER] to move the entry to the number that you typed. For example, if you type 6, the entry you are moving becomes number 6 and the previous rule 6 (if there is one) gets pushed up (or down) one.<br><br>The ordering of your policies is important as they are applied in order of their numbering. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 35.3.1 The Anti-Spam Policy Add or Edit Screen

Click the **Add** or **Edit** icon in the **Anti-X** > **Anti-Spam > General** screen to display the configuration screen as shown next. Use this screen to configure an anti-spam policy that controls what traffic direction of e-mail to check, which e-

mail protocols to scan, the scanning options, and the action to take on spam traffic.

**Figure 423** Anti-X > Anti-Spam > General > Add




The following table describes the labels in this screen.

**Table 185** Anti-X > Anti-Virus > General > Add

| LABEL | DESCRIPTION |
|---|---|
| Enable Policy | Select this check box to have the ZyWALL apply this anti-spam policy to check e-mail traffic for spam. |
| Log | Select how the ZyWALL is to log the event when the DNSBL times out or an e-mail matches the white list, black list, or DNSBL.<br>**no**: Do not create a log.<br>**log**: Create a log on the ZyWALL.<br>**log alert**: An alert is an e-mailed log for more serious events that may need more immediate attention. Select this option to have the ZyWALL send an alert. |
| From<br>To | Select source and destination zones for traffic to scan for spam. The anti-spam policy has the ZyWALL scan traffic coming from the **From** zone and going to the **To** zone. |
| Protocols to Scan | Select which protocols of traffic to scan for spam.<br>**SMTP** applies to traffic using TCP port 25.<br>**POP3** applies to traffic using TCP port 110. |
| Check White List | Select this check box to check e-mail against the white list. The ZyWALL classifies e-mail that matches a white list entry as legitimate (not spam). |
| Check Black List | Select this check box to check e-mail against the black list. The ZyWALL classifies e-mail that matches a black list entry as spam. |

**Table 185** Anti-X > Anti-Virus > General > Add (continued)

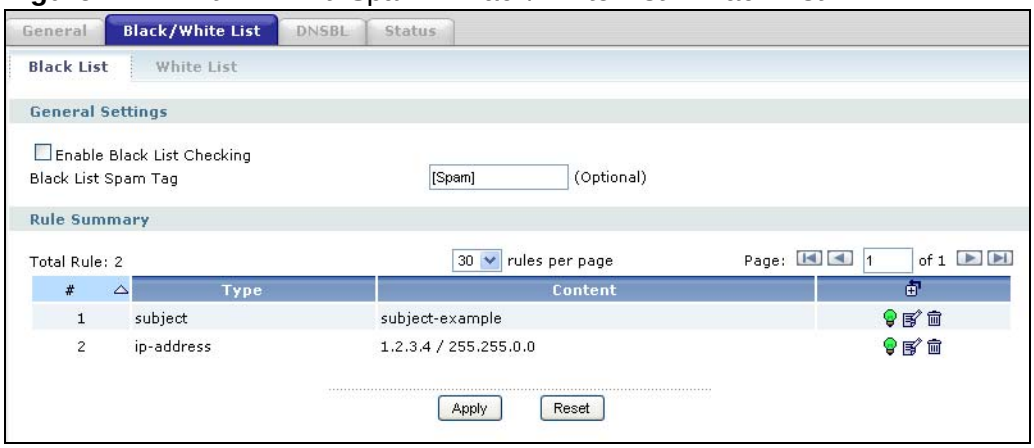
| LABEL | DESCRIPTION |
|---|---|
| Check DNSBL | Select this check box to check e-mail against the ZyWALL's configured DNSBL domains. The ZyWALL classifies e-mail that matches a DNS black list as spam. |
| Actions for Spam Mail | Use this section to set how the ZyWALL is to handle spam mail. |
| SMTP | Select how the ZyWALL is to handle spam SMTP mail.<br>Select **drop** to discard spam SMTP mail.<br>Select **forward** to allow spam SMTP mail to go through.<br>Select **forward with tag** to add a spam tag to an SMTP spam mail's mail subject and send it on to the destination. |
| POP3 | Select how the ZyWALL is to handle spam POP3 mail.<br>Select **forward** to allow spam POP3 mail to go through.<br>Select **forward with tag** to add a spam tag to an POP3 spam mail's mail subject and send it on to the destination. |
| OK | Click **OK** to save your changes. |
| Cancel | Click **Cancel** to exit this screen without saving your changes. |

# 35.4 The Anti-Spam Black List Screen

Click **Anti-X** > **Anti-Spam > Black /White List** to display the **Anti-Spam Black List** screen.

Configure the black list to identify spam e-mail. You can create black list entries based on the sender's or relay server's IP address or e-mail address. You can also create entries that check for particular e-mail header fields with specific values or specific subject text. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

**Figure 424** Anti-X > Anti-Spam > Black/White List > Black List



The following table describes the labels in this screen.

**Table 186** Anti-X > Anti-Spam > Black/White List > Black List

| LABEL | DESCRIPTION |
|---|---|
| General Settings | |
| Enable Black List Checking | Select this check box to have the ZyWALL treat e-mail that matches (an active) black list entry as spam. |
| Black List Spam Tag | Enter a message or label (up to 15 ASCII characters) to add to the mail subject of e-mails that match the ZyWALL's spam black list. |
| Total Rule | This is the number of entries configured. |
| rules per page | Select how many entries you want to display on each page. |
| Page x of x | This is the number of the page of entries currently displayed and the total number of pages of entries. Type a page number to go to or use the arrows to navigate the pages of entries. |
| # | This is the entry's index number in the list. |
| Type | This field displays whether the entry is based on the e-mail's subject, source or relay IP address, source e-mail address, or header. |
| Content | This field displays the subject content, source or relay IP address, source e-mail address, or header value for which the entry checks. |
| Add icon | This column provides icons to add, activate / deactivate, edit, and remove entries.<br>To add an entry, click the **Add** icon at the top of the column.<br>Click an entry's **Active** icon to activate or deactivate the entry. Make sure you click **Apply** to save and apply the change.<br>Click an entry's **Edit** icon to edit the entry.<br>To delete an entry, click the entry's **Remove** icon. The Web Configurator confirms that you want to delete the entry. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

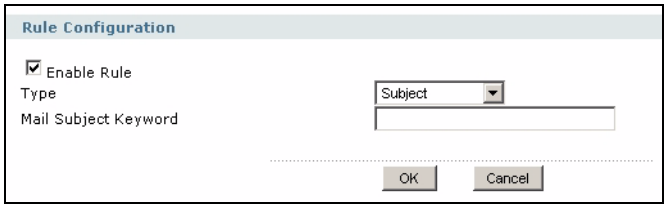
## 35.4.1 The Anti-Spam Black or White List Add/Edit Screen

In the anti-spam **Black List** or **White List** screen, click the **Add** icon or an **Edit** icon to display the following screen.

Use this screen to configure an anti-spam black list entry to identify spam e-mail. You can create entries based on specific subject text, or the sender's or relay's IP

address or e-mail address. You can also create entries that check for particular header fields and values.

**Figure 425** Anti-X > Anti-Spam > Black/White List > Black List (or White List) > Add




The following table describes the labels in this screen.

**Table 187** Anti-X > Anti-Spam > Black/White List > Black List (or White List) > Add

| LABEL | DESCRIPTION |
|---|---|
| Enable Rule | Select this to have the ZyWALL use this entry as part of the black or white list.<br><br>To actually use the entry, you must also turn on the use of the list in the corresponding list screen, enable the anti-spam feature in the anti-spam general screen, and configure an anti-spam policy to use the list. |
| Type | Use this field to base the entry on the e-mail's subject, source or relay IP address, source e-mail address, or header.<br><br>Select **Subject** to have the ZyWALL check e-mail for specific content in the subject line.<br><br>Select **IP Address** to have the ZyWALL check e-mail for a specific source or relay IP address.<br><br>Select **E-Mail Address** to have the ZyWALL check e-mail for a specific source e-mail address or domain name.<br><br>Select **Mail Header** to have the ZyWALL check e-mail for specific header fields and values. Configure black list header entries to check for e-mail from bulk mail programs or with content commonly used in spam. Configure white list header entries to allow certain header values that identify the e-mail as being from a trusted source. |
| Mail Subject Keyword | This field displays when you select the **Subject** type. Enter up to 63 ASCII characters of text to check for in e-mail headers. Spaces are not allowed, although you could substitute a question mark (?). See Section 35.4.2 on page 618 for more details. |
| Sender or Mail Relay IP Address | This field displays when you select the **IP** type. Enter an IP address in dotted decimal notation. |
| Netmask | This field displays when you select the **IP** type. Enter the subnet mask here, if applicable. |
| Sender E-Mail Address | This field displays when you select the **E-Mail** type. Enter a keyword (up to 63 ASCII characters). See Section 35.4.2 on page 618 for more details. |

**Table 187** Anti-X > Anti-Spam > Black/White List > Black List (or White List) > Add

| LABEL | DESCRIPTION |
|---|---|
| Mail Header Field Name | This field displays when you select the **Mail Header** type.<br>Type the name part of an e-mail header (the part that comes before the colon). Use up to 63 ASCII characters.<br>For example, if you want the entry to check the “Received:” header for a specific mail server’s domain, enter “Received” here. |
| Field Value Keyword | This field displays when you select the **Mail Header** type.<br>Type the value part of an e-mail header (the part that comes after the colon). Use up to 63 ASCII characters.<br>For example, if you want the entry to check the “Received:” header for a specific mail server’s domain, enter the mail server’s domain here.<br>See Section 35.4.2 on page 618 for more details. |
| OK | Click **OK** to save your changes. |
| Cancel | Click **Cancel** to exit this screen without saving your changes. |

## 35.4.2 Regular Expressions in Black or White List Entries

The following applies for a black or white list entry based on an e-mail subject, e-mail address, or e-mail header value.

- Use a question mark (?) to let a single character vary. For example, use “a?c” (without the quotation marks) to specify abc, acc and so on.
- You can also use a wildcard (*). For example, if you configure *def.com, any e-mail address that ends in def.com matches. So “mail.def.com” matches.
- The wildcard can be anywhere in the text string and you can use more than one wildcard. You cannot use two wildcards side by side, there must be other characters between them.
- The ZyWALL checks the first header with the name you specified in the entry. So if the e-mail has more than one “Received” header, the ZyWALL checks the first one.

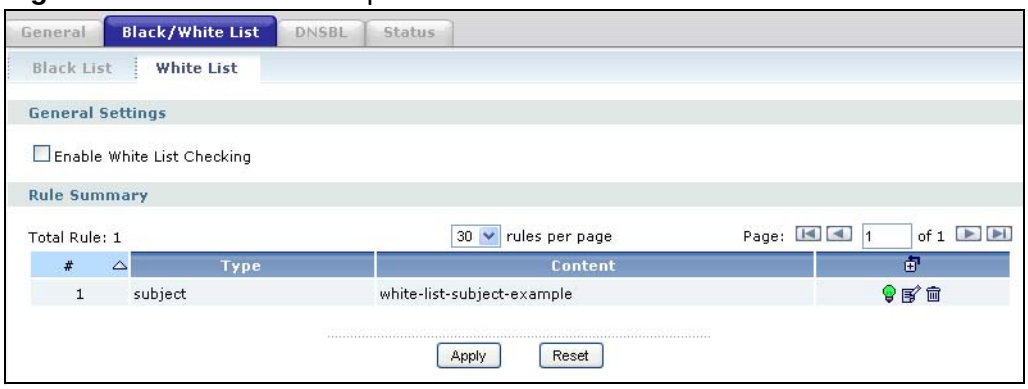
# 35.5 The Anti-Spam White List Screen

Click **Anti-X** > **Anti-Spam > Black/White List** and then the **White List** tab to display the **Anti-Spam White List** screen.

Configure the white list to identify legitimate e-mail. You can create white list entries based on the sender’s or relay’s IP address or e-mail address. You can also

create entries that check for particular header fields and values or specific subject text.

**Figure 426** Anti-X > Anti-Spam > Black/White List > White List




The following table describes the labels in this screen.

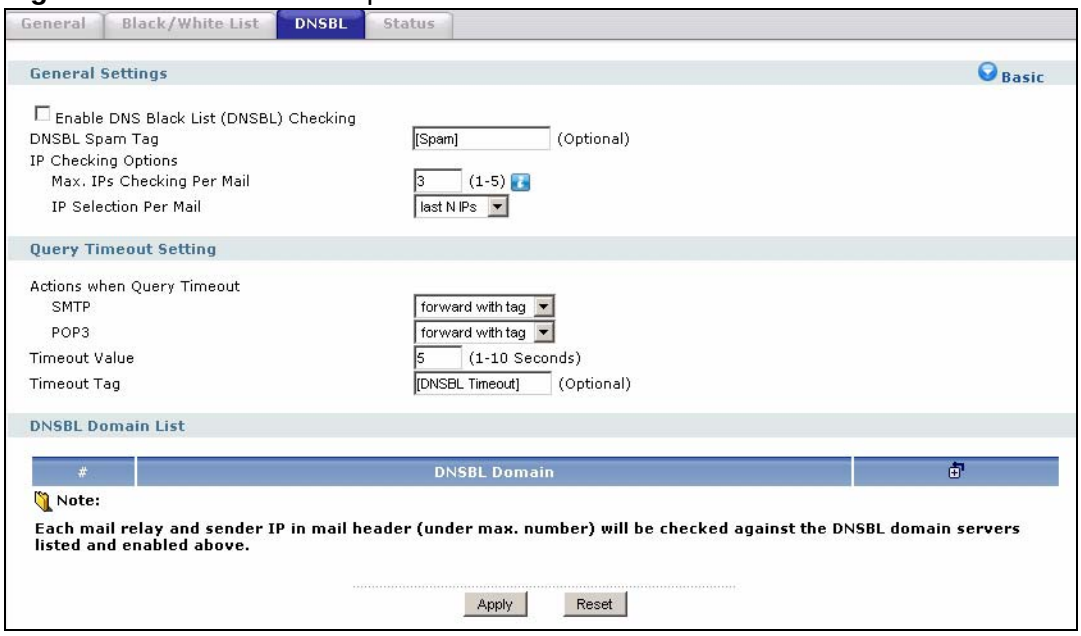
**Table 188** Anti-X > Anti-Spam > Black/White List > White List

| LABEL | DESCRIPTION |
|---|---|
| General Settings | |
| Enable White List Checking | Select this check box to have the ZyWALL forward e-mail that matches (an active) white list entry without doing any more anti-spam checking on that individual e-mail. |
| Total Rule | This is the number of entries configured. |
| rules per page | Select how many entries you want to display on each page. |
| Page x of x | This is the number of the page of entries currently displayed and the total number of pages of entries. Type a page number to go to or use the arrows to navigate the pages of entries. |
| # | This is the entry's index number in the list. |
| Type | This field displays whether the entry is based on the e-mail's subject, source or relay IP address, source e-mail address, or a header. |
| Content | This field displays the subject content, source or relay IP address, source e-mail address, or header value for which the entry checks. |
| Add icon | This column provides icons to add, activate / deactivate, edit, and remove entries.<br><br>To add an entry, click the **Add** icon at the top of the column. See Section 35.4.1 on page 616 for how to add or edit an entry.<br><br>Click an entry's **Active** icon to activate or deactivate the entry. Make sure you click **Apply** to save and apply the change.<br><br>Click an entry's **Edit** icon to edit the entry. See Section 35.4.1 on page 616 for how to add or edit an entry.<br><br>To delete an entry, click the entry's **Remove** icon. The Web Configurator confirms that you want to delete the entry. |
| OK | Click **OK** to save your changes. |
| Cancel | Click **Cancel** to exit this screen without saving your changes. |

# 35.6 The DNSBL Screen

Click **Anti-X** > **Anti-Spam > DNSBL** to display the anti-spam **DNSBL** screen. Use this screen to configure the ZyWALL to check the sender and relay IP addresses in e-mail headers against DNS (Domain Name Service)-based spam Black Lists (DNSBLs).

**Figure 427** Anti-X > Anti-Spam > DNSBL




The following table describes the labels in this screen.

**Table 189** Anti-X > Anti-Spam > DNSBL

| LABEL | DESCRIPTION |
|---|---|
| Enable DNS Black List (DNSBL) Checking | Select this to have the ZyWALL check the sender and relay IP addresses in e-mail headers against the DNSBL servers maintained by the DNSBL domains listed in the ZyWALL. |
| DNSBL Spam Tag | Enter a message or label (up to 15 ASCII characters) to add to the beginning of the mail subject of e-mails that have a sender or relay IP address in the header that matches a black list maintained by one of the DNSBL domains listed in the ZyWALL.<br><br>This tag is only added if the anti-spam policy is configured to forward spam mail with a spam tag. |
| Max. IPs Checking Per Mail | Set up to how many sender and relay server IP addresses in the mail header to check against the DNSBL. |
| IP Selection Per Mail | Select **first N IPs** to have the ZyWALL start checking from the first IP address in the mail header. This is the IP of the sender or the first server that forwarded the mail.<br><br>Select **last N IPs** to have the ZyWALL start checking from the last IP address in the mail header. This is the IP of the last server that forwarded the mail. |

**Table 189** Anti-X > Anti-Spam > DNSBL (continued)

| LABEL | DESCRIPTION |
|---|---|
| Actions when Query Timeout | Use this section to set what the ZyWALL does if the queries to the DNSBL domains time out. |
| SMTP | Select how the ZyWALL is to handle SMTP mail (mail going to an e-mail server) if the queries to the DNSBL domains time out.<br>Select **drop** to discard SMTP mail.<br>Select **forward** to allow SMTP mail to go through.<br>Select **forward with tag** to add a DNSBL timeout tag to the mail subject of an SMTP mail and send it. |
| POP3 | Select how the ZyWALL is to handle POP3 mail (mail coming to an e-mail client) if the queries to the DNSBL domains time out.<br>Select **forward** to allow POP3 mail to go through.<br>Select **forward with tag** to add a DNSBL timeout tag to the mail subject of an POP3 mail and send it. |
| Timeout Value | Set how long the ZyWALL waits for a reply from the DNSBL domains listed below. If there is no reply before this time period expires, the ZyWALL takes the action defined in the relevant **Actions when Query Timeout** field. |
| Timeout Tag | Enter a message or label (up to 15 ASCII characters) to add to the mail subject of e-mails that the ZyWALL forwards if queries to the DNSBL domains time out. |
| # | This is the entry's index number in the list. |
| DNSBL Domain | This is the name of a domain that maintains DNSBL servers. |
| Add icon | This column provides icons to add, activate / deactivate, edit, and remove entries.<br>To add an entry, click the **Add** icon at the top of the column.<br>Click an entry's **Active** icon to activate or deactivate the entry. Make sure you click **Apply** to save and apply the change.<br>Click an entry's **Edit** icon to edit the entry.<br>To delete an entry, click the entry's **Remove** icon. The Web Configurator confirms that you want to delete the entry. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

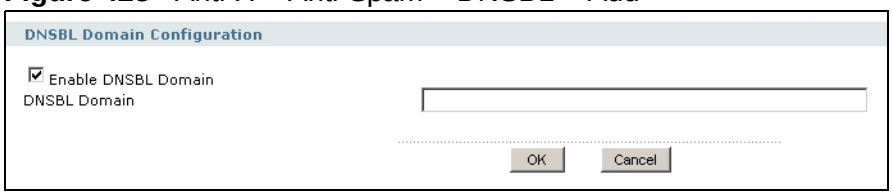
## 35.6.1 The DNSBL Add/Edit Screen

Click the **Add** or **Edit** icon in the **Anti-X** > **Anti-Spam > DNSBL** screen to display the configuration screen as shown next.

Use this screen to specify a DNSBL (spam IP address black list). You need to enter the name of a domain that maintains DNSBL servers.

For the best anti-spam performance, use only the most accurate DNSBLs that you can. Adding other (less accurate) DNSBL domains can decrease the anti-spam performance. Some DNSBLs are more effective than others. You want the DNSBLs that catch as much spam as possible while avoiding false positives (identifying legitimate e-mail as spam). Different DNSBLs also have different usage policies. For example, you can check http://www.spamhaus.org or https://www.sorbs.net for more information.

**Figure 428** Anti-X > Anti-Spam > DNSBL > Add




The following table describes the labels in this screen.

**Table 190** Anti-X > Anti-Spam > DNSBL > Add

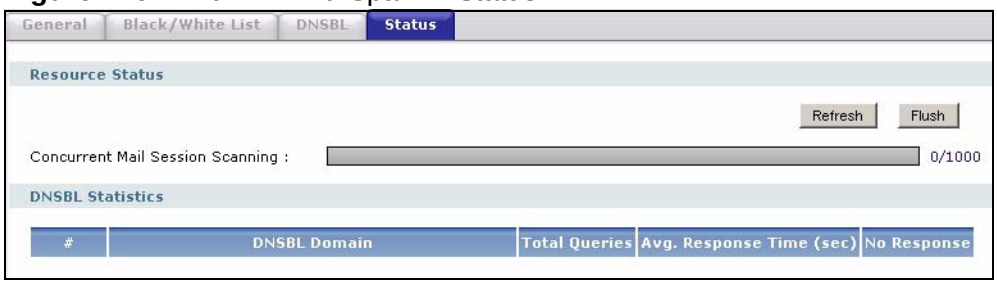
| LABEL | DESCRIPTION |
|---|---|
| General Settings | |
| Enable DNSBL Domain | Select this check box to have the ZyWALL check the sender and relay IP addresses in e-mails against this DNSBL. |
| DNSBL Domain | Enter the domain that is maintaining a DNSBL. |
| OK | Click **OK** to save your changes. |
| Cancel | Click **Cancel** to exit this screen without saving your changes. |

# 35.7 The Anti-Spam Status Screen

Click **Anti-X** > **Anti-Spam > Status** to display the **Anti-Spam Status** screen.

Use the **Anti-Spam Status** screen to see how many e-mail sessions the anti-spam feature is scanning and statistics for the DNSBLs.

**Figure 429** Anti-X > Anti-Spam > Status



The following table describes the labels in this screen.

**Table 191** Anti-X > Anti-Spam > Status

| LABEL | DESCRIPTION |
|---|---|
| Refresh | Click this button to update the information displayed on this screen. |
| Flush | Click this button to clear the DNSBL statistics. This also clears the concurrent mail session scanning bar's historical high. |
| Concurrent Mail Session Scanning | The darker shaded part of the bar shows how much of the ZyWALL's total spam checking capability is currently being used.<br>The lighter shaded part of the bar and the pop-up show the historical high.<br>The first number to the right of the bar is how many e-mail sessions the ZyWALL is presently checking for spam. The second number is the maximum number of e-mail sessions that the ZyWALL can check at once. An e-mail session is when an e-mail client and e-mail server (or two e-mail servers) connect through the ZyWALL. |
| DNSBL Statistics | These are the statistics for the DNSBL the ZyWALL uses. These statistics are for when the ZyWALL actually queries the DNSBL servers. Matches for DNSBL responses stored in the cache do not affect these statistics. |
| # | This is the entry's index number in the list. |
| DNSBL Domain | These are the DNSBLs the ZyWALL uses to check sender and relay IP addresses in e-mails. |
| Total Queries | This is the total number of DNS queries the ZyWALL has sent to this DNSBL. |
| Avg. Response Time (sec) | This is the average for how long it takes to receive a reply from this DNSBL. |
| No Response | This is how many DNS queries the ZyWALL sent to this DNSBL without receiving a reply. |

# 35.8 Anti-Spam Technical Reference

Here is more detailed anti-spam information.

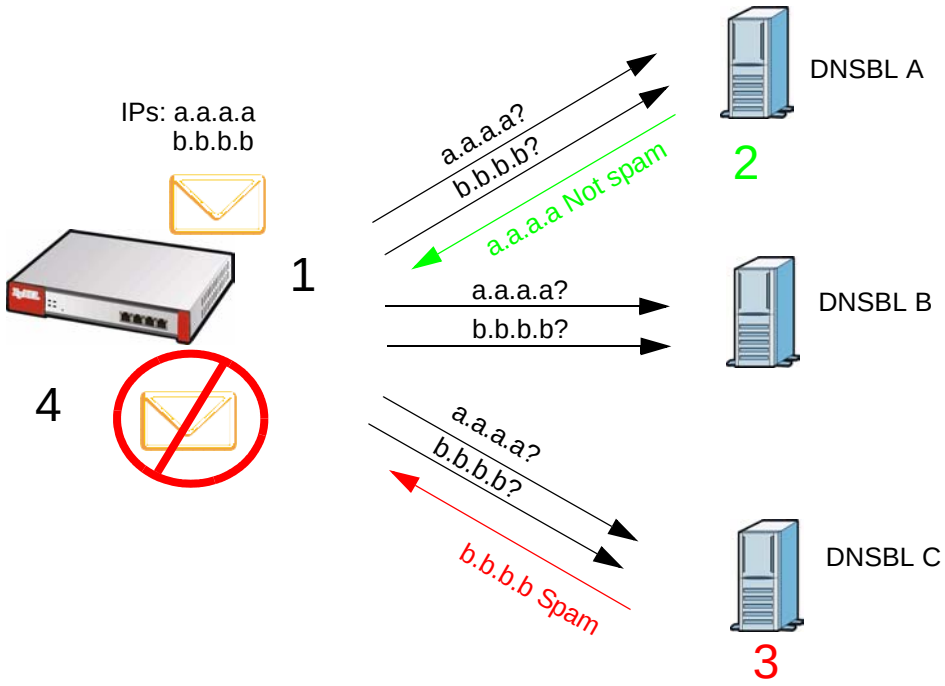
### DNSBL

- The ZyWALL checks only public sender and relay IP addresses, it does not check private IP addresses.
- The ZyWALL sends a separate query (DNS lookup) for each sender or relay IP address in the e-mail's header to each of the ZyWALL's DNSBL domains at the same time.
- The DNSBL servers send replies as to whether or not each IP address matches an entry in their list. Each IP address has a separate reply.

- As long as the replies are indicating the IP addresses do not match entries on the DNSBL lists, the ZyWALL waits until it receives at least one reply for each IP address.
- If the ZyWALL receives a DNSBL reply that one of the IP addresses is in the DNSBL list, the ZyWALL immediately classifies the e-mail as spam and takes the anti-spam policy's configured action for spam. The ZyWALL does not wait for any more DNSBL replies.
- If the ZyWALL receives at least one non-spam reply for each of an e-mail's routing IP addresses, the ZyWALL immediately classifies the e-mail as legitimate and forwards it.
- Any further DNSBL replies that come after the ZyWALL classifies an e-mail as spam or legitimate have no effect.
- The ZyWALL records DNSBL responses for IP addresses in a cache for up to 72 hours. The ZyWALL checks an e-mail's sender and relay IP addresses against the cache first and only sends DNSBL queries for IP addresses that are not in the cache.

Here is an example of an e-mail classified as spam based on DNSBL replies.

**Figure 430** DNSBL Spam Detection Example




**1** The ZyWALL receives an e-mail that was sent from IP address a.a.a.a and relayed by an e-mail server at IP address b.b.b.b. The ZyWALL sends a separate query to each of its DNSBL domains for IP address a.a.a.a. The ZyWALL sends another separate query to each of its DNSBL domains for IP address b.b.b.b.

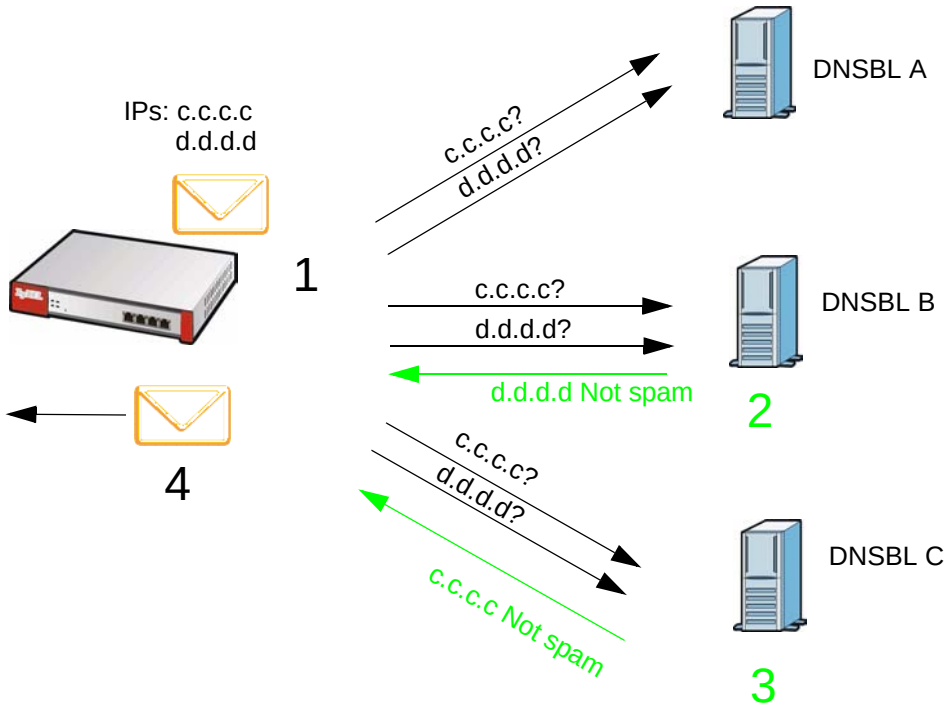
**2** DNSBL A replies that IP address a.a.a.a does not match any entries in its list (not spam).

3 DNSBL C replies that IP address b.b.b.b matches an entry in its list.

4 The ZyWALL immediately classifies the e-mail as spam and takes the action for spam that you defined in the anti-spam policy. In this example it was an SMTP mail and the defined action was to drop the mail. The ZyWALL does not wait for any more DNSBL replies.

Here is an example of an e-mail classified as legitimate based on DNSBL replies.

**Figure 431** DNSBL Legitimate E-mail Detection Example




1 The ZyWALL receives an e-mail that was sent from IP address c.c.c.c and relayed by an e-mail server at IP address d.d.d.d. The ZyWALL sends a separate query to each of its DNSBL domains for IP address c.c.c.c. The ZyWALL sends another separate query to each of its DNSBL domains for IP address d.d.d.d.

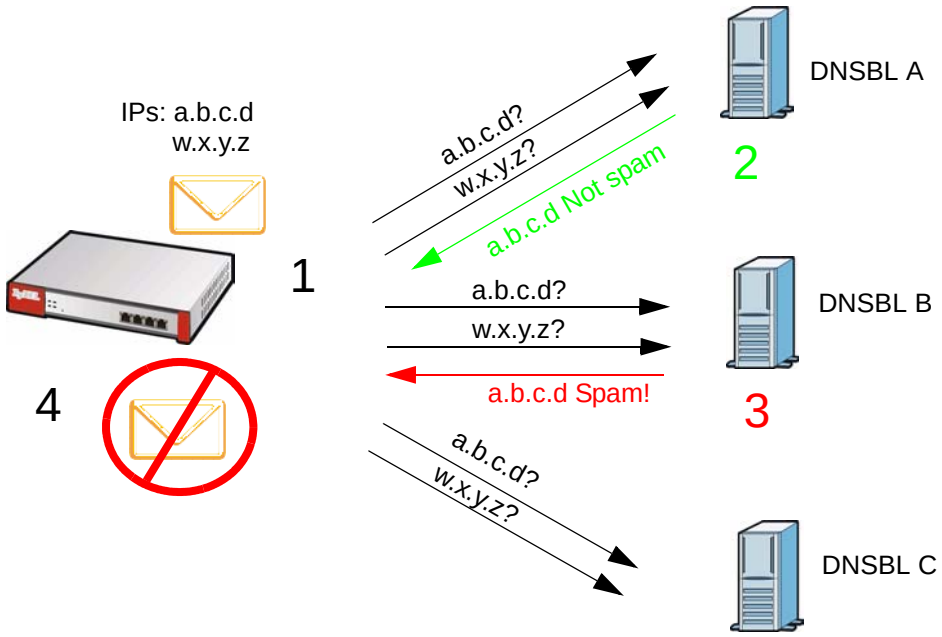
2 DNSBL B replies that IP address d.d.d.d does not match any entries in its list (not spam).

3 DNSBL C replies that IP address c.c.c.c does not match any entries in its list (not spam).

4 Now that the ZyWALL has received at least one non-spam reply for each of the e-mail's routing IP addresses, the ZyWALL immediately classifies the e-mail as legitimate and forwards it. The ZyWALL does not wait for any more DNSBL replies.

If the ZyWALL receives conflicting DNSBL replies for an e-mail routing IP address, the ZyWALL classifies the e-mail as spam. Here is an example.

**Figure 432** Conflicting DNSBL Replies Example




1 The ZyWALL receives an e-mail that was sent from IP address a.b.c.d and relayed by an e-mail server at IP address w.x.y.z. The ZyWALL sends a separate query to each of its DNSBL domains for IP address a.b.c.d. The ZyWALL sends another separate query to each of its DNSBL domains for IP address w.x.y.z.

2 DNSBL A replies that IP address a.b.c.d does not match any entries in its list (not spam).

3 While waiting for a DNSBL reply about IP address w.x.y.z, the ZyWALL receives a reply from DNSBL B saying IP address a.b.c.d is in its list.

4 The ZyWALL immediately classifies the e-mail as spam and takes the action for spam that you defined in the anti-spam policy. In this example it was an SMTP mail and the defined action was to drop the mail. The ZyWALL does not wait for any more DNSBL replies.

# PART VII
# Device HA

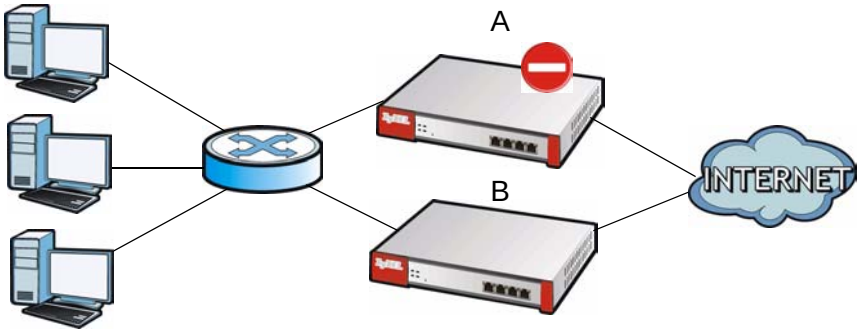
# 36

# Device HA

## 36.1 Overview

Device HA lets a backup ZyWALL (**B**) automatically take over if a master ZyWALL (**A**) fails.

**Figure 433** Device HA Backup Taking Over for the Master




### 36.1.1 What You Can Do in the Device HA Screens

- Use the **General** screen (Section 36.2 on page 631) to configure device HA global settings, and see the status of each interface monitored by device HA.
- Use the **Active-Passive Mode** screens (Section 36.3 on page 632) to use active-passive mode device HA. You can configure general active-passive mode device HA settings, view and manage the list of monitored interfaces, and synchronize backup ZyWALLs.
- Use the **Legacy Mode** screens (Section 36.5 on page 638) to use legacy mode device HA. You can configure general legacy mode HA settings including link monitoring, configure the VRRP group settings and synchronize backup ZyWALLs.

### 36.1.2 What You Need to Know About Device HA

#### Active-Passive Mode and Legacy Mode

- Active-passive mode lets a backup ZyWALL take over if the master ZyWALL fails.

- Legacy mode allows for more complex relationships between the master and backup ZyWALLs, such as active-active or using different ZyWALLs as the master ZyWALL for individual interfaces. Legacy mode configuration involves a greater degree of complexity. Active-passive mode is recommended for general failover deployments.
- The ZyWALLs must all support and be set to use the same device HA mode (either active-passive or legacy).

### Management Access

You can configure a separate management IP address for each interface. You can use it to access the ZyWALL for management whether the ZyWALL is the master or a backup. The management IP address should be in the same subnet as the interface IP address.

### Synchronization

Use synchronization to have a backup ZyWALL copy the master ZyWALL's configuration, signatures (anti-virus, IDP/application patrol, and system protect), and certificates.

Note: Only ZyWALLs of the same model and firmware version can synchronize.

Otherwise you must manually configure the master ZyWALL's settings on the backup (by editing copies of the configuration files in a text editor for example).

### Finding Out More

- See Section 5.4.8 on page 89 for related information on these screens.
- See Section 36.7 on page 643 for device HA background/technical information.
- See Section 6.9 on page 140 for an example of using device HA.

## 36.1.3 Before You Begin

- Configure a static IP address for each interface that you will have device HA monitor.

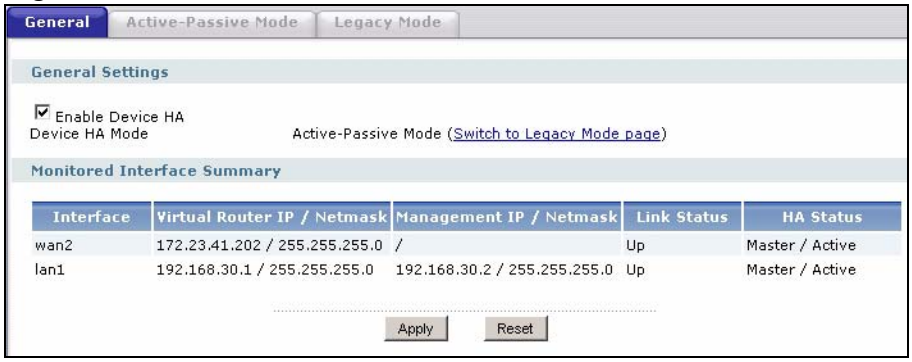
Note: Subscribe to services on the backup ZyWALL before synchronizing it with the master ZyWALL.

- Synchronization includes updates for services to which the master and backup ZyWALLs are both subscribed. For example, a backup subscribed to IDP/AppPatrol, but not anti-virus, gets IDP/AppPatrol updates from the master, but not anti-virus updates. It is highly recommended to subscribe the master and backup ZyWALLs to the same services.

# 36.2 Device HA General

The **Device HA General** screen lets you enable or disable device HA, and displays which device HA mode the ZyWALL is set to use along with a summary of the monitored interfaces.

**Figure 434** Device HA > General




The following table describes the labels in this screen.

**Table 192** Device HA > General

| LABEL | DESCRIPTION |
|---|---|
| Enable Device HA | Turn the ZyWALL's device HA feature on or off. |
| Device HA Mode | This displays whether the ZyWALL is currently set to use active-passive mode device HA or legacy mode device HA. Active-passive mode is recommended for general device failover deployments. Only use legacy mode if you need a more complex relationship between the master and backup ZyWALLs, such as active-active or using different ZyWALLs as the master for individual interfaces.<br>The master and its backups must all use the same device HA mode.<br>Click the link to go to the screen where you can configure the ZyWALL to use the device HA mode that it is not currently using. |
| Monitored Interface Summary | This table shows the status of the interfaces that you selected for monitoring in the other device HA screens. |
| Interface | These are the names of the interfaces that are part of device HA. |
| Virtual Router IP / Netmask | This is the interface's IP address and subnet mask. Whichever ZyWALL is the master uses this virtual router IP address and subnet mask. |
| Management IP / Netmask | This field displays the interface's management IP address and subnet mask. You can use this IP address and subnet mask to access the ZyWALL whether it is in master or backup mode. |
| Link Status | This tells whether the monitored interface's connection is down or up. |

**Table 192** Device HA > General (continued)

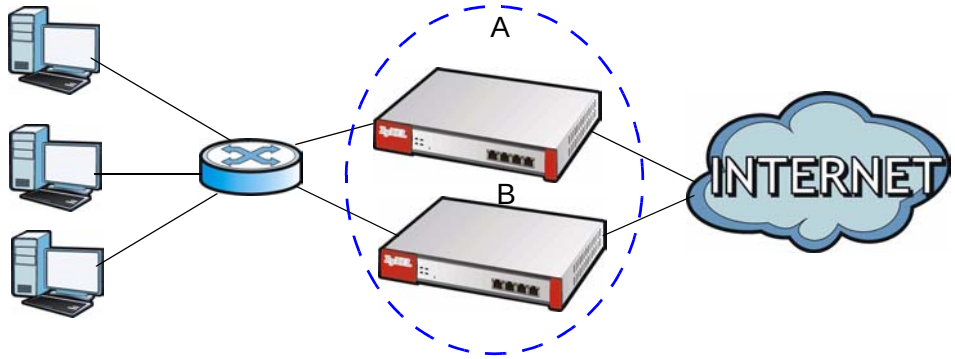
| LABEL | DESCRIPTION |
|---|---|
| HA Status | The text before the slash shows whether the device is configured as the master or the backup role.<br><br>This text after the slash displays the monitored interface's status in the virtual router.<br><br>**Active** - This interface is up and using the virtual IP address and subnet mask.<br><br>**Stand-By** - This interface is a backup interface in the virtual router. It is not using the virtual IP address and subnet mask.<br><br>**Fault** - This interface is not functioning in the virtual router right now. In active-passive mode (or in legacy mode with link monitoring enabled), if one of the master ZyWALL's interfaces loses its connection, the master ZyWALL forces all of its interfaces to the fault state so the backup ZyWALL can take over all of the master ZyWALL's functions. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# 36.3 The Active-Passive Mode Screen

## Virtual Router

The master and backup ZyWALL form a single 'virtual router'. In the following example, master ZyWALL **A** and backup ZyWALL **B** form a virtual router.

**Figure 435** Virtual Router

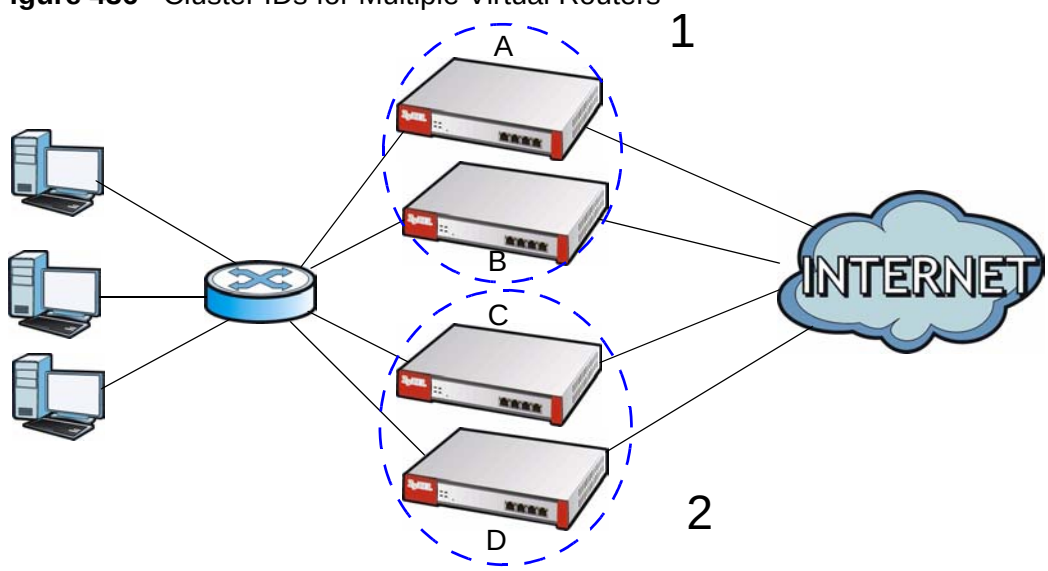



## Cluster ID

You can have multiple ZyWALL virtual routers on your network. Use a different cluster ID to identify each virtual router. In the following example, ZyWALLs **A** and

**B** form a virtual router that uses cluster ID 1. ZyWALLs **C** and **D** form a virtual router that uses cluster ID 2.

**Figure 436** Cluster IDs for Multiple Virtual Routers




## Monitored Interfaces in Active-Passive Mode Device HA

You can select which interfaces device HA monitors. If a monitored interface on the ZyWALL loses its connection, device HA has the backup ZyWALL take over.

Enable monitoring for the same interfaces on the master and backup ZyWALLs. Each monitored interface must have a static IP address and be connected to the same subnet as the corresponding interface on the backup or master ZyWALL.

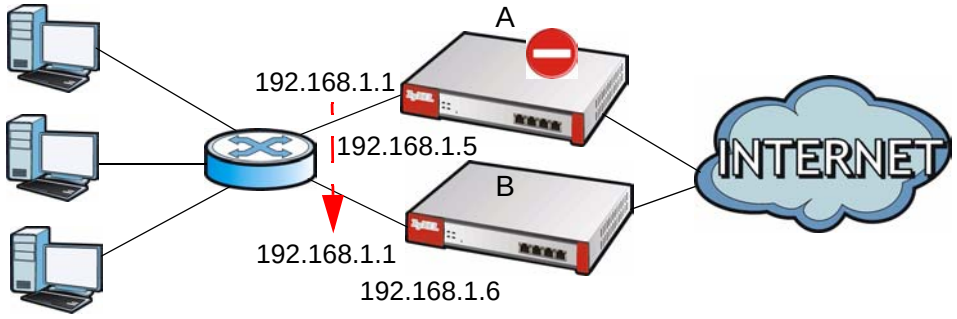
## Virtual Router and Management IP Addresses

- If a backup takes over for the master, it uses the master's IP addresses. These IP addresses are know as the virtual router IP addresses.
- Each interface can also have a management IP address. You can connect to this IP address to manage the ZyWALL regardless of whether it is the master or the backup.

For example, ZyWALL **B** takes over **A**'s 192.168.1.1 LAN interface IP address. This is a virtual router IP address. ZyWALL **A** keeps it's LAN management IP address of

192.168.1.5 and ZyWALL **B** has its own LAN management IP address of 192.168.1.6. These do not change when ZyWALL **B** becomes the master.

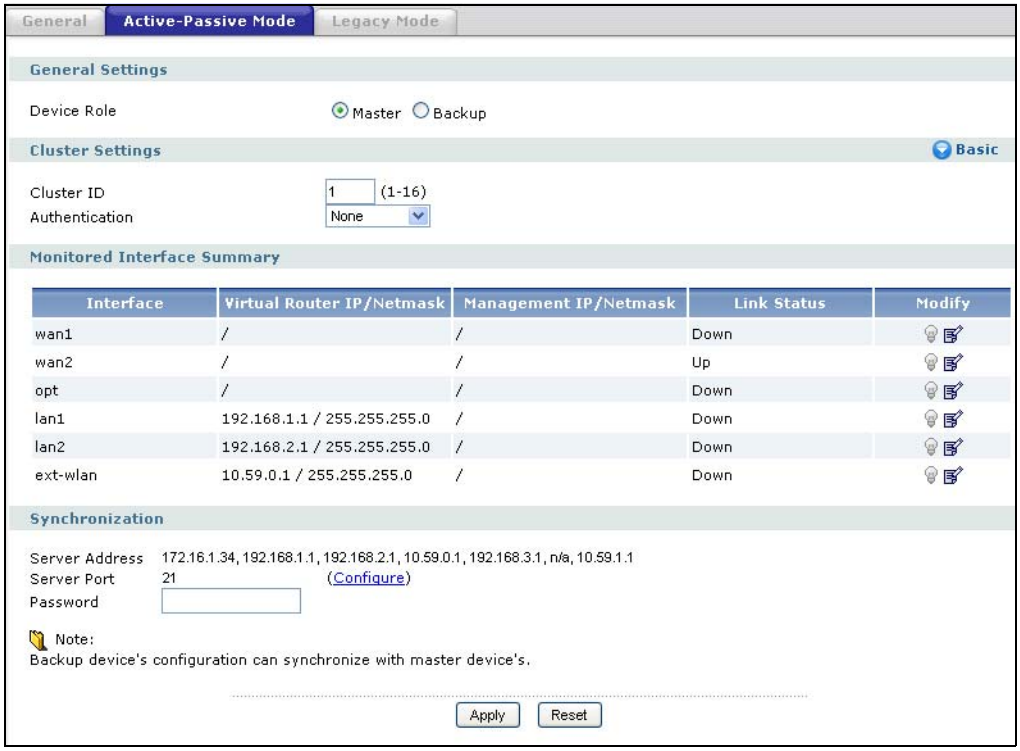
**Figure 437** Management IP Addresses




## 36.3.1 Configuring Active-Passive Mode Device HA

The **Device HA Active-Passive Mode** screen lets you configure general active-passive mode device HA settings, view and manage the list of monitored interfaces, and synchronize backup ZyWALLs. To access this screen, click **Device HA > Active-Passive Mode**.

**Figure 438** Device HA > Active-Passive Mode



The following table describes the labels in this screen. See Section 36.4 on page 637 for more information as well.

**Table 193** Device HA > Active-Passive Mode

| LABEL | DESCRIPTION |
|---|---|
| Device Role | Select the device HA role that the ZyWALL plays in the virtual router. Choices are:<br><br>**Master** - This ZyWALL is the master ZyWALL in the virtual router. This ZyWALL uses the virtual IP address for each monitored interface.<br><br>Note: Do not set this field to **Master** for two or more ZyWALLs in the same virtual router (same cluster ID).<br><br>**Backup** - This ZyWALL is a backup ZyWALL in the virtual router. This ZyWALL does not use any of the virtual IP addresses. |
| Priority | This field is available for a backup ZyWALL. Type the priority of the backup ZyWALL. The backup ZyWALL with the highest value takes over the role of the master ZyWALL if the master ZyWALL becomes unavailable. The priority must be between 1 and 254. (The master interface has priority 255.) |
| Preempt | This field is available for a backup ZyWALL. Select this if this ZyWALL should become the master ZyWALL if a lower-priority ZyWALL is the master when this one is enabled. (If the role is master, the ZyWALL preempts by default.) |
| Cluster Settings | Click **Advanced** to display more settings. Click **Basic** to display fewer settings. |
| Cluster ID | Type the cluster ID number. A virtual router consists of a master ZyWALL and all of its backup ZyWALLs. If you have multiple ZyWALL virtual routers on your network, use a different cluster ID for each virtual router. |
| Authentication | Select the authentication method the virtual router uses. Every interface in a virtual router must use the same authentication method and password. Choices are:<br><br>**None** - this virtual router does not use any authentication method.<br><br>**Text** - this virtual router uses a plain text password for authentication. Type the password in the field next to the radio button. The password can consist of alphanumeric characters, the underscore, and some punctuation marks (+-/*= :; .! @$&%#~ ‘ \ () ), and it can be up to eight characters long.<br><br>**IP AH (MD5)** - this virtual router uses an encrypted MD5 password for authentication. Type the password in the field next to the radio button. The password can consist of alphanumeric characters, the underscore, and some punctuation marks (+-/*= :; .! @$&%#~ ‘ \ () ), and it can be up to eight characters long.<br><br>See Authentication Types on page 295 for more information about authentication methods. |
| Interface | This field identifies the interface. At the time of writing, only the Ethernet interfaces can be included in the virtual router. |

**Table 193** Device HA > Active-Passive Mode (continued)

| LABEL | DESCRIPTION |
|---|---|
| Virtual Router IP / Netmask | This is the master ZyWALL's (static) IP address and subnet mask for this interface. If a backup takes over for the master, it uses this IP address. These fields are blank if the interface is a DHCP client or has no IP settings. |
| Management IP / Netmask | This field displays the interface's management IP address and subnet mask. You can use this IP address and subnet mask to access the ZyWALL whether it is in master or backup mode. |
| Link Status | This tells whether the monitored interface's connection is down or up. |
| Modify | This column provides icons to activate, deactivate, or edit monitored interfaces.<br><br>To activate or deactivate device HA monitoring of an interface, click the interface's **Active** icon. Make sure you click **Apply** to save and apply the change.<br><br>To edit an interface's management IP address and subnet mask, click its **Edit** icon. The **Add / Edit** screen appears. |
| Synchronization | Use synchronization to have a backup ZyWALL copy the master ZyWALL's configuration, certificates, AV signatures, IDP and application patrol signatures, and system protect signatures.<br><br>Every interface's management IP address must be in the same subnet as the interface's IP address (the virtual router IP address). |
| Server Address | If this ZyWALL is set to backup role, enter the IP address or Fully-Qualified Domain Name (FQDN) of the ZyWALL from which to get updated configuration. Usually, you should enter the IP address or FQDN of a virtual router on a secure network.<br><br>If this ZyWALL is set to master role, this field displays the ZyWALL's IP addresses and/or Fully-Qualified Domain Names (FQDN) through which ZyWALLs in backup role can get updated configuration from this ZyWALL. |
| Sync. Now | Click this to copy the specified ZyWALL's configuration. |
| Server Port | If this ZyWALL is set to backup role, enter the port number to use for Secure FTP when synchronizing with the specified master ZyWALL.<br><br>If this ZyWALL is set to master role, this field displays the ZyWALL's Secure FTP port number. Click the link if you need to change the FTP port number.<br><br>Every ZyWALL in the virtual router must use the same port number. If the master ZyWALL changes, you have to manually change this port number in the backups. |
| Password | Enter the password used for verification during synchronization. Every ZyWALL in the virtual router must use the same password.<br><br>If you leave this field blank in the master ZyWALL, no backup ZyWALLs can synchronize from it.<br><br>If you leave this field blank in a backup ZyWALL, it cannot synchronize from the master ZyWALL. |

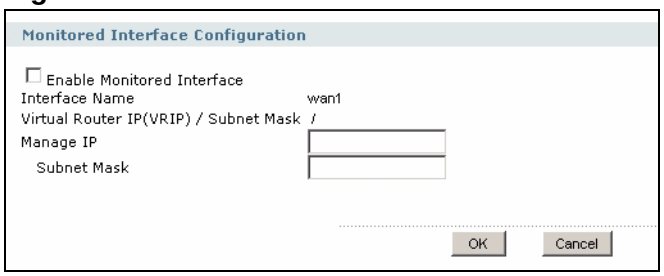
**Table 193** Device HA > Active-Passive Mode (continued)

| LABEL | DESCRIPTION |
|---|---|
| Auto Synchronize | Select this to get the updated configuration automatically from the specified ZyWALL according to the specified **Interval**. The first synchronization begins after the specified **Interval**; the ZyWALL does not synchronize immediately. |
| Interval | When you select **Auto Synchronize**, set how often the ZyWALL synchronizes with the master. |
| Apply | This appears when the ZyWALL is currently using active-passive mode device HA. Click **Apply** to save your changes back to the ZyWALL. |
| Apply & switch to Active-Passive Mode | This appears when the ZyWALL is currently configured for legacy mode device HA. Click **Apply** to save your changes back to the ZyWALL and set it to use active-passive mode device HA. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# 36.4 Configuring an Active-Passive Mode Monitored Interface

The **Device HA Active-Passive Mode Monitored Interface Edit** screen lets you enable or disable monitoring of an interface and set the interface's management IP address and subnet mask. To access this screen, click **Device HA > Active-Passive Mode > Edit**.

**Figure 439** Device HA > Active-Passive Mode > Edit




The following table describes the labels in this screen.

**Table 194** Device HA > Active-Passive Mode > Edit

| LABEL | DESCRIPTION |
|---|---|
| Enable Monitored Interface | Select this to have device HA monitor the status of this interface's connection. |
| Interface Name | This identifies the interface. |
| Virtual Router IP (VRIP) / Subnet Mask | This is the interface's (static) IP address and subnet mask in the virtual router. Whichever ZyWALL is currently serving as the master uses this virtual router IP address and subnet mask. These fields are blank if the interface is a DHCP client or has no IP settings. |

**Table 194** Device HA > Active-Passive Mode > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Management IP | Enter the interface's IP address for management access. You can use this IP address to access the ZyWALL whether it is the master or a backup. This management IP address should be in the same subnet as the interface IP address. |
| Subnet Mask | Enter the subnet mask of the interface's management IP address. |
| OK | Click **OK** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving your changes. |

# 36.5 The Legacy Mode Screen

### Virtual Router Redundancy Protocol (VRRP)

Legacy mode device HA uses Virtual Router Redundancy Protocol (VRRP) to create redundant backup gateways to ensure that a default gateway is always available. The ZyWALL uses a custom VRRP implementation and is not compatible with standard VRRP.

While active-passive mode only requires a single cluster ID for the entire virtual router, legacy mode device HA requires you to configure a separate VRRP group and Virtual Router ID (VRID) for each interface in a virtual router.

### Additional VRRP Notes

- It is possible to set up two virtual routers so that they back up each other.
- VRRP uses IP protocol 112.

### VRRP Groups

In legacy mode, you create a VRRP group to add one of its interfaces to a virtual router. You can add any Ethernet or VLAN interface with a static IP address. You do not configure VRRP groups for virtual interfaces.

- You can only use interfaces that have static IP addresses.
- You can only enable one VRRP group for each interface, and you can only have one active VRRP group for each virtual router.
- If you create a VRRP group for an Ethernet interface that has a VLAN interface configured on it, make sure you create a separate VRRP group for the VLAN interface. This will avoid an IP conflict if the backup ZyWALL takes over for the master.
- When the ZyWALL is the master, the interface uses its IP address, the IP address of the virtual router. If the ZyWALL is a backup, the interface uses its management IP address.

- You can only have one active VRRP group for each interface, and you can only have one active VRRP group for each virtual router (VR ID).
- You can set up authentication for a VRRP group. If you select AH MD5 authentication, the VRRP group uses IP protocol 51 (AH), instead of IP protocol 112 (VRRP).

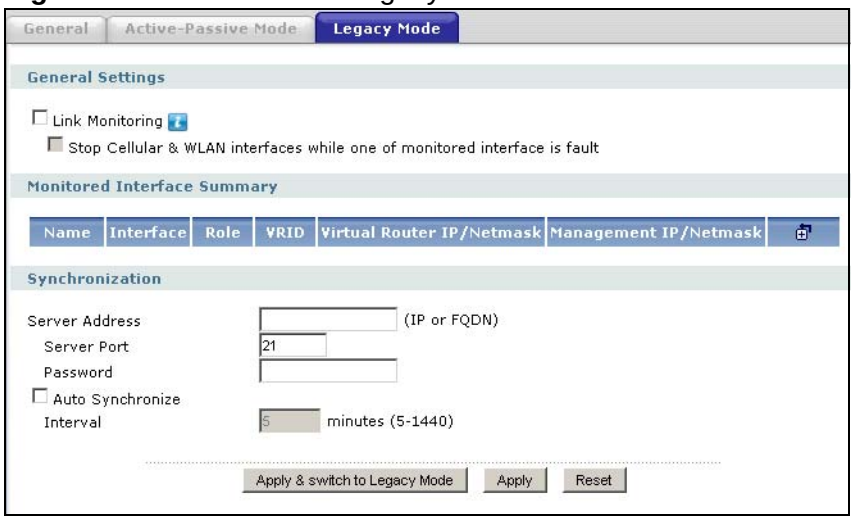
### Link Monitoring and Management Access

Link monitoring has a backup ZyWALL take over all of an unavailable master ZyWALL's static IP addresses. This way the backup ZyWALL takes over all of the master ZyWALL's functions. This also means you can only access the original master ZyWALL through its management IP address.

## 36.6 Configuring the Legacy Mode Screen

The **Device HA Legacy Mode** screen lets you configure general legacy mode HA settings including link monitoring, configure the VRRP group and synchronize backup ZyWALLs. To access this screen, click **Device HA > Legacy Mode**.

**Figure 440** Device HA > Legacy Mode




The following table describes the labels in this screen. See Table 196 on page 642 for more information as well.The Legacy Mode Add/Edit Screen

**Table 195** Device HA > Legacy Mode

| LABEL | DESCRIPTION |
|---|---|
| General Settings | |
| Link Monitoring | Enable link monitoring to have the master ZyWALL shut down all of its VRRP interfaces if one of its VRRP interface links goes down. This way the backup ZyWALL takes over all of the master ZyWALL's functions. |

**Table 195** Device HA > Legacy Mode (continued)

| LABEL | DESCRIPTION |
|---|---|
| Stop Cellular & WLAN interfaces while one of monitored interface is fault | Select this to have the master ZyWALL shut down any 3G or wireless LAN interfaces if one of its VRRP interface links goes down. Clear this if you still want users to be able to use the ZyWALL's 3G connection or wireless LAN even when a VRRP interface link goes down. |
| Monitored Interface Summary | |
| Name | This field displays the name of the VRRP group. |
| Interface | This field displays which interface is part of the virtual router. |
| Role | This field displays which role the interface plays in the virtual router.<br>**Master** - This interface is the master interface in the virtual router. The interface always uses its static IP address, not the management IP address of the VRRP group.<br>**Backup** - This interface is a backup interface in the virtual router. The interface may use its static IP address or the management IP address of the VRRP group, depending on whether or not the backup has become the master. |
| VRID | This field displays the virtual router ID number. |
| Virtual Router IP / Netmask | This is the interface's IP address and subnet mask in the virtual router. |
| Management IP / Netmask | This field displays the management IP address and subnet mask of an interface. |
| Add icon | This column provides icons to activate, deactivate, add, edit, and remove VRRP groups.<br>To activate or deactivate a VRRP group, click the **Active** icon next to the group. Make sure you click **Apply** to save and apply the change. Activating a VRRP group has the ZyWALL monitor the connection of the group's interface. Each interface must have a static IP address and be connected to the same subnet as the group's interface on the other ZyWALL.<br>To add a VRRP group, click the **Add** icon at the top of the column. The **VRRP Group Add/Edit** screen appears.<br>To edit a VRRP group, click the **Edit** icon next to the group. The **VRRP Group Add/Edit** screen appears.<br>To delete a VRRP group, click the **Remove** icon next to the group. The Web Configurator confirms that you want to delete the VRRP group before doing so. |
| Synchronization | |
| Server Address | Enter the IP address or Fully-Qualified Domain Name (FQDN) of the ZyWALL from which to get configuration and subscription service updates (for services to which the backup ZyWALL is subscribed). Usually, you should enter the IP address or FQDN of a virtual router on a secure network. |

**Table 195** Device HA > Legacy Mode (continued)

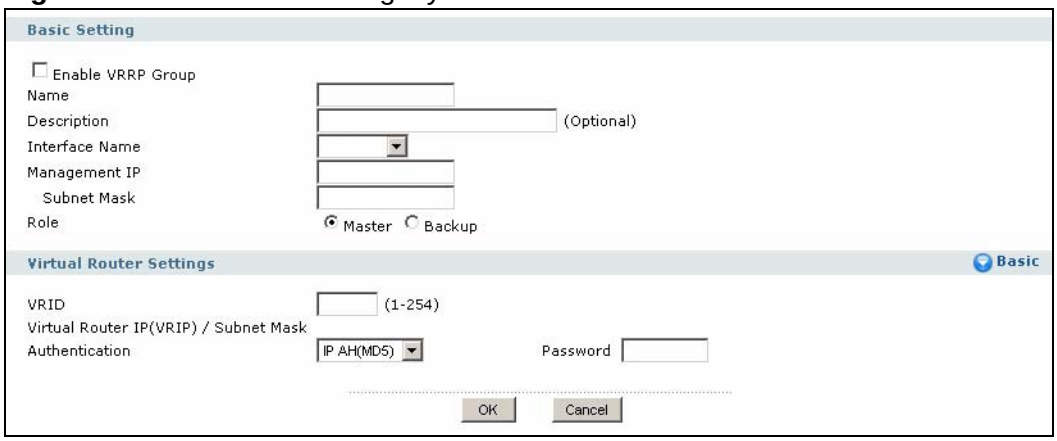
| LABEL | DESCRIPTION |
|---|---|
| Server Port | Enter the port number that the ZyWALL you specified in the **Server Address** field uses for Secure FTP. Every ZyWALL in the virtual router must use the same port number. If the master ZyWALL changes, you have to manually change this port number in the backups. |
| Password | Enter the password used to verify other ZyWALLs during synchronization. This password is different than the one that is used for authentication in the VRRP group. Every ZyWALL in the virtual router must use the same password. If you leave this field blank in the master ZyWALL, it does not allow any backup ZyWALLs to synchronize from it. If you leave this field blank in a backup ZyWALL, it cannot synchronize from the master ZyWALL. |
| Auto Synchronize | Select this to get configuration and subscription service updates automatically from the specified ZyWALL according to the specified **Interval**. The first synchronization begins after the specified **Interval**; the ZyWALL does not synchronize immediately. |
| Interval | This field is only available if **Auto Synchronize** is checked. Type the number of minutes to wait between synchronizations. |
| Apply & switch to Legacy Mode | This appears when the ZyWALL is currently using active-passive mode device HA. Click **Apply** to save your changes back to the ZyWALL and set it to use legacy mode device HA. |
| Apply | This appears when the ZyWALL is currently using legacy mode device HA. Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

Use the **VRRP Group Add/Edit** screen to add or edit VRRP groups.

- You can only use interfaces that have static IP addresses. In addition, you should set the static IP address to the IP address of the virtual router.
- You can only enable one VRRP group for each interface.
- You can only have one active VRRP group for each virtual router (VR ID).

The **Device HA Legacy Mode Add** or **Edit** screen lets you configure a VRRP group. To access this screen, click **Device HA > Legacy Mode > Add** (or **Edit**).

**Figure 441** Device HA > Legacy Mode > Add



The following table describes the labels in this screen.

**Table 196** Device HA > Legacy Mode > Add

| LABEL | DESCRIPTION |
|---|---|
| Enable VRRP Group | Select this to make the specified interface part of the virtual router. Clear this to take the specified interface out of the virtual router. Enabling a VRRP group has the ZyWALL monitor the connection of the group's interface. |
| Name | This field is read-only if you are editing the VRRP group. Type the name of the VRRP group. This field must be unique in the ZyWALL, but it is not used in the virtual router. The virtual router uses the **VRID**. The name can consist of alphanumeric characters, the underscore, and the dash and may be up to fifteen characters long. |
| Description | Type the description of the VRRP group. This field is only for your reference. It may be up to sixty printable ASCII characters long. |
| Interface Name | Select the interface in this device that is part of the virtual router. You can only select interfaces that have static IP addresses. Connect the interface to the same subnet as the group's interface on the other ZyWALL. |
| Manage IP | Enter the interface's IP address for management access. You can use this IP address to access the ZyWALL whether it is the master or a backup. This management IP address should be in the same subnet as the interface IP address so the backup ZyWALL cannot synchronize with the master via this VRRP interface. |
| Subnet Mask | Enter the subnet mask of the interface's management IP address. |
| Role | Select the role that you want the interface to play in the virtual router. Choices are:<br>**Master** - This interface is the master interface in the virtual router. The interface always uses its virtual IP address when its status is active.<br>Note: Do not set this field to **Master** for two or more ZyWALLs in the same virtual router (same VR ID).<br>**Backup** - This interface is a backup interface in the virtual router. The current role depends on the other ZyWALLs in the virtual router. |
| Priority | This field is available if the selected interface is a **Backup** interface. Type the priority of the backup interface. The backup interface with the highest value takes over the role of the master interface if the master interface becomes unavailable. The priority must be between 1 and 254. (The master interface has priority 255.) |
| Preempt | This field is available if the selected interface is a **Backup** interface. Select this if the selected interface should become the master interface if a lower-priority interface is the master when this one is enabled. (If the role is **Master**, the interface preempts by default.) |
| Virtual Router Settings | Click **Advanced** to display more settings. Click **Basic** to display fewer settings. |
| VRID | Type the virtual router ID number. |
| Virtual Router IP (VRIP) / Subnet Mask | Type the interface's IP address and subnet mask in the virtual router. |

**Table 196** Device HA > Legacy Mode > Add (continued)

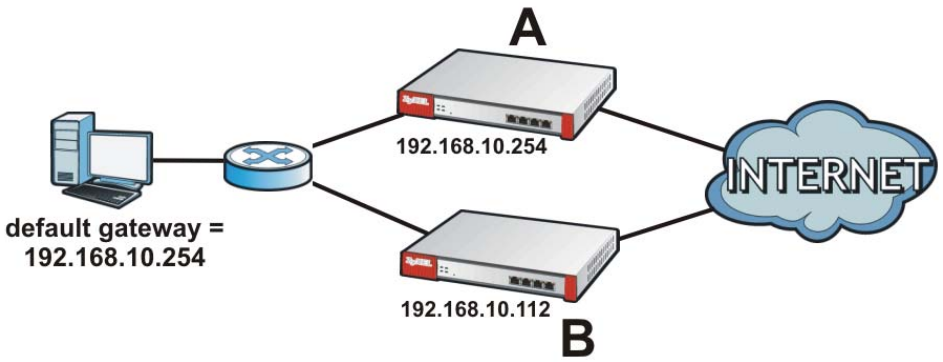
| LABEL | DESCRIPTION |
|---|---|
| Authentication | Select the authentication method used in the virtual router. Every interface in a virtual router must use the same authentication method and password. Choices are:<br><br>**None** - this virtual router does not use any authentication method.<br><br>**Text** - this virtual router uses a plain text password for authentication. Type the password in the field next to the radio button. The password can consist of alphanumeric characters, the underscore, and some punctuation marks (+-/*= :; .! @$&%#~ ‘ \ () ), and it can be up to eight characters long.<br><br>**IP AH (MD5)** - this virtual router uses an encrypted MD5 password for authentication. Type the password in the field next to the radio button. The password can consist of alphanumeric characters, the underscore, and some punctuation marks (+-/*= :; .! @$&%#~ ‘ \ () ), and it can be up to eight characters long.<br><br>See Authentication Types on page 295 for more information about authentication methods. |
| OK | Click **OK** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving your changes. |

# 36.7 Device HA Technical Reference

## Legacy Mode ZyWALL VRRP Application

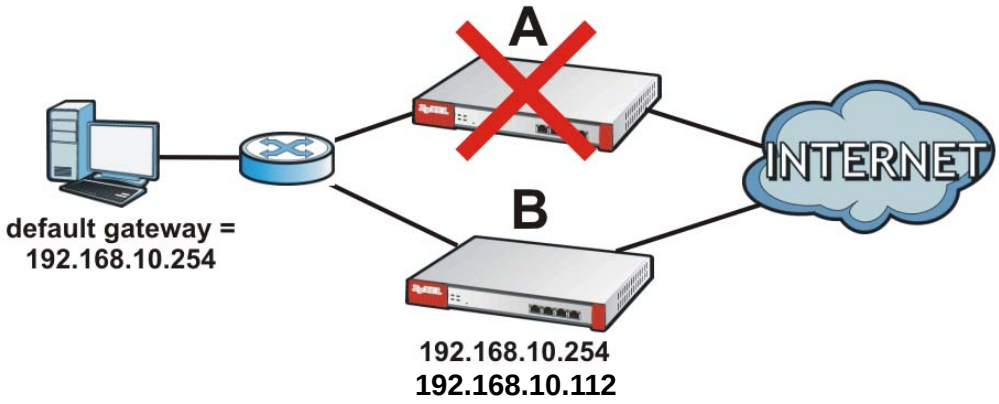
In VRRP, a virtual router represents a number of ZyWALLs associated with one IP address, the IP address of the default gateway. Each virtual router is identified by a unique 8-bit identification number called a Virtual Router ID (VR ID). In the example below, ZyWALL **A** and ZyWALL **B** are part of virtual router 10 with IP address 192.168.10.254.

**Figure 442** Example: VRRP, Normal Operation



The VR ID is not shown. In normal operation, ZyWALL **A** is the master. It has the same IP address as the default gateway and forwards traffic for the network. ZyWALL **B** is a backup. It is using its management IP address 192.168.10.112. ZyWALL **A** sends regular messages to ZyWALL **B** to let ZyWALL **B** know that ZyWALL **A** is available. If ZyWALL **A** becomes unavailable, it stops sending messages to ZyWALL **B**. ZyWALL **B** detects this and assumes the role of the master. This is illustrated below.

**Figure 443** Example: VRRP, Master Becomes Unavailable




ZyWALL **B** is now using the IP address of the default gateway, and it is forwarding packets for the network. The loss of ZyWALL **A** has no effect on the network.

If there is more than one backup ZyWALL, the backup ZyWALL with the highest priority becomes the master. The other backup ZyWALLs remain backups.

If ZyWALL **A** becomes available again, ZyWALL **A** preempts ZyWALL **B** and becomes the master again (the network returns to the state shown in Figure 442 on page 643).

## Synchronization

During synchronization, the master ZyWALL sends the following information to the backup ZyWALL.

- Startup configuration file (**startup-config.conf**)
- AV signatures
- IDP and application patrol signatures
- System protect signatures
- Certificates (**My Certificates**, and **Trusted Certificates**)

Synchronization does not change the device HA settings in the backup ZyWALL.

Synchronization affects the entire device configuration. You can only configure one set of settings for synchronization, regardless of how many VRRP groups you might configure. The ZyWALL uses Secure FTP (on a port number you can change) to synchronize, but it is still recommended that the backup ZyWALL synchronize with a master ZyWALL on a secure network.

The backup ZyWALL gets the configuration from the master ZyWALL. The backup ZyWALL cannot become the master or be managed while it applies the new configuration. This usually takes two or three minutes or longer depending on the configuration complexity.

The following restrictions apply with active-passive mode.

- The master ZyWALL must have no inactive monitored interfaces.
- The backup ZyWALL cannot be the master. This refers to the actual role at the time of synchronization, not the role setting in the configuration screen.

The following synchronization restrictions apply with legacy mode.

- The master ZyWALL must have at least one active VRRP group and no standby VRRP groups.
- The backup ZyWALL cannot be the master in any active VRRP group. This refers to the actual role at the time of synchronization, not the role setting in the VRRP group.

The backup applies the entire configuration if it is different from the backup's current configuration.

# PART VIII
# Objects

# 37

# User/Group

## 37.1 Overview

This chapter describes how to set up user accounts, user groups, and user settings for the ZyWALL. You can also set up rules that control when users have to log in to the ZyWALL before the ZyWALL routes traffic for them.

### 37.1.1 What You Can Do Using The User/Group Screens

- The **User** screen (see Section 37.2 on page 652) provides a summary of all user accounts.
- The **Group** screen (see Section 37.3 on page 655) provides a summary of all user groups. In addition, this screen allows you to add, edit, and remove user groups. User groups may consist of access users and other user groups. You cannot put admin users in user groups
- The **Setting** screen (see Section 37.4 on page 656) controls default settings, login settings, lockout settings, and other user settings for the ZyWALL. You can also use this screen to specify when users must log in to the ZyWALL before it routes traffic for them.

### 37.1.2 What You Need To Know About User/Groups

#### User Account

A user account defines the privileges of a user logged into the ZyWALL. User accounts are used in firewall rules and application patrol, in addition to controlling access to configuration and services in the ZyWALL.

#### User Types

These are the types of user accounts the ZyWALL uses.

**Table 197** Types of User Accounts

| TYPE | ABILITIES | LOGIN METHOD(S) |
|---|---|---|
| Admin Users | | |
| Admin | Change ZyWALL configuration (web, CLI) | WWW, TELNET, SSH, FTP, Console, Dial-in |

**Table 197** Types of User Accounts (continued)

| TYPE | ABILITIES | LOGIN METHOD(S) |
|---|---|---|
| Limited-Admin | Look at ZyWALL configuration (web, CLI)<br>Perform basic diagnostics (CLI) | WWW, TELNET, SSH, Console, Dial-in |
| Access Users | | |
| User | Access network services<br>Browse user-mode commands (CLI) | WWW, TELNET, SSH |
| Guest | Access network services | WWW |
| Ext-User | External User Account | WWW |

Note: The default **admin** account is always authenticated locally, regardless of the authentication method setting. (See Chapter 41 on page 683 for more information about authentication methods.)

### Ext-User Accounts

Set up an **Ext-User** account if the user is authenticated by an external server and you want to set up specific policies for this user in the ZyWALL. If you do not want to set up policies for this user, you do not have to set up an **Ext-User** account.

**Ext-User** users should be authenticated by an external server, such as AD, LDAP or RADIUS. If the ZyWALL tries to use the local database to authenticate an **Ext-User**, the authentication attempt always fails. (This is related to AAA servers and authentication methods, which are discussed in Chapter 41 on page 683 and Chapter 42 on page 695, respectively.)

Note: If the ZyWALL tries to authenticate an **Ext-User** using the local database, the attempt always fails.

Once an **Ext-User** user has been authenticated, the ZyWALL tries to get the user type (see Table 197 on page 649) from the external server. If the external server does not have the information, the ZyWALL sets the user type for this session to **User**.

For the rest of the user attributes, such as reauthentication time, the ZyWALL checks the following places, in order.

1. User account in the remote server.
2. User account (Ext-User) in the ZyWALL.
3. Default user account for AD users (**ad-users**), LDAP users (**ldap-users**) or RADIUS users (**radius-users**) in the ZyWALL.

See Setting up User Attributes in an External Server on page 664 for a list of attributes and how to set up the attributes in an external server.

### User Groups

User groups may consist of user accounts or other user groups. Use user groups when you want to create the same rule for several user accounts, instead of creating separate rules for each one.

Note: You cannot put access users and admin users in the same user group.

Note: You cannot put the default **admin** account into any user group.

The sequence of members in a user group is not important.

### User Awareness

By default, users do not have to log into the ZyWALL to use the network services it provides. The ZyWALL automatically routes packets for everyone. If you want to restrict network services that certain users can use via the ZyWALL, you can require them to log in to the ZyWALL first. The ZyWALL is then 'aware' of the user who is logged in and you can create 'user-aware policies' that define what services they can use. See Section 37.4.3 on page 663 for a user-aware login example.

### Forced User Authentication

Instead of making users for which user-aware policies have been configured go to the ZyWALL **Login** screen manually, you can configure the ZyWALL to display the **Login** screen automatically whenever it routes HTTP traffic for anyone who has not logged in yet.

Note: This works with HTTP traffic only. The ZyWALL does not force users to log in before it routes other kinds of traffic.

The ZyWALL does not automatically route the request that prompted the login, however, so users have to make this request again.

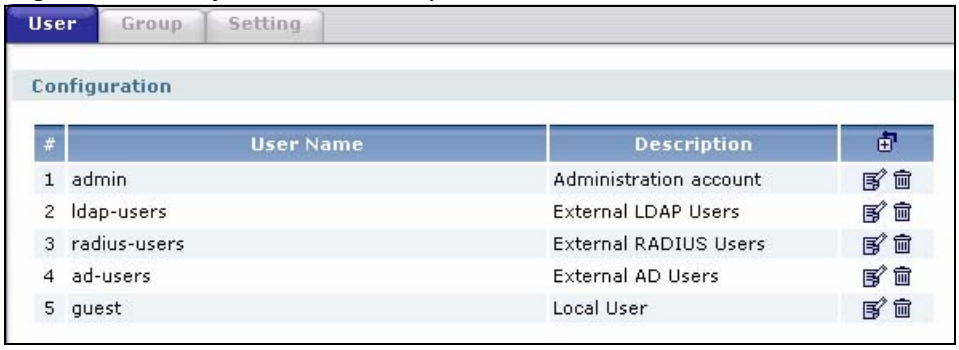
### Finding Out More

- See Section 5.5.1 on page 97 for related information on these screens.
- See Section 37.5 on page 664 for some information on users who use an external authentication server in order to log in.

# 37.2 User Summary Screen

The **User** screen provides a summary of all user accounts. To access this screen, login to the Web Configurator, and click **Object > User/Group**.

**Figure 444** Object > User/Group




The following table describes the labels in this screen.

**Table 198** Object > User/Group

| LABEL | DESCRIPTION |
|---|---|
| # | This field is a sequential value, and it is not associated with a specific user. |
| User Name | This field displays the user name of each user. |
| Description | This field displays the description for each user. |
| Add icon | This column provides icons to add, edit, and remove users.<br>To add a user, click the **Add** icon at the top of the column. The **User Add/Edit** screen appears.<br>To edit a user, click the **Edit** icon next to the user. The **User Add/Edit** screen appears.<br>To delete a user, click the **Remove** icon next to the user. The Web Configurator confirms that you want to delete the user before doing so. |

## 37.2.1 User Add/Edit Screen

The **User Add/Edit** screen allows you to create a new user account or edit an existing one.

### 37.2.1.1 Rules for User Names

Enter a user name from 1 to 31 characters.

The user name can only contain the following characters:

- Alphanumeric A-z 0-9 (there is no unicode support)
- _ [underscores]

- - [dashes]

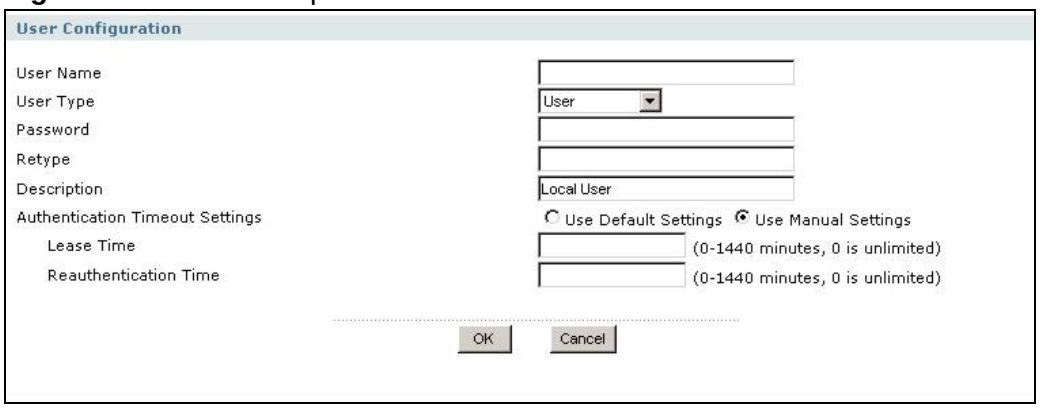
The first character must be alphabetical (A-Z a-z), an underscore (_), or a dash (-). Other limitations on user names are:

- User names are case-sensitive. If you enter a user 'bob' but use 'BOB' when connecting via CIFS or FTP, it will use the account settings used for 'BOB' not ‘bob’.
- User names have to be different than user group names.
- Here are the reserved user names:

| | | | | |
|---|---|---|---|---|
| • adm | • admin | • any | • bin | • daemon |
| • debug | • devicehaecived | • ftp | • games | • halt |
| • ldap-users | • lp | • mail | • news | • nobody |
| • operator | • radius-users | • root | • shutdown | • sshd |
| • sync | • uucp | • zyxel | | |

To access this screen, go to the **User** screen (see Section 37.2 on page 652), and click either the **Add** icon or an **Edit** icon.

**Figure 445** User/Group > User > Edit



The following table describes the labels in this screen.

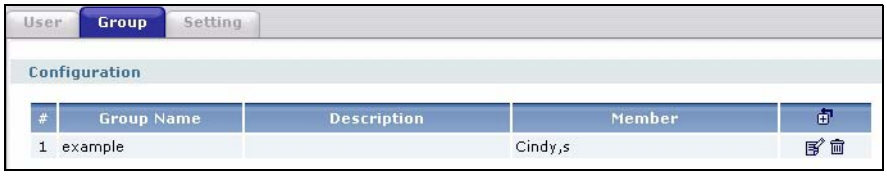
**Table 199** User/Group > User > Edit

| LABEL | DESCRIPTION |
|---|---|
| User Name | Type the user name for this user account. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. User names have to be different than user group names, and some words are reserved. See Section 37.2.1.1 on page 652. |
| User Type | Select what type of user this is. Choices are:<br>• **Admin** - this user can look at and change the configuration of the ZyWALL<br>• **Limited-Admin** - this user can look at the configuration of the ZyWALL but not to change it<br>• **User** - this user has access to the ZyWALL's services but cannot look at the configuration<br>• **Guest** - this user has access to the ZyWALL's services but cannot look at the configuration<br>• **Ext-User** - this user account is maintained in a remote server, such as RADIUS or LDAP. See Ext-User Accounts on page 650 for more information about this type. |
| Password | This field is not available if **you select the Ext-User user type**.<br>Enter the password of this user account. It can consist of 4 - 30 alphanumeric characters. |
| Retype | This field is not available if **you select the Ext-User user type**. Enter the password again. |
| Description | Enter the description of each user, if any. You can use up to 60 printable ASCII characters. Default descriptions are provided. |
| Authentication Timeout Settings | If you want to set authentication timeout to a value other than the default settings, select **Use Manual Settings** then fill your preferred values in the fields that follow. |
| Lease Time | Enter the number of minutes this user has to renew the current session before the user is logged out. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. Admin users renew the session every time the main screen refreshes in the Web Configurator. Access users can renew the session by clicking the **Renew** button on their screen. If you allow access users to renew time automatically (see Section 37.4 on page 656), the users can select this check box on their screen as well. In this case, the session is automatically renewed before the lease time expires. |
| Reauthentication Time | Type the number of minutes this user can be logged into the ZyWALL in one session before the user has to log in again. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. Unlike **Lease Time**, the user has no opportunity to renew the session without logging out. |
| OK | Click **OK** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving your changes. |

# 37.3 User Group Summary Screen

User groups consist of access users and other user groups. You cannot put admin users in user groups. The **Group** screen provides a summary of all user groups. In addition, this screen allows you to add, edit, and remove user groups. To access this screen, login to the Web Configurator, and click **Object > User/Group > Group**.

**Figure 446** Object > User/Group > Group




The following table describes the labels in this screen. See Section 37.3.1 on page 656 for more information as well.

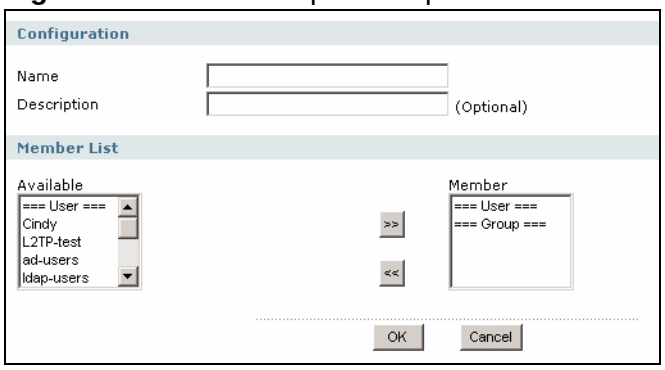
**Table 200** Object > User/Group > Group

| LABEL | DESCRIPTION |
|---|---|
| # | This field is a sequential value, and it is not associated with a specific user group. |
| Group Name | This field displays the name of each user group. |
| Description | This field displays the description for each user group. |
| Member | This field lists the members in the user group. Each member is separated by a comma. |
| Add icon | This column provides icons to add, edit, and remove user groups.<br><br>To add a user group, click the **Add** icon at the top of the column. The **Group Add/Edit** screen appears.<br><br>To edit a user group, click the **Edit** icon next to the user group. The **Group Add/Edit** screen appears.<br><br>To delete a user group, click the **Remove** icon next to the user group. The Web Configurator confirms that you want to delete the user group before doing so. If you delete the group, you do not delete the users in the group. |

### 37.3.1 Group Add/Edit Screen

The **Group Add/Edit** screen allows you to create a new user group or edit an existing one. To access this screen, go to the **Group** screen (see Section 37.3 on page 655), and click either the **Add** icon or an **Edit** icon.

**Figure 447** User/Group > Group > Add




The following table describes the labels in this screen.

**Table 201** User/Group > Group > Add

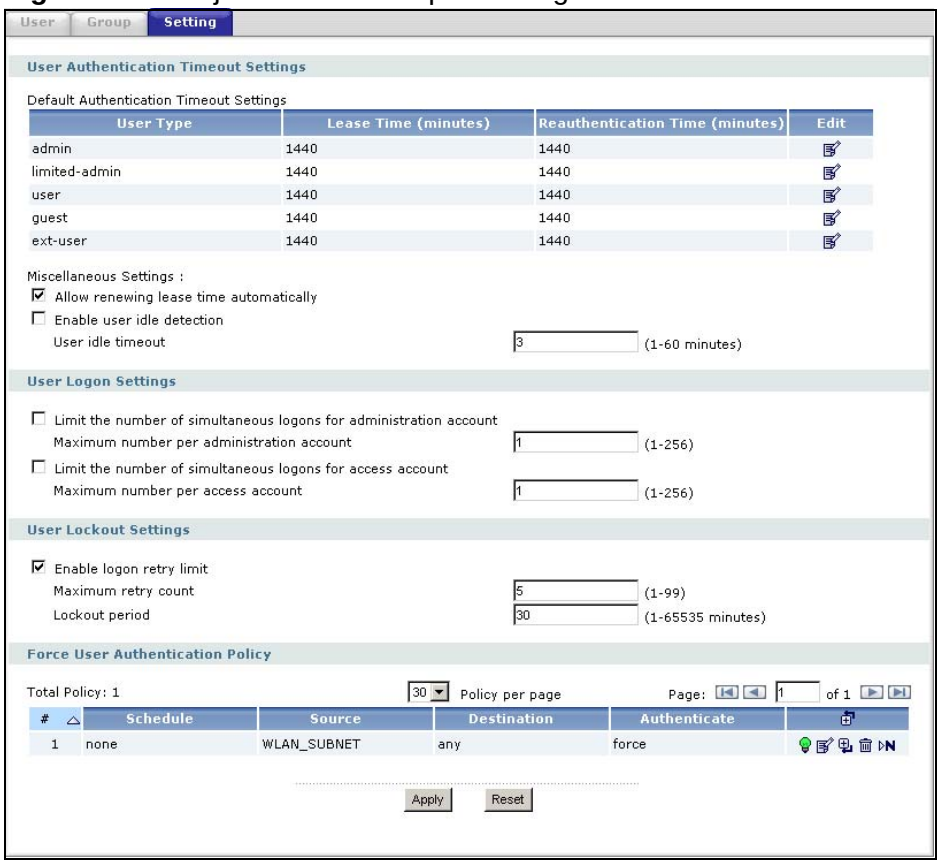
| LABEL | DESCRIPTION |
|---|---|
| Name | Type the name for this user group. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. User group names have to be different than user names. |
| Description | Enter the description of the user group, if any. You can use up to 60 characters, punctuation marks, and spaces. |
| Available | This field displays the names of the users and user groups that can be added to the user group.<br><br>Select users and groups that you want to be members of this group and click the right arrow to add them to the member list. |
| Member | This field displays the names of the users and user groups that have been added to the user group. The order of members is not important. To remove members, select them and click the left arrow. |
| OK | Click **OK** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving your changes. |

## 37.4 Setting Screen

The **Setting** screen controls default settings, login settings, lockout settings, and other user settings for the ZyWALL. You can also use this screen to specify when users must log in to the ZyWALL before it routes traffic for them.

To access this screen, login to the Web Configurator, and click **Object > User/Group > Setting**.

**Figure 448** Object > User/Group > Setting




The following table describes the labels in this screen.

**Table 202** Object > User/Group > Setting

| LABEL | DESCRIPTION |
|---|---|
| User Authentication Timeout Settings | |
| Default Authentication Timeout Settings | This authentication timeout settings are used by default when you create a new user account. They also control the settings for any existing user accounts that are set to use the default settings. You can still manually configure any user account's authentication timeout settings. |

**Table 202** Object > User/Group > Setting (continued)

| LABEL | DESCRIPTION |
|---|---|
| User Type | These are the kinds of user account the ZyWALL supports.<br><br>**admin** - this user can look at and change the configuration of the ZyWALL<br><br>**limited-admin** - this user can look at the configuration of the ZyWALL but not to change it<br><br>**user** - this user has access to the ZyWALL's services but cannot look at the configuration<br><br>**guest** - this user has access to the ZyWALL's services but cannot look at the configuration<br><br>**ext-user** - this user account is maintained in a remote server, such as RADIUS or LDAP. See Ext-User Accounts on page 650 for more information about this type. |
| Lease Time (minutes) | This is the default lease time for each type of user account. It defines the number of minutes the user has to renew the current session before the user is logged out.<br><br>Admin users renew the session every time the main screen refreshes in the web configurator. Access users can renew the session by clicking the **Renew** button on their screen. If you allow access users to renew time automatically (see Section 37.4 on page 656), the users can select this check box on their screen as well. In this case, the session is automatically renewed before the lease time expires. |
| Reauthentication Time (minutes) | This is the default reauthentication time for each type of user account. It defines the number of minutes the user can be logged into the ZyWALL in one session before having to log in again. Unlike **Lease Time**, the user has no opportunity to renew the session without logging out. |
| Edit | Click the icon to open a screen where you can edit the default settings for that type of user account. |
| Miscellaneous Settings | |
| Allow renewing lease time ... | Select this check box if access users can renew lease time automatically, as well as manually, simply by checking the **Updating lease time automatically** check box on their screen. |
| Enable user idle detection | This is applicable for access users.<br><br>Select this check box if you want the ZyWALL to monitor how long each access user is logged in and idle (in other words, there is no traffic for this access user). The ZyWALL automatically logs out the access user once the **User idle timeout** has been reached. |
| User idle timeout | This is applicable for access users.<br><br>This field is effective when **Enable user idle detection** is checked. Type the number of minutes each access user can be logged in and idle before the ZyWALL automatically logs out the access user. |
| User Logon Settings | |

**Table 202** Object > User/Group > Setting (continued)

| LABEL | DESCRIPTION |
|---|---|
| Limit ... for administration account | Select this check box if you want to set a limit on the number of simultaneous logins by admin users. If you do not select this, admin users can login as many times as they want at the same time using the same or different IP addresses. |
| Maximum number per administration account | This field is effective when **Limit ... for administration account** is checked. Type the maximum number of simultaneous logins by each admin user. |
| Limit ... for access account | Select this check box if you want to set a limit on the number of simultaneous logins by non-admin users. If you do not select this, access users can login as many times as they want as long as they use different IP addresses. |
| Maximum number per access account | This field is effective when **Limit ... for access account** is checked. Type the maximum number of simultaneous logins by each access user. |
| User Lockout Settings | |
| Enable logon retry limit | Select this check box to set a limit on the number of times each user can login unsuccessfully (for example, wrong password) before the IP address is locked out for a specified amount of time. |
| Maximum retry count | This field is effective when **Enable logon retry limit** is checked. Type the maximum number of times each user can login unsuccessfully before the IP address is locked out for the specified **lockout period**. The number must be between 1 and 99. |
| Lockout period | This field is effective when **Enable logon retry limit** is checked. Type the number of minutes the user must wait to try to login again, if **logon retry limit** is enabled and the **maximum retry count** is reached. This number must be between 1 and 65,535 (about 45.5 days). |
| Force User Authentication Policy | Use this section to specify when users must log in to the ZyWALL before the ZyWALL routes HTTP traffic for them. Once users have logged in, the ZyWALL can enforce user-aware policies.<br>This section displays the conditions that are applied, in sequence, to decide what the appropriate action is.<br>By default, LAN users do not have to log into the ZyWALL.<br>Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order. |
| Total Policy | This is the number of entries configured. |
| Policy per page | Select how many entries to display per page in the screen. |
| Page x of x | This is the number of the page of entries currently displayed and the total number of pages of entries. Type a page number to go to or use the arrows to navigate the pages of entries. |
| # | This field is a sequential value, and it is not associated with a specific condition. |
| Schedule | This field displays the schedule object that specifies when this condition applies. It displays **none** if this condition always applies. |

**Table 202** Object > User/Group > Setting (continued)

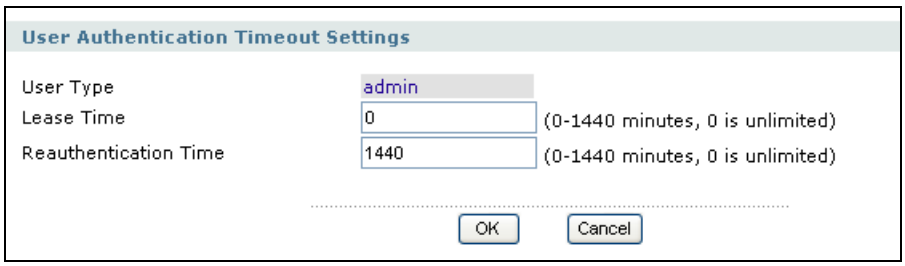
| LABEL | DESCRIPTION |
|---|---|
| Source | This field displays the source address object of traffic to which this condition applies. It displays **any** if this condition applies to traffic from all source addresses. |
| Destination | This field displays the destination address object of traffic to which this condition applies. It displays **any** if this condition applies to traffic from all destination addresses. |
| Authenticate | This field displays whether users must log in (**force**) or whether users do not have to log in (**skip**) when this condition is checked and satisfied. |
| Add icon | This column provides icons to add, edit, move, and remove conditions. It also provides icons to activate and deactivate conditions.<br><br>To add a condition, click the **Add** icon at the top of the column or next to each condition. If you click the one at the top of the column, the new condition is first in the list. If you click the one next to a condition, the new condition appears right below this condition.<br><br>To edit a condition, click the **Edit** icon at the top of the column or next to each condition. The **Force User Authentication Policy Add/Edit** screen appears.<br><br>To remove a condition, click on the **Remove** icon next to the condition. The Web Configurator confirms that you want to delete the condition before doing so.<br><br>To move a condition up or down in the list, click on the **Move to N** icon next to the condition, and type the line number (**#** field) where you want to move this condition. The **#** field is updated accordingly.<br><br>To activate or deactivate a condition, click the **Active** icon next to the condition. Make sure you click **Apply** to save and apply the change. |
| Apply | Click **Apply** to save the changes. |
| Reset | Click **Reset** to start configuring this screen again. |

## 37.4.1 Default User Authentication Timeout Settings Edit Screens

The **Default Authentication Timeout Settings Edit** screen allows you to set the default authentication timeout settings for the selected type of user account. These default authentication timeout settings also control the settings for any existing user accounts that are set to use the default settings. You can still manually configure any user account's authentication timeout settings.

To access this screen, go to the **Object > User/Group > Setting** screen (see Section 37.4 on page 656), and click one of the **Default Authentication Timeout Settings** section's **Edit** icons.

**Figure 449** Object > User/Group > Setting > Default Authentication Timeout Settings Edit




The following table describes the labels in this screen.

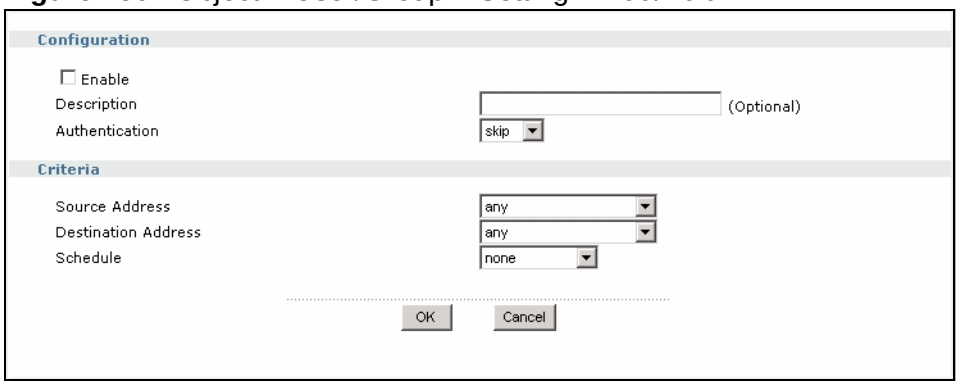
**Table 203** Object > User/Group > Setting > Default Authentication Timeout Settings Edit

| LABEL | DESCRIPTION |
|---|---|
| User Type | This read-only field identifies the type of user account for which you are configuring the default settings.<br>• **Admin** - this user can look at and change the configuration of the ZyWALL<br>• **Limited-Admin** - this user can look at the configuration of the ZyWALL but not to change it<br>• **User** - this user has access to the ZyWALL's services but cannot look at the configuration<br>• **Guest** - this user has access to the ZyWALL's services but cannot look at the configuration<br>• **Ext-User** - this user account is maintained in a remote server, such as RADIUS or LDAP. See Ext-User Accounts on page 650 for more information about this type. |
| Lease Time | Enter the number of minutes this type of user account has to renew the current session before the user is logged out. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited.<br>Admin users renew the session every time the main screen refreshes in the web configurator. Access users can renew the session by clicking the **Renew** button on their screen. If you allow access users to renew time automatically (see Section 37.4 on page 656), the users can select this check box on their screen as well. In this case, the session is automatically renewed before the lease time expires. |
| Reauthentication Time | Type the number of minutes this type of user account can be logged into the ZyWALL in one session before the user has to log in again. You can specify 1 to 1440 minutes. You can enter 0 to make the number of minutes unlimited. Unlike **Lease Time**, the user has no opportunity to renew the session without logging out. |
| OK | Click **OK** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving your changes. |

## 37.4.2 Force User Authentication Policy Add/Edit Screen

Use this screen to specify a condition when users must log in or do not have to log in to the ZyWALL before their HTTP traffic can pass through the ZyWALL.

**Figure 450** Object > User/Group > Setting > Add/Edit




The following table describes the labels in this screen.

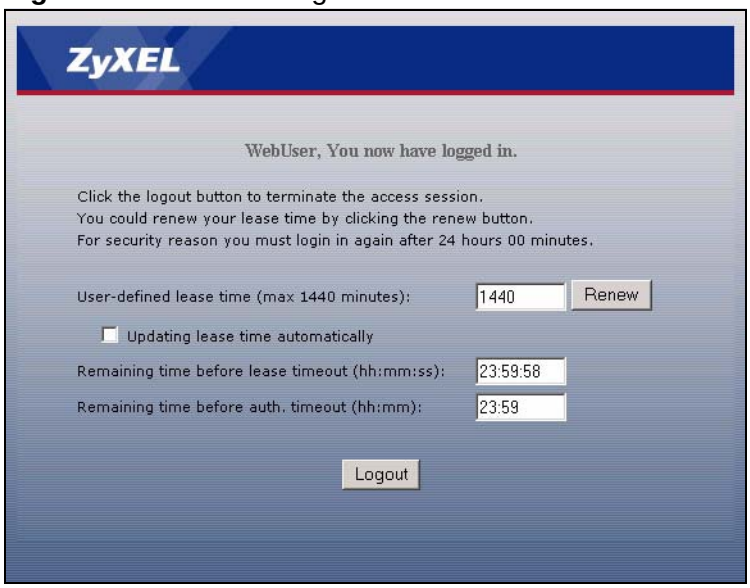
**Table 204** Object > User/Group > Setting > Add/Edit

| LABEL | DESCRIPTION |
|---|---|
| Enable | Select this if you want this condition to be active. |
| Description | Enter a description for this condition. It can be up to 60 printable ASCII characters long. |
| Authentication | Select whether users must log in (**force**) or whether users do not have to log in (**skip**) when this condition is checked and satisfied. |
| Source Address | Select a source IP address object or select **Create Object** to configure a new one.<br><br>Select **any** if this condition applies to traffic from all source addresses. |
| Destination Address | Select the destination address of traffic to which this condition applies or select **Create Object** to configure a new one. Select **any** if this condition applies to traffic from all destination addresses. |
| Schedule | Select the schedule object that specifies when this condition applies or select **Create Object** to configure a new one (see Chapter 40 on page 677 for details). Select **none** if this condition always applies. |
| OK | Select this to save your changes and return to the previous screen. |
| Cancel | Select this to return to the previous screen without saving any changes. |

## 37.4.3 User Aware Login Example

Access users cannot use the Web Configurator to browse the configuration of the ZyWALL. Instead, when access users log in to the ZyWALL (forced in the screen as shown in Figure 448 on page 657 or otherwise), the following screen appears.

**Figure 451** Web Configurator for Non-Admin Users




The following table describes the labels in this screen.

**Table 205** Web Configurator for Non-Admin Users

| LABEL | DESCRIPTION |
|---|---|
| User-defined lease time (max ... minutes) | Access users can specify a lease time shorter than or equal to the one that you specified. The default value is the lease time that you specified. |
| Renew | Access users can click this button to reset the lease time, the amount of time remaining before the ZyWALL automatically logs them out. The ZyWALL sets this amount of time according to the<br>• **User-defined lease time** field in this screen<br>• **Lease time** field in the **User Add/Edit** screen (see Section 37.2.1 on page 652)<br>• **Lease time** field in the **Setting** screen (see Section 37.4 on page 656) |
| Updating lease time automatically | This box appears if you checked the **Allow renewing lease time automatically** box in the **Setting** screen. (See Section 37.4 on page 656.) Access users can select this check box to reset the lease time automatically 30 seconds before it expires. Otherwise, access users have to click the **Renew** button to reset the lease time. |

**Table 205** Web Configurator for Non-Admin Users (continued)

| LABEL | DESCRIPTION |
|---|---|
| Remaining time before lease timeout | This field displays the amount of lease time that remains, though the user might be able to reset it. |
| Remaining time before auth. timeout | This field displays the amount of time that remains before the ZyWALL automatically logs the access user out, regardless of the lease time. |

# 37.5 User /Group Technical Reference

This section provides some information on users who use an external authentication server in order to log in.

### Setting up User Attributes in an External Server

To set up user attributes, such as reauthentication time, in LDAP or RADIUS servers, use the following keywords in the user configuration file.

**Table 206** LDAP/RADIUS: Keywords for User Attributes

| KEYWORD | CORRESPONDING ATTRIBUTE IN WEB CONFIGURATOR |
|---|---|
| type | **User Type**. Possible Values: admin, limited-admin, user, guest. |
| leaseTime | **Lease Time**. Possible Values: 1-1440 (minutes). |
| reauthTime | **Reauthentication Time**. Possible Values: 1-1440 (minutes). |

The following examples show you how you might set up user attributes in LDAP and RADIUS servers.

**Figure 452** LDAP Example: Keywords for User Attributes

```
type: admin
leaseTime: 99
reauthTime: 199
```

**Figure 453** RADIUS Example: Keywords for User Attributes

```
type=user;leaseTime=222;reauthTime=222
```

### Creating a Large Number of Ext-User Accounts

If you plan to create a large number of **Ext-User** accounts, you might use CLI commands, instead of the Web Configurator, to create the accounts. Extract the user names from the LDAP or RADIUS server, and create a shell script that creates the user accounts. See Chapter 46 on page 781 for more information about shell scripts.

# 38

# Addresses

## 38.1 Overview

Address objects can represent a single IP address or a range of IP addresses. Address groups are composed of address objects and other address groups.

### 38.1.1 What You Can Do Using The Addresses Screens

- The **Address** screen (Section 38.2 on page 665) provides a summary of all addresses in the ZyWALL. Use the **Address Add/Edit** screen to create a new address or edit an existing one.
- Use the **Address Group** summary screen (Section 38.3 on page 668) and the **Address Group Add/Edit** screen, to maintain address groups in the ZyWALL.

### 38.1.2 What You Need To Know About Addresses /Groups

Address objects and address groups are used in dynamic routes, firewall rules, application patrol, content filtering, and VPN connection policies. For example, addresses are used to specify where content restrictions apply in content filtering. Please see the respective sections for more information about how address objects and address groups are used in each one.

Address groups are composed of address objects and address groups. The sequence of members in the address group is not important.

See Section 5.5 on page 96 for related information on these screens.

## 38.2 Address Summary Screen

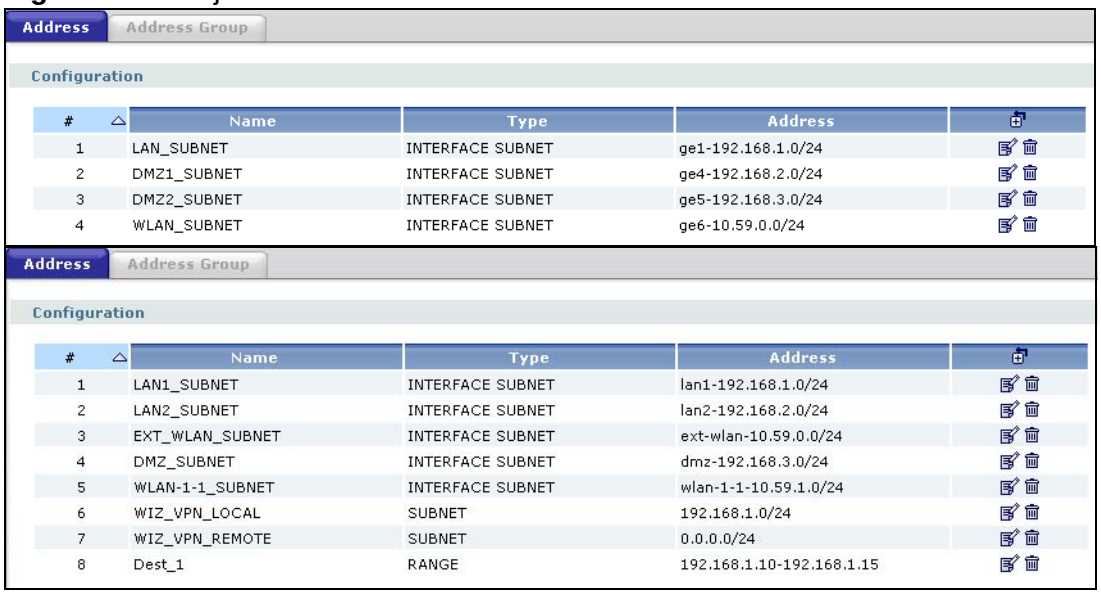
The address screens are used to create, maintain, and remove addresses. There are the types of address objects.

- **HOST** - a host address is defined by an **IP Address**.
- **RANGE** - a range address is defined by a **Starting IP Address** and an **Ending IP Address**.

- **SUBNET** - a network address is defined by a **Network** IP address and **Netmask** subnet mask.

The **Address** screen provides a summary of all addresses in the ZyWALL. To access this screen, click **Object** > **Address > Address**. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

**Figure 454** Object > Address > Address




The following table describes the labels in this screen. See Section 38.2.1 on page 667 for more information as well.

**Table 207** Object > Address > Address

| LABEL | DESCRIPTION |
|---|---|
| # | This field is a sequential value, and it is not associated with a specific address. |
| Name | This field displays the configured name of each address object. |
| Type | This field displays the type of each address object. "**INTERFACE**" means the object uses the settings of one of the ZyWALL's interfaces. |

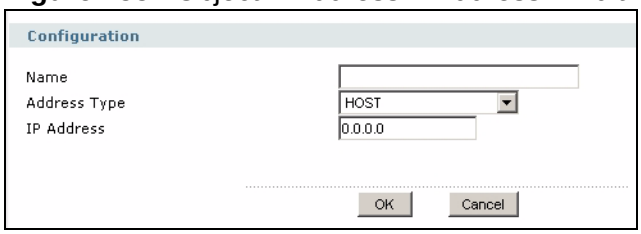
**Table 207** Object > Address > Address (continued)

| LABEL | DESCRIPTION |
|---|---|
| Address | This field displays the IP addresses represented by each address object. If the object's settings are based on one of the ZyWALL's interfaces, the name of the interface displays first followed by the object's current address settings. |
| Add icon | This column provides icons to add, edit, and remove addresses.<br><br>To add an address, click the **Add** icon at the top of the column. The **Address Add/Edit** screen appears.<br><br>To edit an address, click the **Edit** icon next to the address. The **Address Add/Edit** screen appears.<br><br>To delete an address, click on the **Remove** icon next to the address. The Web Configurator confirms that you want to delete the address before doing so. |

## 38.2.1 Address Add/Edit Screen

The **Address Add/Edit** screen allows you to create a new address or edit an existing one. To access this screen, go to the **Address** screen (see Section 38.2 on page 665), and click either the **Add** icon or an **Edit** icon.

**Figure 455** Object > Address > Address > Edit




The following table describes the labels in this screen.

**Table 208** Object > Address > Address > Edit

| LABEL | DESCRIPTION |
|---|---|
| Name | Type the name used to refer to the address. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| Address Type | Select the type of address you want to create. Choices are: **HOST**, **RANGE**, **SUBNET**, **INTERFACE IP**, **INTERFACE SUBNET**, and **INTERFACE GATEWAY**.<br><br>Note: The ZyWALL automatically updates address objects that are based on an interface's IP address, subnet, or gateway if the interface's IP address settings change. For example, if you change ge1's IP address, the ZyWALL automatically updates the corresponding interface-based, LAN subnet address object. |

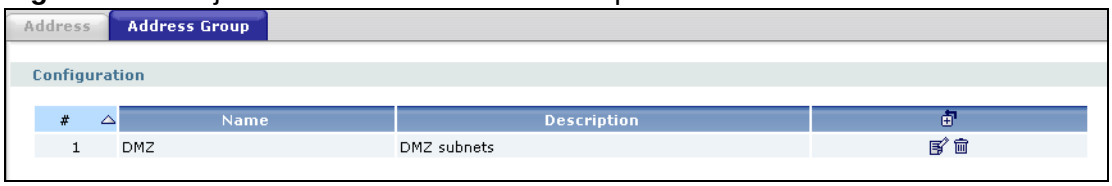
**Table 208** Object > Address > Address > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| IP Address | This field is only available if the **Address Type** is **HOST**. This field cannot be blank. Enter the IP address that this address object represents. |
| Starting IP Address | This field is only available if the **Address Type** is **RANGE**. This field cannot be blank. Enter the beginning of the range of IP addresses that this address object represents. |
| Ending IP Address | This field is only available if the **Address Type** is **RANGE**. This field cannot be blank. Enter the end of the range of IP address that this address object represents. |
| Network | This field is only available if the **Address Type** is **SUBNET**, in which case this field cannot be blank. Enter the IP address of the network that this address object represents. |
| Netmask | This field is only available if the **Address Type** is **SUBNET**, in which case this field cannot be blank. Enter the subnet mask of the network that this address object represents. Use dotted decimal format. |
| Interface | If you selected **INTERFACE IP**, **INTERFACE SUBNET**, or **INTERFACE GATEWAY** as the **Address Type**, use this field to select the interface of the network that this address object represents. |
| OK | Click **OK** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving your changes. |

# 38.3 Address Group Summary Screen

The **Address Group** screen provides a summary of all address groups. To access this screen, click **Object** > **Address > Address Group**. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

**Figure 456** Object > Address > Address Group




The following table describes the labels in this screen. See Section 38.3.1 on page 669 for more information as well.

**Table 209** Object > Address > Address Group

| LABEL | DESCRIPTION |
|---|---|
| # | This field is a sequential value, and it is not associated with a specific address group. |
| Name | This field displays the name of each address group. |

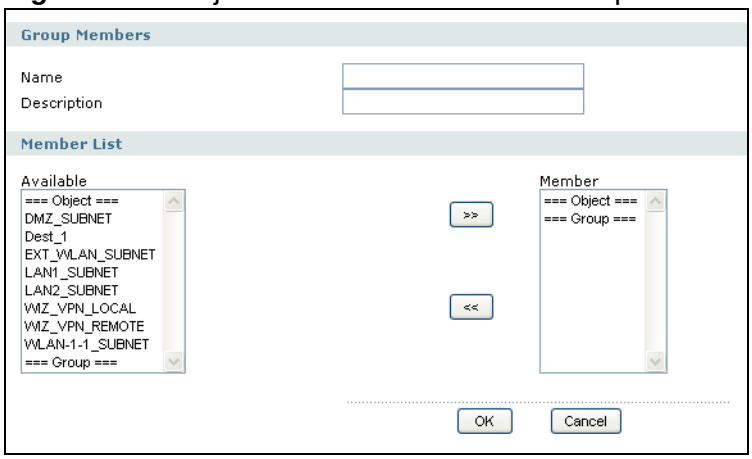
**Table 209** Object > Address > Address Group (continued)

| LABEL | DESCRIPTION |
|---|---|
| Description | This field displays the description of each address group, if any. |
| Add icon | This column provides icons to add, edit, and remove address groups.<br><br>To add an address group, click the **Add** icon at the top of the column. The **Address Group Add/Edit** screen appears.<br><br>To edit an address group, click the **Edit** icon next to the address group. The **Address Group Add/Edit** screen appears.<br><br>To delete an address group, click on the **Remove** icon next to the address group. The Web Configurator confirms that you want to delete the address group. |

## 38.3.1 Address Group Add/Edit Screen

The **Address Group Add/Edit** screen allows you to create a new address group or edit an existing one. To access this screen, go to the **Address Group** screen (see Section 38.3 on page 668), and click either the **Add** icon or an **Edit** icon.

**Figure 457** Object > Address > Address Group > Add




The following table describes the labels in this screen.

**Table 210** Object > Address > Address Group > Add

| LABEL | DESCRIPTION |
|---|---|
| Name | Enter a name for the address group. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| Description | This field displays the description of each address group, if any. You can use up to 60 characters, punctuation marks, and spaces. |
| Available | This field displays the names of the address and address group objects that can be added to the address group.<br><br>Select address and address group objects that you want to be members of this group and click the right arrow to add them to the member list. |

**Table 210** Object > Address > Address Group > Add (continued)

| LABEL | DESCRIPTION |
|---|---|
| Member | This field displays the names of the address and address group objects that have been added to the address group. The order of members is not important. To remove members, select them and click the left arrow. |
| OK | Click **OK** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving your changes. |

# 39

# Services

## 39.1 Overview

Use service objects to define TCP applications, UDP applications, and ICMP messages. You can also create service groups to refer to multiple service objects in other features.

### 39.1.1 What You Can Do in the Services Screens

- Use the **Service** screens (Section 39.2 on page 672) to view and configure the ZyWALL's list of services and their definitions.
- Use the **Service Group** screens (Section 39.2 on page 672) to view and configure the ZyWALL's list of service groups.

### 39.1.2 What You Need to Know About Protocols

#### IP Protocols

IP protocols are based on the eight-bit protocol field in the IP header. This field represents the next-level protocol that is sent in this packet. This section discusses three of the most common IP protocols.

Computers use Transmission Control Protocol (TCP, IP protocol 6) and User Datagram Protocol (UDP, IP protocol 17) to exchange data with each other. TCP guarantees reliable delivery but is slower and more complex. Some uses are FTP, HTTP, SMTP, and TELNET. UDP is simpler and faster but is less reliable. Some uses are DHCP, DNS, RIP, and SNMP.

TCP creates connections between computers to exchange data. Once the connection is established, the computers exchange data. If data arrives out of sequence or is missing, TCP puts it in sequence or waits for the data to be re-transmitted. Then, the connection is terminated.

In contrast, computers use UDP to send short messages to each other. There is no guarantee that the messages arrive in sequence or that the messages arrive at all.

Both TCP and UDP use ports to identify the source and destination. Each port is a 16-bit number. Some port numbers have been standardized and are used by low-level system processes; many others have no particular meaning.

Unlike TCP and UDP, Internet Control Message Protocol (ICMP, IP protocol 1) is mainly used to send error messages or to investigate problems. For example, ICMP is used to send the response if a computer cannot be reached. Another use is ping. ICMP does not guarantee delivery, but networks often treat ICMP messages differently, sometimes looking at the message itself to decide where to send it.

### Service Objects and Service Groups

Use service objects to define IP protocols.

- TCP applications
- UDP applications
- ICMP messages
- user-defined services (for other types of IP protocols)

These objects are used in policy routes, firewall rules, and IDP profiles.

Use service groups when you want to create the same rule for several services, instead of creating separate rules for each service. Service groups may consist of services and other service groups. The sequence of members in the service group is not important.

### Finding Out More

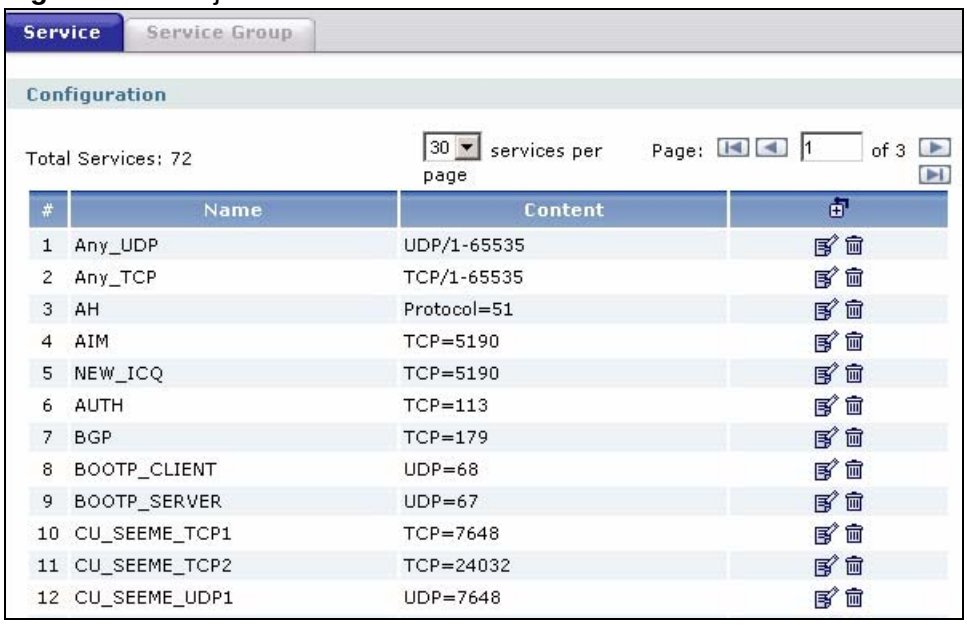
- See Section 5.5 on page 96 for related information on these screens.
- See Appendix B on page 905 for a list of commonly-used services.

## 39.2 The Service Summary Screen

The **Service** summary screen provides a summary of all services and their definitions. In addition, this screen allows you to add, edit, and remove services.

To access this screen, log in to the Web Configurator, and click **Object > Service > Service**. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

**Figure 458** Object > Service > Service




The following table describes the labels in this screen.

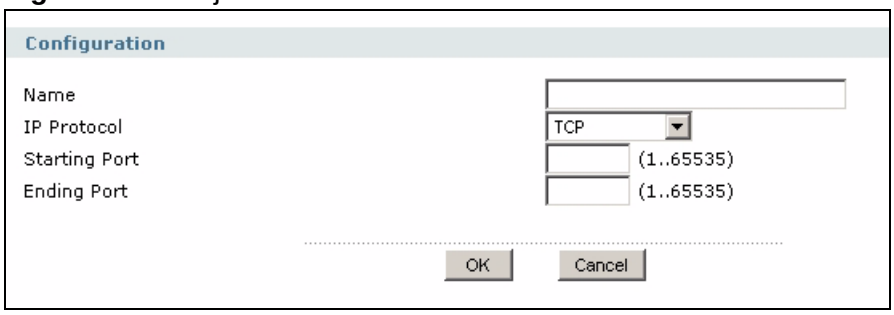
**Table 211** Object > Service > Service

| LABEL | DESCRIPTION |
|---|---|
| Total Services | This displays the total number of services configured on the ZyWALL. |
| services per page | Select the number of services you want to appear per page here. |
| Page x of x | This is the number of the page of entries currently displayed and the total number of pages of entries. Type a page number to go to or use the arrows to navigate the pages of entries. |
| # | This field is a sequential value, and it is not associated with a specific service. |
| Name | This field displays the name of each service. |
| Content | This field displays a description of each service. |
| Add icon | This column provides icons to add, edit, and remove services.<br><br>To add a service, click the **Add** icon at the top of the column. The **Service Add/Edit** screen appears.<br><br>To edit a service, click the **Edit** icon next to the service. The **Service Add/Edit** screen appears.<br><br>To delete a service, click the **Remove** icon next to the service. The Web Configurator confirms that you want to delete the service before doing so. |

### 39.2.1 The Service Add/Edit Screen

The **Service Add/Edit** screen allows you to create a new service or edit an existing one. To access this screen, go to the **Service** screen (see Section 39.2 on page 672), and click either the **Add** icon or an **Edit** icon.

**Figure 459** Object > Service > Service > Edit




The following table describes the labels in this screen.

**Table 212** Object > Service > Service > Edit

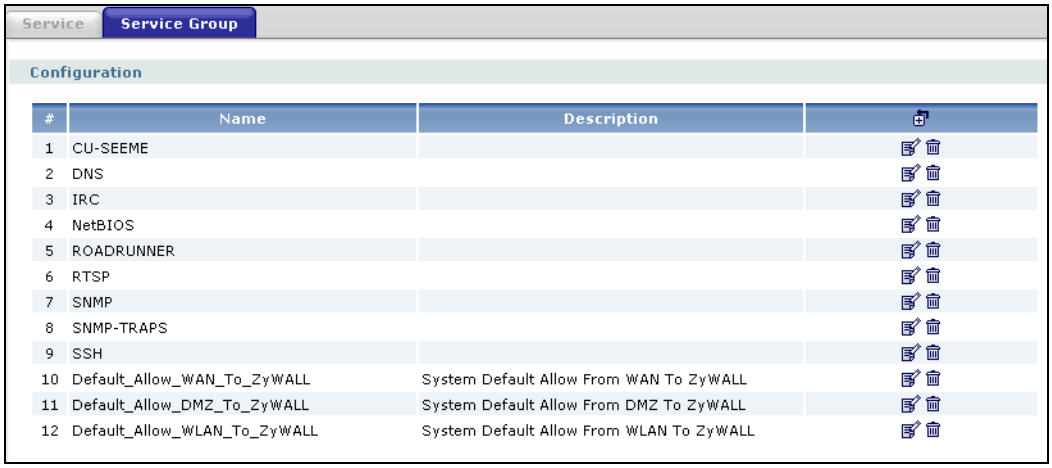
| LABEL | DESCRIPTION |
|---|---|
| Name | Type the name used to refer to the service. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| IP Protocol | Select the protocol the service uses. Choices are: **TCP**, **UDP**, **ICMP**, and **User Defined**. |
| Starting Port<br><br>Ending Port | This field appears if the **IP Protocol** is **TCP** or **UDP**. Specify the port number(s) used by this service. If you fill in one of these fields, the service uses that port. If you fill in both fields, the service uses the range of ports. |
| ICMP Type | This field appears if the **IP Protocol** is **ICMP Type**.<br><br>Select the ICMP message used by this service. This field displays the message text, not the message number. |
| IP Protocol Number | This field appears if the **IP Protocol** is **User Defined**.<br><br>Enter the number of the next-level protocol (IP protocol). Allowed values are 0 - 255. |
| OK | Click **OK** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving your changes. |

## 39.3 The Service Group Summary Screen

The **Service Group** summary screen provides a summary of all service groups. In addition, this screen allows you to add, edit, and remove service groups.

To access this screen, log in to the Web Configurator, and click **Object** > **Service** > **Service Group**.

**Figure 460** Object > Service > Service Group




The following table describes the labels in this screen. See Section 39.3.1 on page 676 for more information as well.

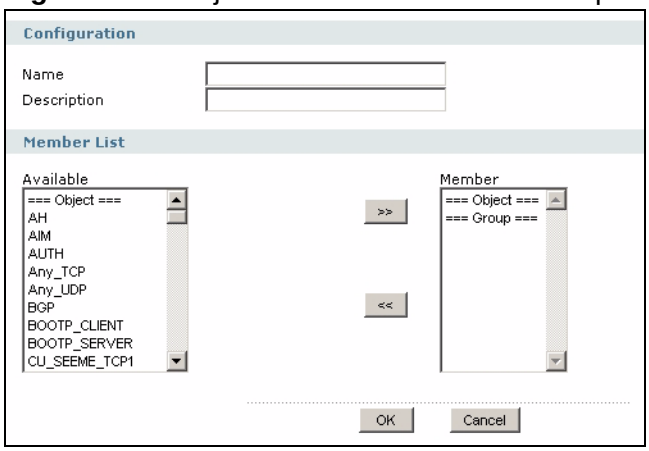
**Table 213** Object > Service > Service Group

| LABEL | DESCRIPTION |
|---|---|
| # | This field is a sequential value, and it is not associated with a specific service group. |
| Name | This field displays the name of each service group.<br><br>By default, the ZyWALL uses services starting with “Default_Allow_” in the firewall rules to allow certain services to connect to the ZyWALL. |
| Description | This field displays the description of each service group, if any. |
| Add icon | This column provides icons to add, edit, and remove service groups.<br><br>To add a service group, click the **Add** icon at the top of the column. The **Service Group Add/Edit** screen appears.<br><br>To edit a service group, click the **Edit** icon next to the service group. The **Service Group Add/Edit** screen appears.<br><br>To delete a service group, click on the **Remove** icon next to the service group. The Web Configurator confirms that you want to delete the service group. |

## 39.3.1 The Service Group Add/Edit Screen

The **Service Group Add/Edit** screen allows you to create a new service group or edit an existing one. To access this screen, go to the **Service Group** screen (see Section 39.3 on page 674), and click either the **Add** icon or an **Edit** icon.

**Figure 461** Object > Service > Service Group > Edit




The following table describes the labels in this screen.

**Table 214** Object > Service > Service Group > Edit

| LABEL | DESCRIPTION |
|---|---|
| Name | Enter the name of the service group. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| Description | Enter a description of the service group, if any. You can use up to 60 printable ASCII characters. |
| Available | This field displays the names of the service and service group objects that can be added to the service group.<br><br>Select service and service group objects that you want to be members of this group and click the right arrow to add them to the member list. |
| Member | This field displays the names of the service and service group objects that have been added to the service group. The order of members is not important. To remove members, select them and click the left arrow. |
| OK | Click **OK** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving your changes. |

# 40

# Schedules

## 40.1 Overview

Use schedules to set up one-time and recurring schedules for policy routes, firewall rules, application patrol, and content filtering. The ZyWALL supports one-time and recurring schedules. One-time schedules are effective only once, while recurring schedules usually repeat. Both types of schedules are based on the current date and time in the ZyWALL.

Note: Schedules are based on the ZyWALL's current date and time.

### 40.1.1 What You Can Do in the Schedule Screens

- Use the **Schedule** summary screen (Section 40.2 on page 678) to see a list of all schedules in the ZyWALL.
- Use the **One-Time Schedule Add / Edit** screen (Section 40.2.1 on page 679) to create or edit a one-time schedule.
- Use the **Recurring Schedule Add / Edit** screen (Section 40.2.2 on page 680) to create or edit a recurring schedule.

### 40.1.2 What You Need to Know About Schedules

#### One-time Schedules

One-time schedules begin on a specific start date and time and end on a specific stop date and time. One-time schedules are useful for long holidays and vacation periods.

#### Recurring Schedules

Recurring schedules begin at a specific start time and end at a specific stop time on selected days of the week (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday). Recurring schedules always begin and end in the same day. Recurring schedules are useful for defining the workday and off-work hours.

### Finding Out More

- See Section 5.5 on page 96 for related information on these screens.
- See Section 45.3 on page 732 for information about the ZyWALL's current date and time.

## 40.2 The Schedule Summary Screen

The **Schedule** summary screen provides a summary of all schedules in the ZyWALL. To access this screen, click **Object** > **Schedule**.

**Figure 462** Object > Schedule


The following table describes the labels in this screen. See Section 40.2.1 on page 679 and Section 40.2.2 on page 680 for more information as well.

**Table 215** Object > Schedule

| LABEL | DESCRIPTION |
|---|---|
| One Time | |
| # | This field is a sequential value, and it is not associated with a specific schedule. |
| Name | This field displays the name of the schedule, which is used to refer to the schedule. |
| Start Day / Time | This field displays the date and time at which the schedule begins. |
| Stop Day / Time | This field displays the date and time at which the schedule ends. |
| Add icon | This column provides icons to add, edit, and remove schedules.<br>To add a schedule, click the **Add** icon at the top of the column. The **Schedule Add / Edit** screen appears.<br>To edit a schedule, click the **Edit** icon next to the schedule. The **Schedule Add / Edit** screen appears.<br>To delete a schedule, click the **Remove** icon next to the schedule. The Web Configurator confirms that you want to delete the schedule before doing so. |
| Recurring | |

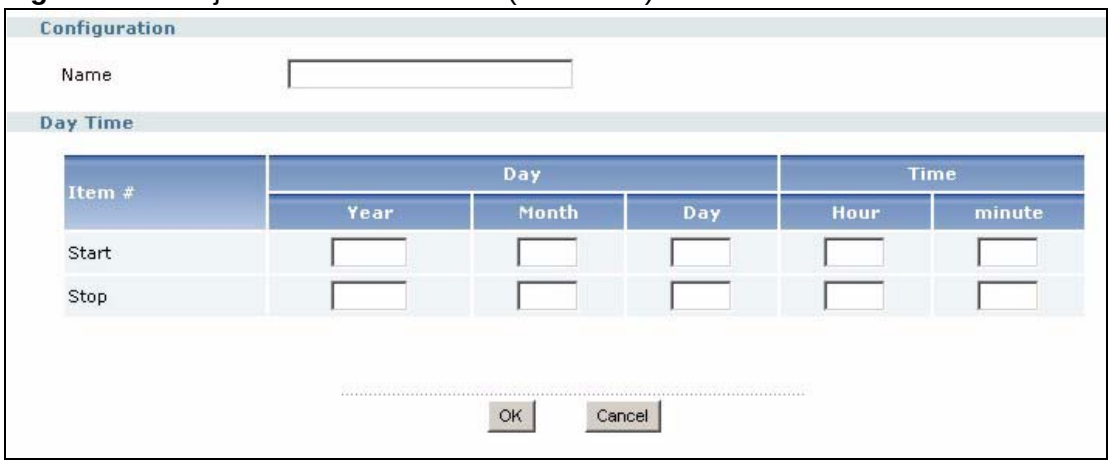
**Table 215** Object > Schedule (continued)

| LABEL | DESCRIPTION |
|---|---|
| # | This field is a sequential value, and it is not associated with a specific schedule. |
| Name | This field displays the name of the schedule, which is used to refer to the schedule. |
| Start Time | This field displays the time at which the schedule begins. |
| Stop Time | This field displays the time at which the schedule ends. |
| Add icon | This column provides icons to add, edit, and remove schedules.<br><br>To add a schedule, click the **Add** icon at the top of the column. The **Schedule Add / Edit** screen appears.<br><br>To edit a schedule, click the **Edit** icon next to the schedule. The **Schedule Add / Edit** screen appears.<br><br>To delete a schedule, click the **Remove** icon next to the schedule. The Web Configurator confirms that you want to delete the schedule before doing so. |

## 40.2.1 The One-Time Schedule Add/Edit Screen

The **One-Time Schedule Add / Edit** screen allows you to define a one-time schedule or edit an existing one. To access this screen, go to the **Schedule** screen (see Section 40.2 on page 678), and click either the **Add** icon or an **Edit** icon in the **One Time** section.

**Figure 463** Object > Schedule > Edit (One Time)



The following table describes the labels in this screen.

**Table 216** Object > Schedule > Edit (One Time)

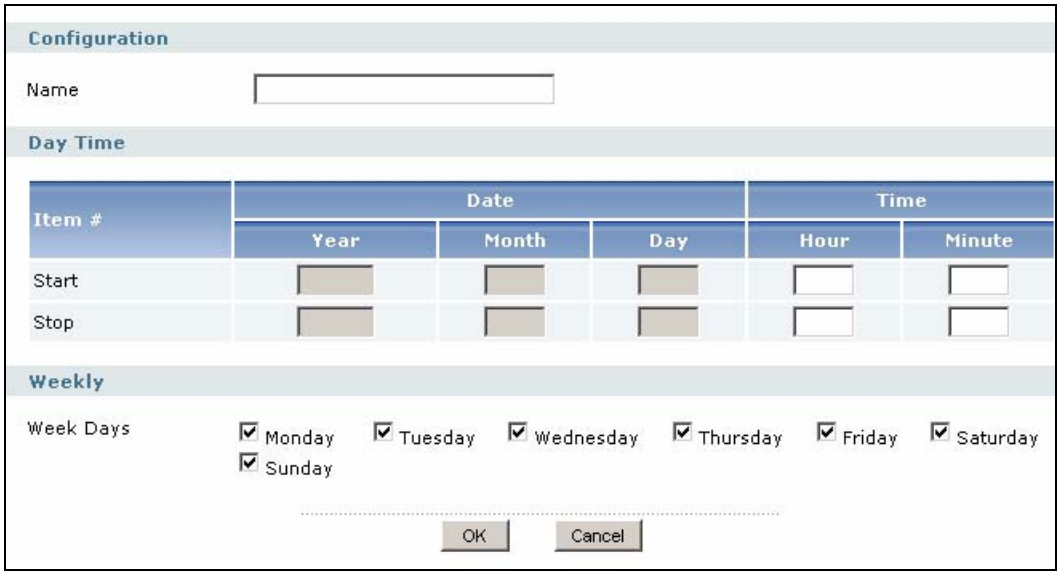
| LABEL | DESCRIPTION |
|---|---|
| Configuration | |
| Name | Type the name used to refer to the one-time schedule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| Date Time | |
| Start | Type the year, month, day, hour, and minute when the schedule begins.<br>**Year** - 1900 - 2999<br>**Month** - 1 - 12<br>**Day** - 1 - 31 (it is not possible to specify illegal dates, such as February 31.)<br>**Hour** - 0 - 23<br>**Minute** - 0 - 59<br>All of these fields are required. |
| Stop | Type the year, month, day, hour, and minute when the schedule ends.<br>**Year** - 1900 - 2999<br>**Month** - 1 - 12<br>**Day** - 1 - 31 (it is not possible to specify illegal dates, such as February 31.)<br>**Hour** - 0 - 23<br>**Minute** - 0 - 59<br>All of these fields are required. |
| OK | Click **OK** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving your changes. |

## 40.2.2 The Recurring Schedule Add/Edit Screen

The **Recurring Schedule Add/Edit** screen allows you to define a recurring schedule or edit an existing one. To access this screen, go to the **Schedule** screen

(see Section 40.2 on page 678), and click either the **Add** icon or an **Edit** icon in the **Recurring** section.

**Figure 464** Object > Schedule > Edit (Recurring)




The **Year**, **Month**, and **Day** columns are not used in recurring schedules and are disabled in this screen. The following table describes the remaining labels in this screen.

**Table 217** Object > Schedule > Edit (Recurring)

| LABEL | DESCRIPTION |
|---|---|
| Configuration | |
| Name | Type the name used to refer to the recurring schedule. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. |
| Date Time | |
| Start | Type the hour and minute when the schedule begins each day.<br>**Year** - disabled<br>**Month** - disabled<br>**Day** - disabled<br>**Hour** - 0 - 23<br>**Minute** - 0 - 59<br>The **Hour** and **Minute** fields are both required.<br>To set all day (24 hours), configure the start hour and minute both to 0. |

**Table 217** Object > Schedule > Edit (Recurring) (continued)

| LABEL | DESCRIPTION |
|---|---|
| Stop | Type the hour and minute when the schedule ends each day.<br>**Year** - disabled<br>**Month** - disabled<br>**Day** - disabled<br>**Hour** - 0 - 23<br>**Minute** - 0 - 59<br>The **Hour** and **Minute** fields are both required.<br>To set all day (24 hours), configure the stop hour to 23 and minute to 59. |
| Weekly | |
| Week Days | Select each day of the week the recurring schedule is effective. |
| OK | Click **OK** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving your changes. |

# 41

# AAA Server

## 41.1 Overview

You can use a AAA (Authentication, Authorization, Accounting) server to provide access control to your network. The AAA server can be a Active Directory, LDAP, or RADIUS server. Use the **AAA Server** screens to create and manage objects that contain settings for using individual AAA servers or groups of AAA servers. You use AAA server objects in configuring authentication method objects (see Chapter 42 on page 695).

### 41.1.1 Directory Service (AD/LDAP) Overview

LDAP/AD allows a client (the ZyWALL) to connect to a server to retrieve information from a directory. A network example is shown next.

**Figure 465** Example: Directory Service Client and Server

The following describes the user authentication procedure via an LDAP/AD server.

1. A user logs in with a user name and password pair.
2. The ZyWALL tries to bind (or log in) to the LDAP/AD server.
3. When the binding process is successful, the ZyWALL checks the user information in the directory against the user name and password pair.
4. If it matches, the user is allowed access. Otherwise, access is blocked.

## 41.1.2 RADIUS Server Overview

RADIUS (Remote Authentication Dial-In User Service) authentication is a popular protocol used to authenticate users by means of an external server instead of (or in addition to) an internal device user database that is limited to the memory capacity of the device. In essence, RADIUS authentication allows you to validate a large number of users from a central location.

**Figure 466** RADIUS Server Network Example

## 41.1.3 ASAS

ASAS (Authenex Strong Authentication System) is a RADIUS server that works with the One-Time Password (OTP) feature. Purchase a ZyWALL OTP package in order to use this feature. The package contains server software and physical OTP tokens (PIN generators). Do the following to use OTP. See the documentation included on the ASAS' CD for details.

1. Install the ASAS server software on a computer.
2. Create user accounts on the ZyWALL and in the ASAS server.
3. Import each token's database file (located on the included CD) into the server.
4. Assign users to OTP tokens (on the ASAS server).
5. Configure the ASAS as a RADIUS server in the ZyWALL's **Object > AAA Server** screens.
6. Give the OTP tokens to (local or remote) users.

## 41.1.4 What You Can Do Using The AAA Screens

- Use the **Object > AAA Server > Active Directory** (or **LDAP**) screens (Section 41.2.1 on page 687) to configure the Active Directory or LDAP default server settings.
- Use the **Object > AAA Server > RADIUS** screen (Section 41.4 on page 690) to configure the default external RADIUS server to use for user authentication.

### 41.1.5 What You Need To Know About AAA Servers

#### AAA Servers Supported by the ZyWALL

The following lists the types of authentication server the ZyWALL supports.

- Local user database

  The ZyWALL uses the built-in local user database to authenticate administrative users logging into the ZyWALL's Web Configurator or network access users logging into the network through the ZyWALL. You can also use the local user database to authenticate VPN users.

- Directory Service (LDAP/AD)

  LDAP (Lightweight Directory Access Protocol)/AD (Active Directory) is a directory service that is both a directory and a protocol for controlling access to a network. The directory consists of a database specialized for fast information retrieval and filtering activities. You create and store user profile and login information on the external server.

- RADIUS

  RADIUS (Remote Authentication Dial-In User Service) authentication is a popular protocol used to authenticate users by means of an external or built-in RADIUS server. RADIUS authentication allows you to validate a large number of users from a central location.

#### Finding Out More

See Section 6.6.3 on page 129 for an example of how to set up user authentication using a radius server.

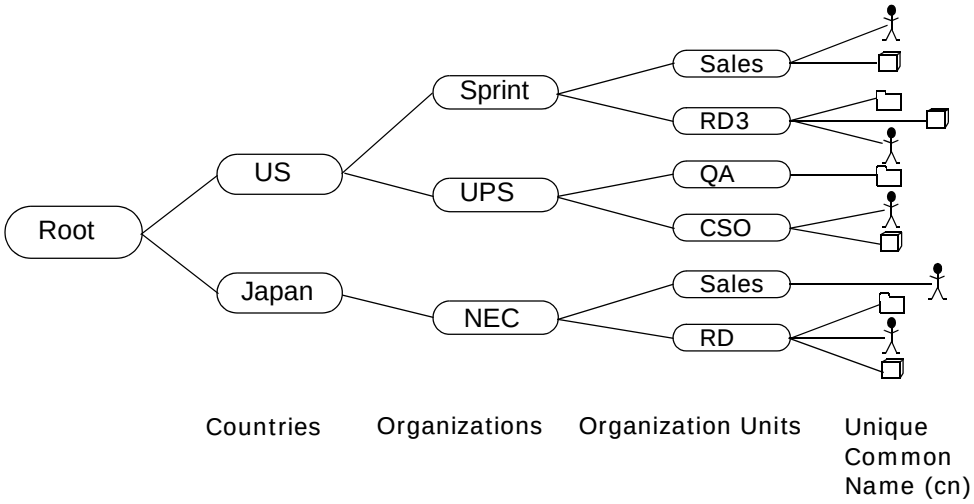
## 41.2 Active Directory or LDAP Default Server Screen

#### Directory Structure

The directory entries are arranged in a hierarchical order much like a tree structure. Normally, the directory structure reflects the geographical or

organizational boundaries. The following figure shows a basic directory structure branching from countries to organizations to organizational units to individuals.

**Figure 467** Basic Directory Structure




## Distinguished Name (DN)

A DN uniquely identifies an entry in a directory. A DN consists of attribute-value pairs separated by commas. The leftmost attribute is the Relative Distinguished Name (RDN). This provides a unique name for entries that have the same "parent DN" ("cn=domain1.com, ou=Sales, o=MyCompany" in the following examples).

```
cn=domain1.com, ou = Sales, o=MyCompany, c=US
cn=domain1.com, ou = Sales, o=MyCompany, c=JP
```

## Base DN

A base DN specifies a directory. A base DN usually contains information such as the name of an organization, a domain name and/or country. For example, o=MyCompany, c=UK where o means organization and c means country.

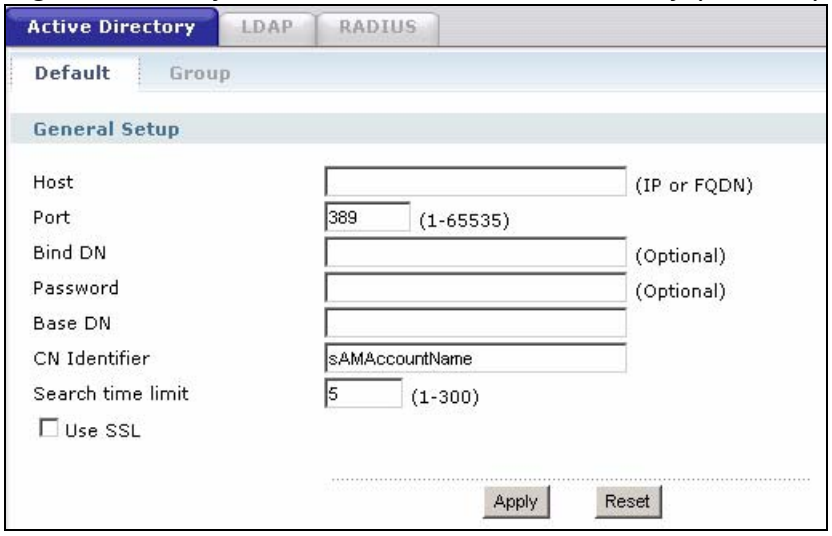
## Bind DN

A bind DN is used to authenticate with an LDAP/AD server. For example a bind DN of cn=zywallAdmin allows the ZyWALL to log into the LDAP/AD server using the user name of zywallAdmin. The bind DN is used in conjunction with a bind password. When a bind DN is not specified, the ZyWALL will try to log in as an anonymous user. If the bind password is incorrect, the login will fail.

## 41.2.1 Configuring Active Directory or LDAP Default Server Settings

To configure the Active Directory or LDAP default server settings, click **Object > AAA Server > Active Directory** (or **LDAP**) to display the screen as shown.

**Figure 468** Object > AAA Server > Active Directory (or LDAP) > Default




The following table describes the labels in this screen.

**Table 218** Object > AAA Server > Active Directory (or LDAP) > Default

| LABEL | DESCRIPTION |
|---|---|
| Host | Enter the IP address (in dotted decimal notation) or the fully-qualified domain name (up to 63 alphanumerical characters) of an AD or LDAP server. |
| Port | Specify the port number on the AD or LDAP server to which the ZyWALL sends authentication requests. Enter a number between 1 and 65535. The default is **389**. |
| Bind DN | Specify the bind DN for logging into the AD or LDAP server. Enter up to 127 alphanumerical characters.<br><br>For example, `cn=zywallAdmin` specifies `zywallAdmin` as the user name. |
| Password | If required, enter the password (up to 15 alphanumerical characters) for the ZyWALL to bind (or log in) to the AD or LDAP server. |
| Base DN | Specify the directory (up to 127 alphanumerical characters). For example, `o=ZyXEL, c=US`. |
| CN Identifier | Specify the unique common name that uniquely identifies a record in the AD or LDAP directory. Enter up to 127 alphanumerical characters. |
| Search time limit | Specify the timeout period (between 1 and 300 seconds) before the ZyWALL disconnects from the AD or LDAP server. In this case, user authentication fails.<br><br>The search timeout occurs when either the user information is not in the AD or LDAP server or the server is down. |

**Table 218** Object > AAA Server > Active Directory (or LDAP) > Default (continued)

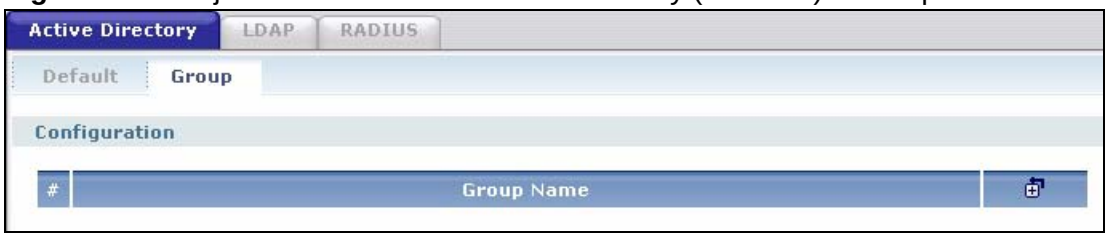
| LABEL | DESCRIPTION |
|---|---|
| Use SSL | Select **Use SSL** to establish a secure connection to the AD or LDAP server. |
| Apply | Click **Apply** to save the changes. |
| Reset | Click **Reset** to start configuring this screen again. |

# 41.3 Active Directory or LDAP Group Summary Screen

You can configure a group of AD or LDAP servers in the **Active Directory** (or **LDAP**) **> Group** screen. This is useful if you have more than one AD server or more than one LDAP server for user authentication in a network. You can create up to 16 AD server groups with up to four members in each group on the ZyWALL. You can also create up to 16 LDAP server groups with up to four members in each group on the ZyWALL.

Click **Object > AAA Server > Active Directory** (or **LDAP**) **> Group** to display the **Active Directory** (or **LDAP**) **> Group** screen.

**Figure 469** Object > AAA Server > Active Directory (or LDAP) > Group




The following table describes the labels in this screen.

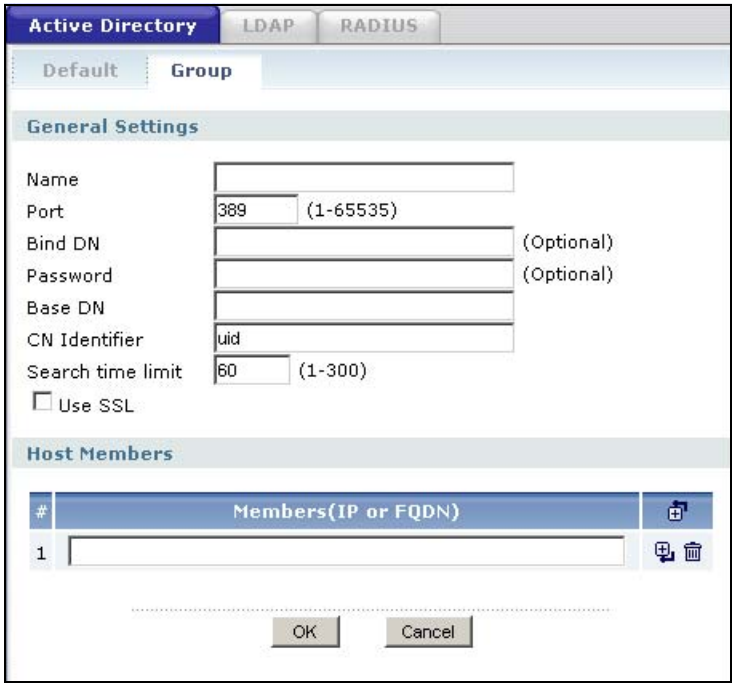
**Table 219** Object > AAA Server > Active Directory (or LDAP) > Group

| LABEL | DESCRIPTION |
|---|---|
| # | This field displays the index number. |
| Group Name | This field displays the descriptive name for identification purposes. |
| Add icon | Click **Add** to add a new entry.<br>Click **Edit** to edit the settings of an entry.<br>Click **Delete** to remove an entry. |

## 41.3.1 Creating an Active Directory or LDAP Group

Click **Object > AAA Server > Active Directory** (or **LDAP**) **> Group** to display the **Active Directory** (or **LDAP**) **> Group** screen. Click the **Add** icon or an **Edit** icon to display the configuration fields.

**Figure 470** Object > AAA Server > Active Directory (or LDAP) > Group > Add




The following table describes the labels in this screen.

**Table 220** Object > AAA Server > Active Directory (or LDAP) > Group > Add

| LABEL | DESCRIPTION |
|---|---|
| General Settings | All AD or LDAP servers in a group share the same settings in the fields below. |
| Host | Enter a descriptive name (up to 63 alphanumerical characters). for identification purposes. |
| Port | Specify the port number on the AD or LDAP server(s) to which the ZyWALL sends authentication requests. Enter a number between 1 and 65535.<br><br>This port number should be the same on all AD or LDAP server(s) in this group. |
| Bind DN | Specify the bind DN for logging into the AD or LDAP server. Enter up to 127 alphanumerical characters.<br><br>For example, `cn=zywallAdmin` specifies `zywallAdmin` as the user name. |
| Password | If required, enter the password (up to 15 alphanumerical characters) for the ZyWALL to bind (or log in) to the AD or LDAP server. |

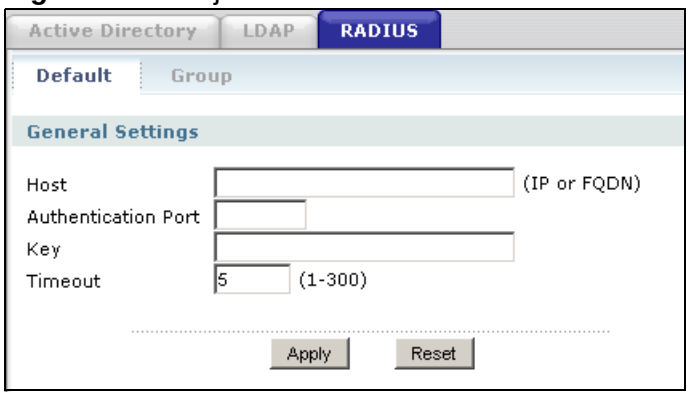
**Table 220** Object > AAA Server > Active Directory (or LDAP) > Group > Add

| LABEL | DESCRIPTION |
|---|---|
| Base DN | Specify the directory (up to 127 alphanumerical characters). For example, o=ZyXEL, c=US. |
| CN Identifier | Specify the unique common name that uniquely identifies a record in the AD or LDAP directory. Enter up to 127 alphanumerical characters. |
| Search time limit | Specify the timeout period (between 1 and 300 seconds) before the ZyWALL disconnects from the AD or LDAP server. In this case, user authentication fails.<br><br>Search timeout occurs when either the user information is not in the AD or LDAP server(s) or the AD or LDAP server(s) is down. |
| Use SSL | Select **Use SSL** to establish a secure connection to the AD or LDAP server(s). |
| Host Members | The ordering of the LDAP servers is important as the ZyWALL uses the AD or LDAP servers for user authentication in the order they appear in this table. |
| # | This field displays the index number. |
| Members | Specify the URI (Uniform Resource Identifier) of an AD or LDAP server. You can enter the IP address (in dotted decimal notation) or the fully qualified domain name (FQDN; up to 63 alphanumerical characters) of the AD or LDAP server. |
| Add icon | Click **Add** to add a new AD or LDAP server. You can add up to four AD or LDAP member servers.<br><br>Click **Delete** to remove an AD or LDAP server. |
| OK | Click **OK** to save the changes. |
| Cancel | Click **Cancel** to discard the changes. |

# 41.4 Configuring a Default RADIUS Server

To configure the default external RADIUS server to use for user authentication, click **Object > AAA Server > RADIUS** to display the screen as shown.

**Figure 471** Object > AAA Server > RADIUS > Default



The following table describes the labels in this screen.

**Table 221** Object > AAA Server > RADIUS > Default

| LABEL | DESCRIPTION |
|---|---|
| Host | Enter the IP address (in dotted decimal notation) or the domain name (up to 63 alphanumeric characters) of a RADIUS server. |
| Authentication Port | The default port of the RADIUS server for authentication is **1812**.<br>You need not change this value unless your network administrator instructs you to do so with additional information. |
| Key | Enter a password (up to 15 alphanumeric characters) as the key to be shared between the external authentication server and the ZyWALL.<br>The key is not sent over the network. This key must be the same on the external authentication server and the ZyWALL. |
| Timeout | Specify the timeout period (between 1 and 300 seconds) before the ZyWALL disconnects from the RADIUS server. In this case, user authentication fails.<br>Search timeout occurs when either the user information is not in the RADIUS server or the RADIUS server is down. |
| Apply | Click **Apply** to save the changes. |
| Reset | Click **Reset** to start configuring this screen again. |

# 41.5 Configuring a Group of RADIUS Servers

You can configure a group of RADIUS servers in the **RADIUS > Group** screen. This is useful if you have more than one authentication server for user authentication in a network.

Click **Object > AAA Server > RADIUS > Group** to display the **RADIUS > Group** screen.

**Figure 472** Object > AAA Server > RADIUS > Group


The following table describes the labels in this screen.

**Table 222** Object > AAA Server > RADIUS > Group

| LABEL | DESCRIPTION |
|---|---|
| # | This field displays the index number. |

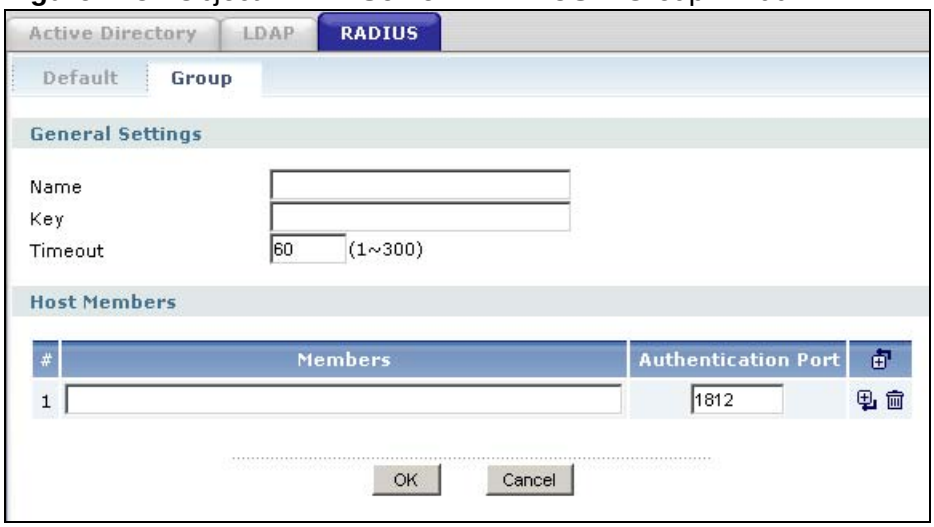
**Table 222** Object > AAA Server > RADIUS > Group (continued)

| LABEL | DESCRIPTION |
|---|---|
| Group Name | This field displays the descriptive name for identification purposes. |
| Add icon | Click **Add** to add a new entry.<br>Click **Edit** to edit the settings of an entry.<br>Click **Delete** to remove an entry. |

## 41.5.1 Adding a RADIUS Server Member

Click **Object > AAA Server > RADIUS > Group** to display the **RADIUS > Group** screen. Click the **Add** icon or an **Edit** icon to display the configuration fields.

**Figure 473** Object > AAA Server > RADIUS > Group > Add




The following table describes the labels in this screen.

**Table 223** Object > AAA Server > RADIUS > Group > Add

| LABEL | DESCRIPTION |
|---|---|
| General Settings | All RADIUS servers in a group share the same settings in the fields below. |
| Name | Enter a descriptive name (up to 63 alphanumeric characters) for identification purposes. |
| Key | Enter a password (up to 15 alphanumeric characters) as the key to be shared between the external authentication server and the ZyWALL.<br>The key is not sent over the network. This key must be the same on the external authentication server and the ZyWALL. |

**Table 223** Object > AAA Server > RADIUS > Group > Add (continued)

| LABEL | DESCRIPTION |
|---|---|
| Timeout | Specify the timeout period (between 1 and 300 seconds) before the ZyWALL disconnects from the RADIUS server. In this case, user authentication fails.<br><br>Search timeout occurs when either the user information is not in the RADIUS server or the RADIUS server is down. |
| Host Members | The ordering of the RADIUS servers is important as the ZyWALL uses the RADIUS servers for user authentication in the order they appear in this table. |
| # | This field displays the index number. |
| Members | Enter the IP address (in dotted decimal notation) or the domain name (up to 63 alphanumeric characters) of a RADIUS server. |
| Authentication Port | The default port of the RADIUS server for authentication is **1812**.<br><br>You need not change this value unless your network administrator instructs you to do so with additional information. |
| Add icon | Click **Add** to add a new RADIUS server. You can add up to four RADIUS member servers.<br><br>Click **Delete** to remove a RADIUS server. |
| OK | Click **OK** to save the changes. |
| Cancel | Click **Cancel** to discard the changes. |

# 42

# Authentication Method

## 42.1 Overview

Authentication method objects set how the ZyWALL authenticates wireless, HTTP/HTTPS clients, peer IPSec routers (extended authentication), and L2TP VPN clients. Configure authentication method objects to have the ZyWALL use the local user database, and/or the authentication servers and authentication server groups specified by AAA server objects. By default, user accounts created and stored on the ZyWALL are authenticated locally.

### 42.1.1 What You Can Do Using The Auth. Method Screens

- Use the **Object > Auth. Method** screen (Section 42.2 on page 696) to view authentication method objects.
- Use the **Object > Auth. Method > Add** screen (Section 42.3 on page 697) to create a new authentication method object.

#### Finding Out More

See Section 6.6.3 on page 129 for an example of how to set up user authentication using a radius server.

### 42.1.2 Before You Begin

Configure AAA server objects (see Chapter 41 on page 683) before you configure authentication method objects.

### 42.1.3 Example: Selecting a VPN Authentication Method

After you set up an authentication method object in the **Auth. Method** screens, you can use it in the **VPN Gateway** screen to authenticate VPN users for establishing a VPN connection. Refer to the chapter on VPN for more information.

Follow the steps below to specify the authentication method for a VPN connection.

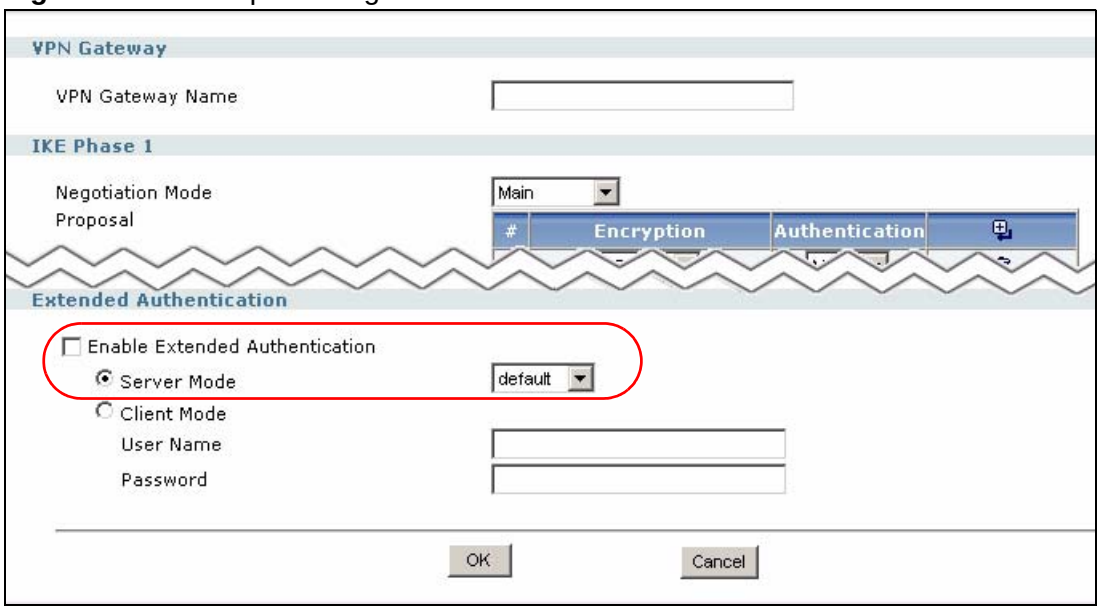
1 Access the **VPN > IPSec VPN > VPN Gateway** > **Edit** screen.

2 Select **Enable Extended Authentication**.

3 Select **Server Mode** and select an authentication method object from the drop-down list box.

4 Click **OK** to save the settings.

**Figure 474** Example: Using Authentication Method in VPN




# 42.2 Viewing Authentication Method Objects

Click **Object > Auth. Method** to display the screen as shown.

Note: You can create up to 16 authentication method objects.

**Figure 475** Object > Auth. Method


The following table describes the labels in this screen.

**Table 224** Object > Auth. Method

| LABEL | DESCRIPTION |
|---|---|
| # | This field displays the index number. |
| Method Name | This field displays a descriptive name for identification purposes. |

**Table 224** Object > Auth. Method (continued)

| LABEL | DESCRIPTION |
|---|---|
| Method List | This field displays the authentication method(s) for this entry. |
| Add icon | Click **Add** to add a new entry.<br>Click **Edit** to edit the settings of an entry.<br>Click **Delete** to remove an entry. |

# 42.3 Creating an Authentication Method Object

Follow the steps below to create an authentication method object.

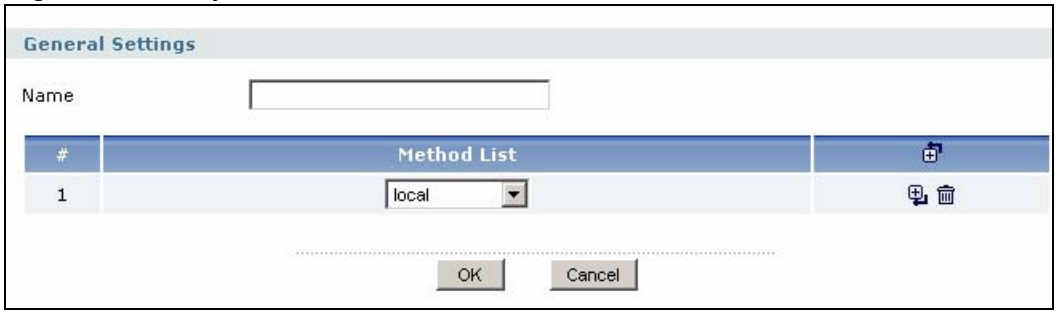
1. Click **Object > Auth. Method**.
2. Click **Add**.
3. Specify a descriptive name for identification purposes in the **Name** field. You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. For example, “My_Device”.
4. Click **Add** to insert an authentication method in the table.
5. Select a server object from the **Method List** drop-down list box.
6. You can add up to four server objects to the table. The ordering of the **Method List** column is important. The ZyWALL authenticates the users using the databases (in the local user database or the external authentication server) in the order they appear in this screen.

   If two accounts with the same username exist on two authentication servers you specify, the ZyWALL does not continue the search on the second authentication server when you enter the username and password that doesn’t match the one on the first authentication server.

   Note: You can NOT select two server objects of the same type.

7 Click **OK** to save the settings or click **Cancel** to discard all changes and return to the previous screen.

**Figure 476** Object > Auth. Method > Add




The following table describes the labels in this screen.

**Table 225** Object > Auth. Method > Add

| LABEL | DESCRIPTION |
|---|---|
| Name | Specify a descriptive name for identification purposes.<br><br>You may use 1-31 alphanumeric characters, underscores(_), or dashes (-), but the first character cannot be a number. This value is case-sensitive. For example, “My_Device”. |
| Method List | Select a server object from the drop-down list box. You can create a server object in the **AAA Server** screen (see Chapter 41 on page 683 for more information).<br><br>The ZyWALL authenticates the users using the databases (in the local user database or the external authentication server) in the order they appear in this screen.<br><br>If two accounts with the same username exist on two authentication servers you specify, the ZyWALL does not continue the search on the second authentication server when you enter the username and password that doesn’t match the one on the first authentication server. |
| Add icon | Click **Add** to add a new entry.<br><br>Click **Edit** to edit the settings of an entry.<br><br>Click **Delete** to delete an entry. |
| OK | Click **OK** to save the changes. |
| Cancel | Click **Cancel** to discard the changes. |

# 43

# Certificates

## 43.1 Overview

The ZyWALL can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

### 43.1.1 What You Can Do in the Certificate Screens

- Use the **My Certificate** screens (see Section 43.2 on page 703 to Section 43.2.3 on page 712) to generate and export self-signed certificates or certification requests and import the ZyWALL's CA-signed certificates.
- Use the **Trusted Certificates** screens (see Section 43.3 on page 713 to Section 43.3.2 on page 718) to save CA certificates and trusted remote host certificates to the ZyWALL. The ZyWALL trusts any valid certificate that you have imported as a trusted certificate. It also trusts any valid certificate signed by any of the certificates that you have imported as a trusted certificate.

### 43.1.2 What You Need to Know About Certificates

When using public-key cryptology for authentication, each host has two keys. One key is public and can be made openly available. The other key is private and must be kept secure.

These keys work like a handwritten signature (in fact, certificates are often referred to as "digital signatures"). Only you can write your signature exactly as it should look. When people know what your signature looks like, they can verify whether something was signed by you, or by someone else. In the same way, your private key "writes" your digital signature and your public key allows people to verify whether data was signed by you, or by someone else. This process works as follows.

1 Tim wants to send a message to Jenny. He needs her to be sure that it comes from him, and that the message content has not been altered by anyone else along the way. Tim generates a public key pair (one public key and one private key).

2 Tim keeps the private key and makes the public key openly available. This means that anyone who receives a message seeming to come from Tim can read it and verify whether it is really from him or not.

3 Tim uses his private key to sign the message and sends it to Jenny.

4 Jenny receives the message and uses Tim's public key to verify it. Jenny knows that the message is from Tim, and that although other people may have been able to read the message, no-one can have altered it (because they cannot re-sign the message with Tim's private key).

5 Additionally, Jenny uses her own private key to sign a message and Tim uses Jenny's public key to verify the message.

The ZyWALL uses certificates based on public-key cryptology to authenticate users attempting to establish a connection, not to encrypt the data that you send after establishing a connection. The method used to secure the data that you send through an established connection depends on the type of connection. For example, a VPN tunnel might use the triple DES encryption algorithm.

The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates.

A certification path is the hierarchy of certification authority certificates that validate a certificate. The ZyWALL does not trust a certificate if any certificate on its path has expired or been revoked.

Certification authorities maintain directory servers with databases of valid and revoked certificates. A directory of certificates that have been revoked before the scheduled expiration is called a CRL (Certificate Revocation List). The ZyWALL can check a peer's certificate against a directory server's list of revoked certificates. The framework of servers, software, procedures and policies that handles keys is called PKI (public-key infrastructure).

### Advantages of Certificates

Certificates offer the following benefits.

- The ZyWALL only has to store the certificates of the certification authorities that you decide to trust, no matter how many devices you need to authenticate.
- Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

### Self-signed Certificates

You can have the ZyWALL act as a certification authority and sign its own certificates.

### Factory Default Certificate

The ZyWALL generates its own unique self-signed certificate when you first turn it on. This certificate is referred to in the GUI as the factory default certificate.

### Certificate File Formats

Any certificate that you want to import has to be in one of these file formats:

- Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.
- PEM (Base-64) encoded X.509: This Privacy Enhanced Mail format uses lowercase letters, uppercase letters and numerals to convert a binary X.509 certificate into a printable form.
- Binary PKCS#7: This is a standard that defines the general syntax for data (including digital signatures) that may be encrypted. A PKCS #7 file is used to transfer a public key certificate. The private key is not included. The ZyWALL currently allows the importation of a PKS#7 file that contains a single certificate.
- PEM (Base-64) encoded PKCS#7: This Privacy Enhanced Mail (PEM) format uses lowercase letters, uppercase letters and numerals to convert a binary PKCS#7 certificate into a printable form.
- Binary PKCS#12: This is a format for transferring public key and private key certificates.The private key in a PKCS #12 file is within a password-encrypted envelope. The file's password is not connected to your certificate's public or private passwords. Exporting a PKCS #12 file creates this and you must provide it to decrypt the contents when you import the file into the ZyWALL.

Note: Be careful not to convert a binary file to text during the transfer process. It is easy for this to occur since many programs use text files by default.

### Finding Out More

- See Section 5.5 on page 96 for related information on these screens.
- See Section 43.4 on page 719 for certificate background information.

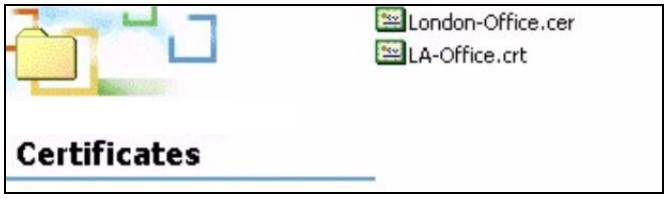
## 43.1.3 Verifying a Certificate

Before you import a trusted certificate into the ZyWALL, you should verify that you have the correct certificate. You can do this using the certificate's fingerprint. A certificate's fingerprint is a message digest calculated using the MD5 or SHA1 algorithm. The following procedure describes how to check a certificate's fingerprint to verify that you have the actual certificate.

1 Browse to where you have the certificate saved on your computer.

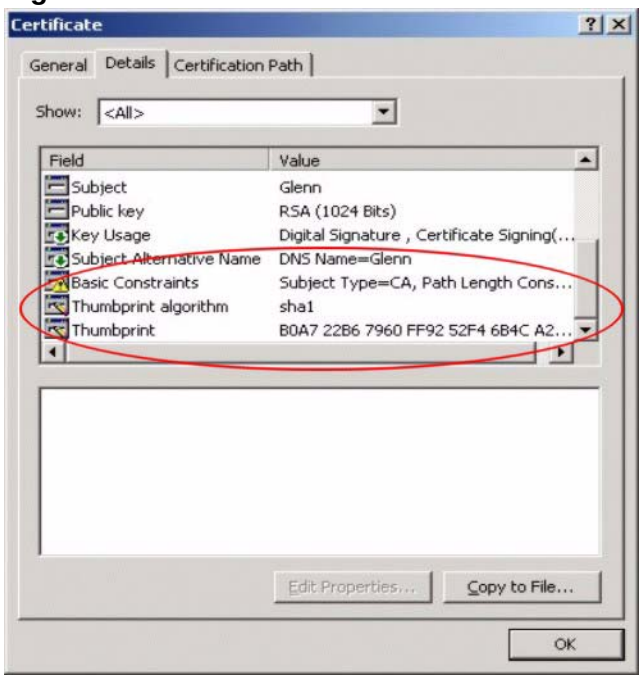
2 Make sure that the certificate has a ".cer" or ".crt" file name extension.

**Figure 477** Remote Host Certificates




3 Double-click the certificate's icon to open the **Certificate** window. Click the **Details** tab and scroll down to the **Thumbprint Algorithm** and **Thumbprint** fields.

**Figure 478** Certificate Details

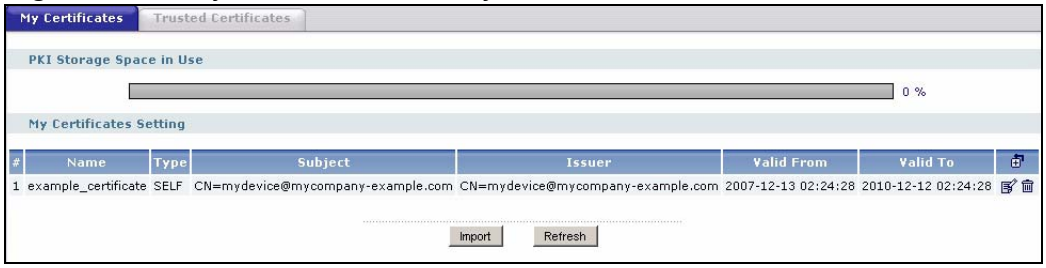



4 Use a secure method to verify that the certificate owner has the same information in the **Thumbprint Algorithm** and **Thumbprint** fields. The secure method may very based on your situation. Possible examples would be over the telephone or through an HTTPS connection.

# 43.2 The My Certificates Screen

Click **Object > Certificate > My Certificates** to open the **My Certificates** screen. This is the ZyWALL's summary list of certificates and certification requests.

**Figure 479** Object > Certificate > My Certificates




The following table describes the labels in this screen.

**Table 226** Object > Certificate > My Certificates

| LABEL | DESCRIPTION |
|---|---|
| PKI Storage Space in Use | This bar displays the percentage of the ZyWALL's PKI storage space that is currently in use. When the storage space is almost full, you should consider deleting expired or unnecessary certificates before adding more certificates. |
| # | This field displays the certificate index number. The certificates are listed in alphabetical order. |
| Name | This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name. |
| Type | This field displays what kind of certificate this is.<br><br>**REQ** represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the **My Certificate Import** screen to import the certificate and replace the request.<br><br>**SELF** represents a self-signed certificate.<br><br>**CERT** represents a certificate issued by a certification authority. |
| Subject | This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information. |
| Issuer | This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the **Subject** field. |
| Valid From | This field displays the date that the certificate becomes applicable. |
| Valid To | This field displays the date that the certificate expires. The text displays in red and includes an Expired! message if the certificate has expired. |

**Table 226** Object > Certificate > My Certificates (continued)

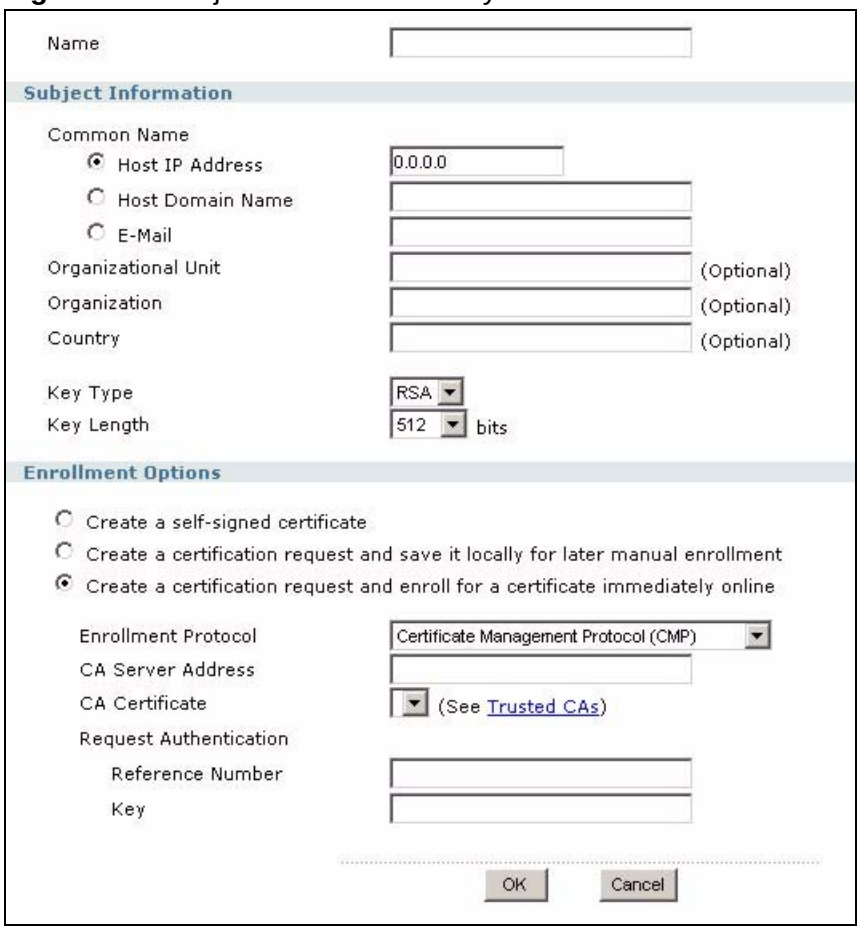
| LABEL | DESCRIPTION |
|---|---|
| Add icon | Click the **Add** icon to go to the screen where you can have the ZyWALL generate a certificate or a certification request.<br><br>Click the **Edit** icon to open a screen with an in-depth list of information about the certificate.<br><br>The ZyWALL keeps all of your certificates unless you specifically delete them. Uploading a new firmware or default configuration file does not delete your certificates.<br><br>Click the **Delete** icon to remove a certificate. A window displays asking you to confirm that you want to delete the certificate. Subsequent certificates move up by one when you take this action.<br><br>You cannot delete certificates that any of the ZyWALL's features are configured to use. |
| Import | Click **Import** to open a screen where you can save a certificate to the ZyWALL. |
| Refresh | Click **Refresh** to display the current validity status of the certificates. |

## 43.2.1 The My Certificates Add Screen

Click **Object > Certificate > My Certificates** and then the **Add** icon to open the **My Certificates Add** screen. Use this screen to have the ZyWALL create a self-

signed certificate, enroll a certificate with a certification authority or generate a certification request.

**Figure 480** Object > Certificate > My Certificates > Add




The following table describes the labels in this screen.

**Table 227** Object > Certificate > My Certificates > Add

| LABEL | DESCRIPTION |
|---|---|
| Name | Type a name to identify this certificate. You can use up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters. |
| Subject Information | Use these fields to record information that identifies the owner of the certificate. You do not have to fill in every field, although the **Common Name** is mandatory. The certification authority may add fields (such as a serial number) to the subject information when it issues a certificate. It is recommended that each certificate have unique subject information. |

**Table 227** Object > Certificate > My Certificates > Add (continued)

| LABEL | DESCRIPTION |
|---|---|
| Common Name | Select a radio button to identify the certificate's owner by IP address, domain name or e-mail address. Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address is for identification purposes only and can be any string.<br><br>A domain name can be up to 255 characters. You can use alphanumeric characters, the hyphen and periods.<br><br>An e-mail address can be up to 63 characters. You can use alphanumeric characters, the hyphen, the @ symbol, periods and the underscore. |
| Organizational Unit | Identify the organizational unit or department to which the certificate owner belongs. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore. |
| Organization | Identify the company or group to which the certificate owner belongs. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore. |
| Country | Identify the nation where the certificate owner is located. You can use up to 31 characters. You can use alphanumeric characters, the hyphen and the underscore. |
| Key Type | Select **RSA** to use the Rivest, Shamir and Adleman public-key algorithm.<br><br>Select **DSA** to use the Digital Signature Algorithm public-key algorithm. |
| Key Length | Select a number from the drop-down list box to determine how many bits the key should use (512 to 2048). The longer the key, the more secure it is. A longer key also uses more PKI storage space. |
| Enrollment Options | These radio buttons deal with how and when the certificate is to be generated. |
| Create a self-signed certificate | Select **Create a self-signed certificate** to have the ZyWALL generate the certificate and act as the Certification Authority (CA) itself. This way you do not need to apply to a certification authority for certificates. |
| Create a certification request and save it locally for later manual enrollment | Select **Create a certification request and save it locally for later manual enrollment** to have the ZyWALL generate and store a request for a certificate. Use the **My Certificate Details** screen to view the certification request and copy it to send to the certification authority.<br><br>Copy the certification request from the **My Certificate Details** screen (see Section 43.2.2 on page 709) and then send it to the certification authority. |

**Table 227** Object > Certificate > My Certificates > Add (continued)

| LABEL | DESCRIPTION |
|---|---|
| Create a certification request and enroll for a certificate immediately online | Select **Create a certification request and enroll for a certificate immediately online** to have the ZyWALL generate a request for a certificate and apply to a certification authority for a certificate.<br><br>You must have the certification authority's certificate already imported in the **Trusted Certificates** screen.<br><br>When you select this option, you must select the certification authority's enrollment protocol and the certification authority's certificate from the drop-down list boxes and enter the certification authority's server address. You also need to fill in the **Reference Number** and **Key** if the certification authority requires them. |
| Enrollment Protocol | This field applies when you select **Create a certification request and enroll for a certificate immediately online**. Select the certification authority's enrollment protocol from the drop-down list box.<br><br>**Simple Certificate Enrollment Protocol (SCEP)** is a TCP-based enrollment protocol that was developed by VeriSign and Cisco.<br><br>**Certificate Management Protocol (CMP)** is a TCP-based enrollment protocol that was developed by the Public Key Infrastructure X.509 working group of the Internet Engineering Task Force (IETF) and is specified in RFC 2510. |
| CA Server Address | This field applies when you select **Create a certification request and enroll for a certificate immediately online**. Enter the IP address (or URL) of the certification authority server.<br><br>For a URL, you can use up to 511 of the following characters. a-zA-Z0-9'()+,/:.=?;!*#@$_%- |
| CA Certificate | This field applies when you select **Create a certification request and enroll for a certificate immediately online**. Select the certification authority's certificate from the **CA Certificate** drop-down list box.<br><br>You must have the certification authority's certificate already imported in the **Trusted Certificates** screen. Click **Trusted CAs** to go to the **Trusted Certificates** screen where you can view (and manage) the ZyWALL's list of certificates of trusted certification authorities. |
| Request Authentication | When you select **Create a certification request and enroll for a certificate immediately online**, the certification authority may want you to include a reference number and key to identify you when you send a certification request.<br><br>Fill in both the **Reference Number** and the **Key** fields if your certification authority uses CMP enrollment protocol. Just the **Key** field displays if your certification authority uses the SCEP enrollment protocol.<br><br>For the reference number, use 0 to 99999999.<br><br>For the key, use up to 31 of the following characters. a-zA-Z0-9;\|`~!@#$%^&*()_+\{}':,./<>=- |

**Table 227** Object > Certificate > My Certificates > Add (continued)

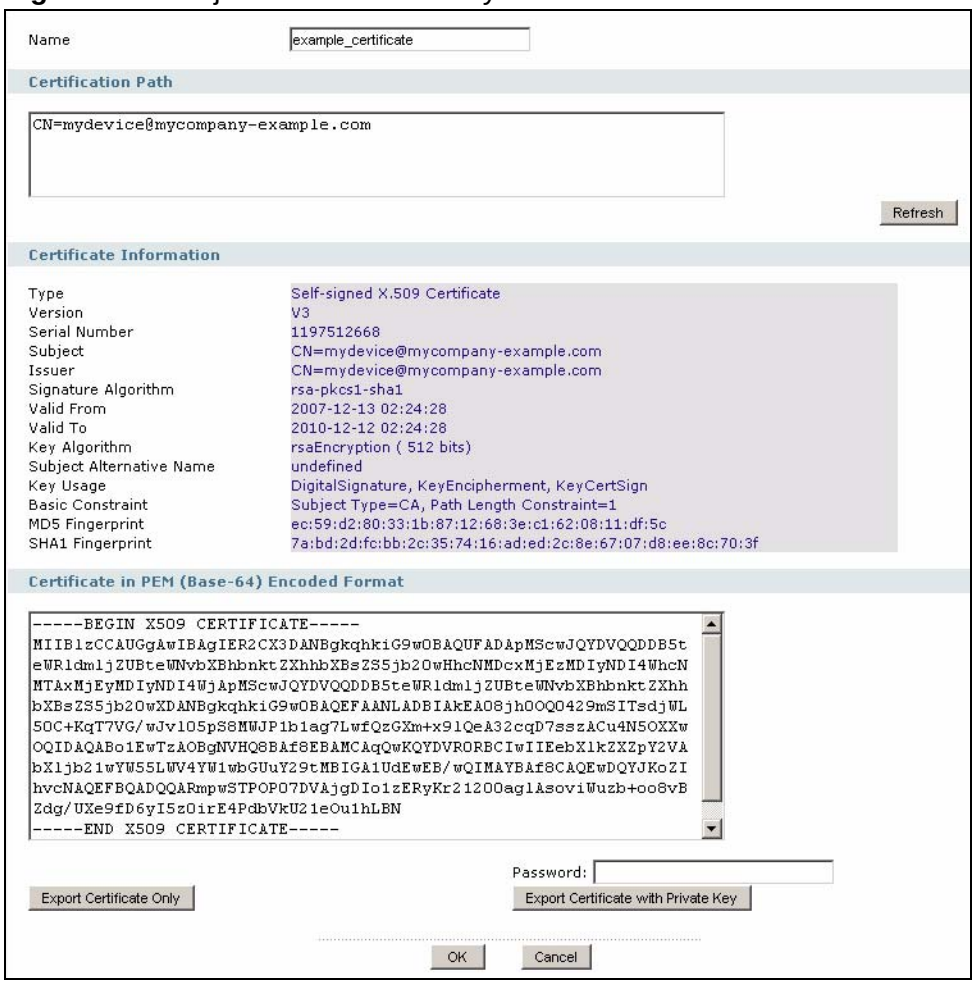
| LABEL | DESCRIPTION |
|---|---|
| OK | Click **OK** to begin certificate or certification request generation. |
| Cancel | Click **Cancel** to quit and return to the **My Certificates** screen. |

If you configured the **My Certificate Create** screen to have the ZyWALL enroll a certificate and the certificate enrollment is not successful, you see a screen with a **Return** button that takes you back to the **My Certificate Create** screen. Click **Return** and check your information in the **My Certificate Create** screen. Make sure that the certification authority information is correct and that your Internet connection is working properly if you want the ZyWALL to enroll a certificate online.

## 43.2.2 The My Certificates Edit Screen

Click **Object > Certificate > My Certificates** and then the **Edit** icon to open the **My Certificate Edit** screen. You can use this screen to view in-depth certificate information and change the certificate's name.

**Figure 481** Object > Certificate > My Certificates > Edit



The following table describes the labels in this screen.

**Table 228** Object > Certificate > My Certificates > Edit

| LABEL | DESCRIPTION |
|---|---|
| Name | This field displays the identifying name of this certificate. You can use up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters. |
| Certification Path | This field displays for a certificate, not a certification request.<br><br>Click the **Refresh** button to have this read-only text box display the hierarchy of certification authorities that validate the certificate (and the certificate itself).<br><br>If the issuing certification authority is one that you have imported as a trusted certification authority, it may be the only certification authority in the list (along with the certificate itself). If the certificate is a self-signed certificate, the certificate itself is the only one in the list. The ZyWALL does not trust the certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked. |
| Refresh | Click **Refresh** to display the certification path. |
| Certificate Information | These read-only fields display detailed information about the certificate. |
| Type | This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). "X.509" means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates. |
| Version | This field displays the X.509 version number. " |
| Serial Number | This field displays the certificate's identification number given by the certification authority or generated by the ZyWALL. |
| Subject | This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C). |
| Issuer | This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country.<br><br>With self-signed certificates, this is the same as the **Subject Name** field.<br><br>"none" displays for a certification request. |
| Signature Algorithm | This field displays the type of algorithm that was used to sign the certificate. The ZyWALL uses rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Some certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm). |
| Valid From | This field displays the date that the certificate becomes applicable. "none" displays for a certification request. |
| Valid To | This field displays the date that the certificate expires. The text displays in red and includes an Expired! message if the certificate has expired. "none" displays for a certification request. |

**Table 228** Object > Certificate > My Certificates > Edit

| LABEL | DESCRIPTION |
|---|---|
| Key Algorithm | This field displays the type of algorithm that was used to generate the certificate's key pair (the ZyWALL uses RSA encryption) and the length of the key set in bits (1024 bits for example). |
| Subject Alternative Name | This field displays the certificate owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL). |
| Key Usage | This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text. |
| Basic Constraint | This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path. This field does not display for a certification request. |
| MD5 Fingerprint | This is the certificate's message digest that the ZyWALL calculated using the MD5 algorithm. |
| SHA1 Fingerprint | This is the certificate's message digest that the ZyWALL calculated using the SHA1 algorithm. |
| Certificate in PEM (Base-64) Encoded Format | This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses lowercase letters, uppercase letters and numerals to convert a binary certificate into a printable form.<br><br>You can copy and paste a certification request into a certification authority's web page, an e-mail that you send to the certification authority or a text editor and save the file on a management computer for later manual enrollment.<br><br>You can copy and paste a certificate into an e-mail to send to friends or colleagues or you can copy and paste a certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example). |
| Export | This button displays for a certification request. Use this button to save a copy of the request without its private key. Click this button and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**. |
| Export Certificate Only | Use this button to save a copy of the certificate without its private key. Click this button and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**. |
| Password | If you want to export the certificate with its private key, create a password and type it here. Make sure you keep this password in a safe place. You will need to use it if you import the certificate to another device. |
| Export Certificate with Private Key | Use this button to save a copy of the certificate with its private key. Type the certificate's password and click this button. Click **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**. |

**Table 228** Object > Certificate > My Certificates > Edit

| LABEL | DESCRIPTION |
|---|---|
| OK | Click **OK** to save your changes back to the ZyWALL. You can only change the name. |
| Cancel | Click **Cancel** to quit and return to the **My Certificates** screen. |

## 43.2.3 The My Certificates Import Screen

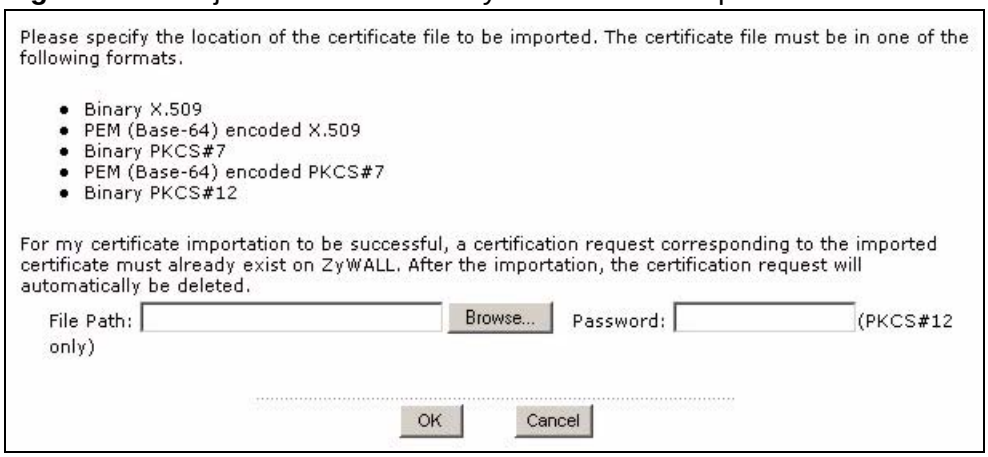
Click **Object > Certificate > My Certificates > Import** to open the **My Certificate Import** screen. Follow the instructions in this screen to save an existing certificate to the ZyWALL.

Note: You can import a certificate that matches a corresponding certification request that was generated by the ZyWALL. You can also import a certificate in PKCS#12 format, including the certificate's public and private keys.

The certificate you import replaces the corresponding request in the **My Certificates** screen.

You must remove any spaces from the certificate's filename before you can import it.

**Figure 482** Object > Certificate > My Certificates > Import




The following table describes the labels in this screen.

**Table 229** Object > Certificate > My Certificates > Import

| LABEL | DESCRIPTION |
|---|---|
| File Path | Type in the location of the file you want to upload in this field or click **Browse** to find it.<br><br>You cannot import a certificate with the same name as a certificate that is already in the ZyWALL. |
| Browse | Click **Browse** to find the certificate file you want to upload. |

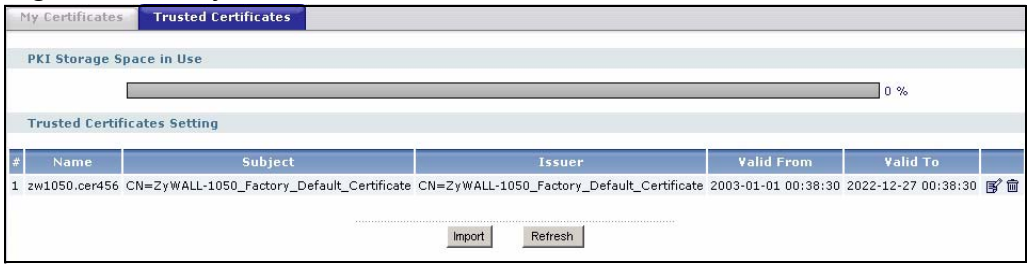
**Table 229** Object > Certificate > My Certificates > Import (continued)

| LABEL | DESCRIPTION |
|---|---|
| Password | This field only applies when you import a binary PKCS#12 format file. Type the file's password that was created when the PKCS #12 file was exported. |
| OK | Click **OK** to save the certificate on the ZyWALL. |
| Cancel | Click **Cancel** to quit and return to the **My Certificates** screen. |

# 43.3 The Trusted Certificates Screen

Click **Object > Certificate > Trusted Certificates** to open the **Trusted Certificates** screen. This screen displays a summary list of certificates that you have set the ZyWALL to accept as trusted. The ZyWALL also accepts any valid certificate signed by a certificate on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certificates.

**Figure 483** Object > Certificate > Trusted Certificates




The following table describes the labels in this screen.

**Table 230** Object > Certificate > Trusted Certificates

| LABEL | DESCRIPTION |
|---|---|
| PKI Storage Space in Use | This bar displays the percentage of the ZyWALL's PKI storage space that is currently in use. When the storage space is almost full, you should consider deleting expired or unnecessary certificates before adding more certificates. |
| # | This field displays the certificate index number. The certificates are listed in alphabetical order. |
| Name | This field displays the name used to identify this certificate. |
| Subject | This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information. |
| Issuer | This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the **Subject** field. |
| Valid From | This field displays the date that the certificate becomes applicable. |

**Table 230** Object > Certificate > Trusted Certificates (continued)

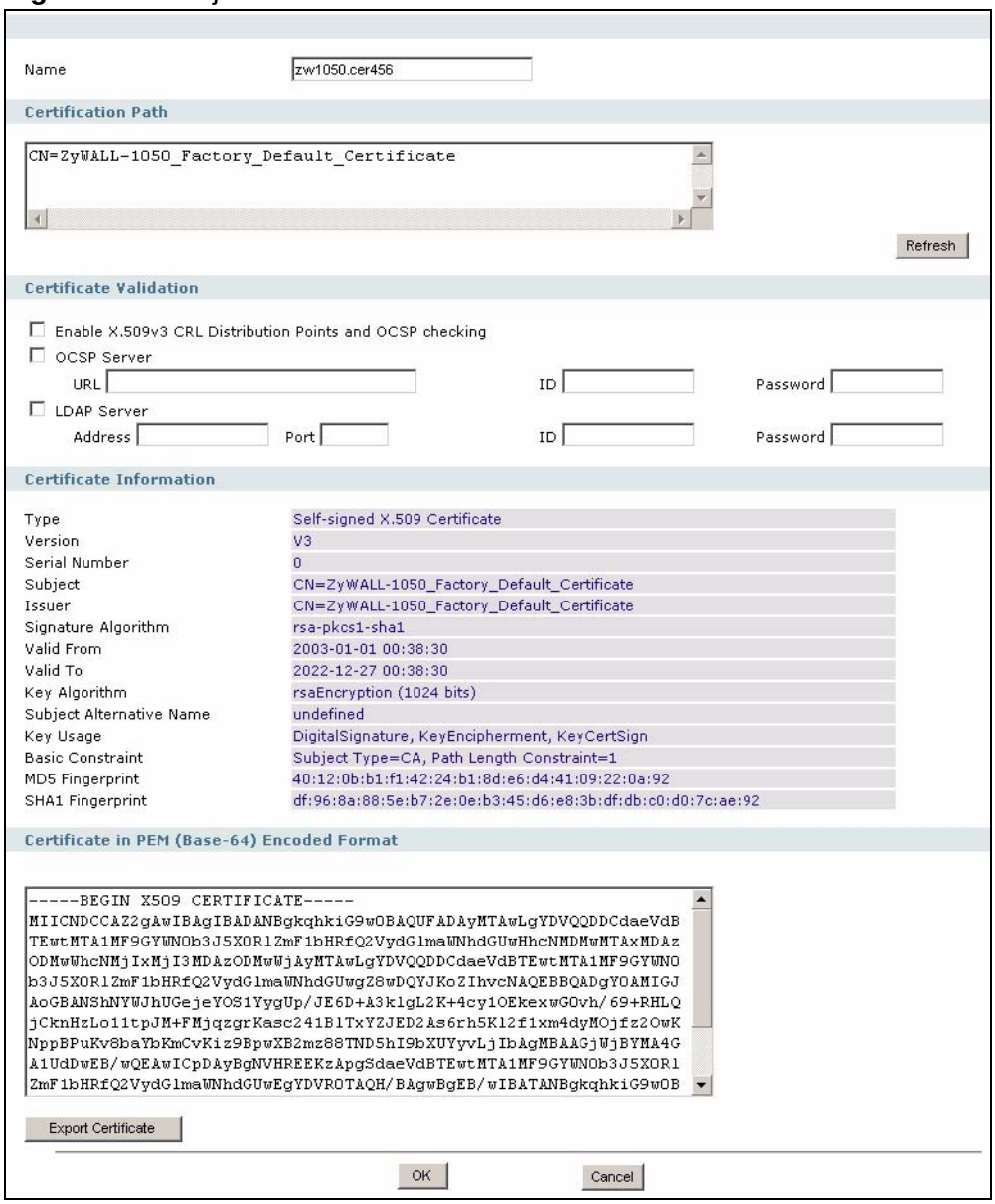
| LABEL | DESCRIPTION |
|---|---|
| Valid To | This field displays the date that the certificate expires. The text displays in red and includes an Expired! message if the certificate has expired. |
| (icons) | Click the **Edit** icon to open a screen with an in-depth list of information about the certificate.<br><br>The ZyWALL keeps all of your certificates unless you specifically delete them. Uploading a new firmware or default configuration file does not delete your certificates.<br><br>Click the **Delete** icon to remove a certificate. A window displays asking you to confirm that you want to delete the certificates. Note that subsequent certificates move up by one when you take this action. |
| Import | Click **Import** to open a screen where you can save the certificate of a certification authority that you trust, from your computer to the ZyWALL. |
| Refresh | Click this button to display the current validity status of the certificates. |

## 43.3.1 The Trusted Certificates Edit Screen

Click **Object > Certificate > Trusted Certificates** and then a certificate's **Edit** icon to open the **Trusted Certificates Edit** screen. Use this screen to view in-depth information about the certificate, change the certificate's name and set whether or not you want the ZyWALL to check a certification authority's list of

revoked certificates before trusting a certificate issued by the certification authority.

**Figure 484** Object > Certificate > Trusted Certificates > Edit



The following table describes the labels in this screen.

**Table 231** Object > Certificate > Trusted Certificates > Edit

| LABEL | DESCRIPTION |
|---|---|
| Name | This field displays the identifying name of this certificate. You can change the name. You can use up to 31 alphanumeric and ;'~!@#$%^&()_+[]{}',.=- characters. |
| Certification Path | Click the **Refresh** button to have this read-only text box display the end entity's certificate and a list of certification authority certificates that shows the hierarchy of certification authorities that validate the end entity's certificate. If the issuing certification authority is one that you have imported as a trusted certificate, it may be the only certification authority in the list (along with the end entity's own certificate). The ZyWALL does not trust the end entity's certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked. |
| Refresh | Click **Refresh** to display the certification path. |
| Enable X.509v3 CRL Distribution Points and OCSP checking | Select this check box to have the ZyWALL check incoming certificates that are signed by this certificate against a Certificate Revocation List (CRL) or an OCSP server. You also need to configure the OSCP or LDAP server details. |
| OCSP Server | Select this check box if the directory server uses OCSP (Online Certificate Status Protocol). |
| URL | Type the protocol, IP address and pathname of the OCSP server. |
| ID | The ZyWALL may need to authenticate itself in order to assess the OCSP server. Type the login name (up to 31 ASCII characters) from the entity maintaining the server (usually a certification authority). |
| Password | Type the password (up to 31 ASCII characters) from the entity maintaining the OCSP server (usually a certification authority). |
| LDAP Server | Select this check box if the directory server uses LDAP (Lightweight Directory Access Protocol). LDAP is a protocol over TCP that specifies how clients access directories of certificates and lists of revoked certificates. |
| Address | Type the IP address (in dotted decimal notation) of the directory server. |
| Port | Use this field to specify the LDAP server port number.<br>You must use the same server port number that the directory server uses.<br>389 is the default server port number for LDAP. |
| ID | The ZyWALL may need to authenticate itself in order to assess the CRL directory server. Type the login name (up to 31 ASCII characters) from the entity maintaining the server (usually a certification authority). |
| Password | Type the password (up to 31 ASCII characters) from the entity maintaining the CRL directory server (usually a certification authority). |
| Certificate Information | These read-only fields display detailed information about the certificate. |

**Table 231** Object > Certificate > Trusted Certificates > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Type | This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). X.509 means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates. |
| Version | This field displays the X.509 version number. |
| Serial Number | This field displays the certificate's identification number given by the certification authority. |
| Subject | This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C). |
| Issuer | This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country.<br><br>With self-signed certificates, this is the same information as in the **Subject Name** field. |
| Signature Algorithm | This field displays the type of algorithm that was used to sign the certificate. Some certification authorities use rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Other certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm). |
| Valid From | This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable. |
| Valid To | This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired. |
| Key Algorithm | This field displays the type of algorithm that was used to generate the certificate's key pair (the ZyWALL uses RSA encryption) and the length of the key set in bits (1024 bits for example). |
| Subject Alternative Name | This field displays the certificate's owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL). |
| Key Usage | This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text. |
| Basic Constraint | This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path. |
| MD5 Fingerprint | This is the certificate's message digest that the ZyWALL calculated using the MD5 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate. |

**Table 231** Object > Certificate > Trusted Certificates > Edit (continued)

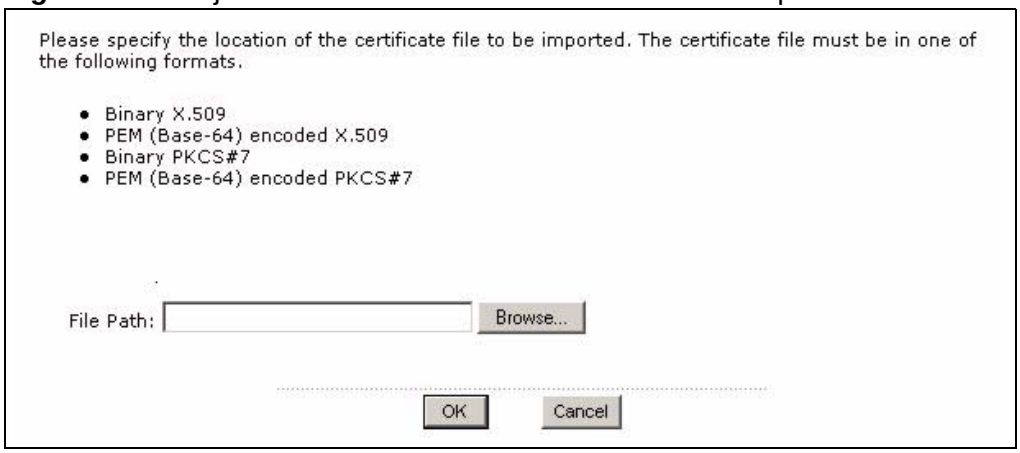
| LABEL | DESCRIPTION |
|---|---|
| SHA1 Fingerprint | This is the certificate's message digest that the ZyWALL calculated using the SHA1 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate. |
| Certificate in PEM (Base-64) Encoded Format | This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses lowercase letters, uppercase letters and numerals to convert a binary certificate into a printable form.<br>You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example). |
| Export Certificate | Click this button and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**. |
| OK | Click **OK** to save your changes back to the ZyWALL. You can only change the name. |
| Cancel | Click **Cancel** to quit and return to the **Trusted Certificates** screen. |

## 43.3.2 The Trusted Certificates Import Screen

Click **Object > Certificate > Trusted Certificates > Import** to open the **Trusted Certificates Import** screen. Follow the instructions in this screen to save a trusted certificate to the ZyWALL.

Note: You must remove any spaces from the certificate's filename before you can import the certificate.

**Figure 485** Object > Certificate > Trusted Certificates > Import



The following table describes the labels in this screen.

**Table 232** Object > Certificate > Trusted Certificates > Import

| LABEL | DESCRIPTION |
|---|---|
| File Path | Type in the location of the file you want to upload in this field or click **Browse** to find it.<br>You cannot import a certificate with the same name as a certificate that is already in the ZyWALL. |
| Browse | Click **Browse** to find the certificate file you want to upload. |
| OK | Click **OK** to save the certificate on the ZyWALL. |
| Cancel | Click **Cancel** to quit and return to the previous screen. |

# 43.4 Certificates Technical Reference

## OCSP

OCSP (Online Certificate Status Protocol) allows an application or device to check whether a certificate is valid. With OCSP the ZyWALL checks the status of individual certificates instead of downloading a Certificate Revocation List (CRL). OCSP has two main advantages over a CRL. The first is real-time status information. The second is a reduction in network traffic since the ZyWALL only gets information on the certificates that it needs to verify, not a huge list. When the ZyWALL requests certificate status information, the OCSP server returns a “expired”, “current” or “unknown” response.

# 44

# SSL Application

## 44.1 Overview

You use SSL application objects in SSL VPN. Configure an SSL application object to specify the type of application and the address of the local computer, server, or web site SSL users are to be able to access. You can apply one or more SSL application objects in the **VPN > SSL VPN** screen for a user account/user group.

### 44.1.1 What You Can Do in the SSL Application Screens

- Use the **SSL Application** screen (Section 44.2 on page 723) to view the ZyWALL's configured SSL application objects.
- Use the **SSL Application Edit** screen to create or edit web-based application objects to allow remote users to access an application via standard web browsers (Section 44.2.1 on page 724).
- You can also use the **SSL Application Edit** screen to specify the name of a folder on a Linux or Windows file server which remote users can access using a standard web browser (Section 44.2.2 on page 726).

### 44.1.2 What You Need to Know About SSL Application Objects

#### Application Types

You can configure the following types of SSL applications on the ZyWALL.

- Web-based

  A web-based application allows remote users to access an intranet site using standard web browsers.
- File sharing

  Configure file sharing to allow users to access files on the intranet.

### Remote User Screen Links

Available SSL application names are displayed as links in remote user screens. Depending on the application type, remote users can simply click the links or follow the steps in the pop-up dialog box to access.

### Remote Desktop Connections

Use SSL VPN to allow remote users to manage LAN computers. Depending on the functions supported by the remote desktop software, they can install or remove software, run programs, change settings, and open, copy, create, and delete files. This is useful for troubleshooting, support, administration, and remote access to files and programs.

The LAN computer to be managed must have VNC (Virtual Network Computing) or RDP (Remote Desktop Protocol) server software installed. The remote user's computer does not use VNC or RDP client software. The ZyWALL works with the following remote desktop connection software:

**RDP**

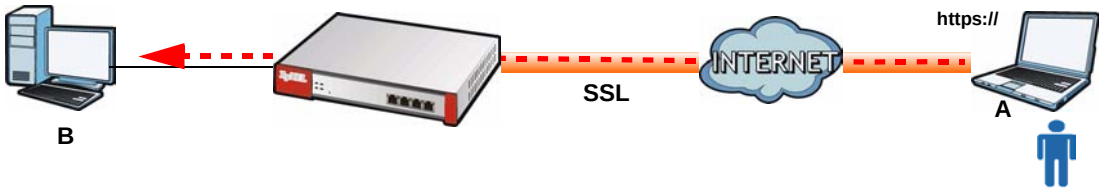
- Windows Remote Desktop (supported in Internet Explorer)

**VNC**

- RealVNC
- TightVNC
- UltraVNC

For example, user A uses an SSL VPN connection to log into the ZyWALL. Then he manages LAN computer B which has RealVNC server software installed.

**Figure 486** SSL-protected Remote Management




## 44.1.3 Example: Specifying a Web Site for Access

This example shows you how to create a web-based application for an internal web site. The address of the web site is http://info with web page encryption.

1 Click **Object > SSL Application** in the navigation panel.

2 Click the **Add** button and select **Web Application** in the **Type** field.

3 Enter a descriptive name in the **Display Name** field. For example, “CompanyIntranet”.

4 In the **Address** field, enter “http://info”.

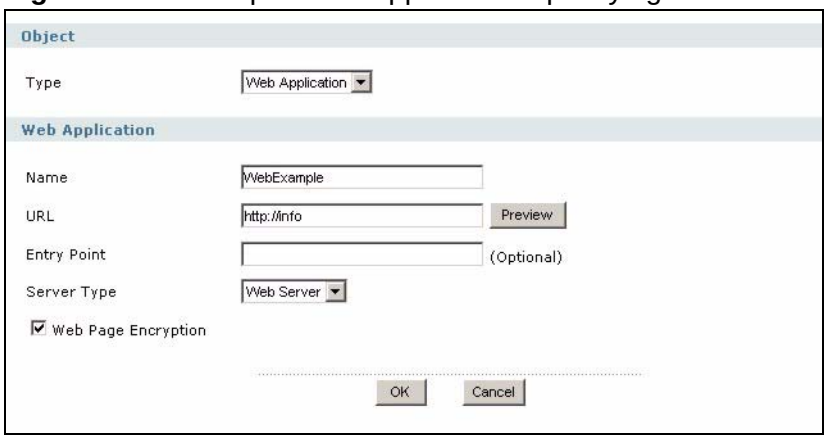
5 In the **Server Type** field, select **Web Server**.

6 Select **Web Page Encryption** to prevent users from saving the web content.

7 Click **Apply** to save the settings.

The configuration screen should look similar to the following figure.

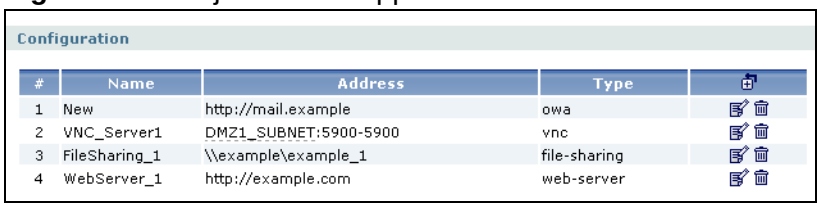
**Figure 487** Example: SSL Application: Specifying a Web Site for Access




# 44.2 The SSL Application Screen

The main **SSL Application** screen displays a list of the configured SSL application objects. Click **Object > SSL Application** in the navigation panel.

**Figure 488** Object > SSL Application



The following table describes the labels in this screen.

**Table 233** Object > SSL Application

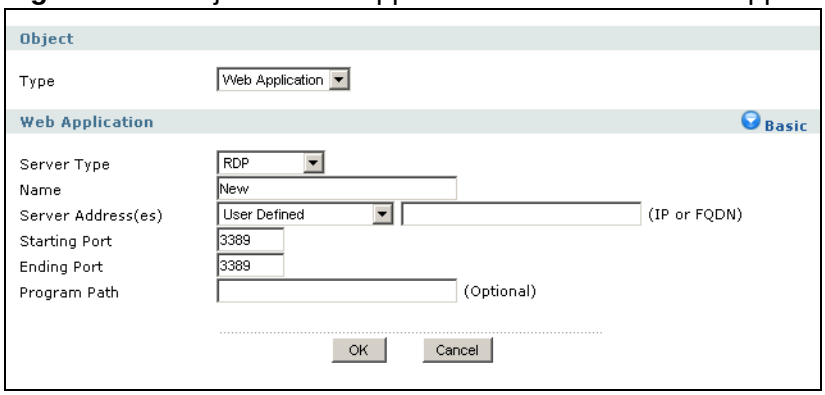
| LABEL | DESCRIPTION |
|---|---|
| # | This field displays the index number. |
| Name | This field displays the name of the object. |
| Address | This field displays the IP address/URL of the application server or the location of a file share. |
| Type | This field shows whether the object is a file-sharing, web-server, Outlook Web Access, Virtual Network Computing, or Remote Desktop Protocol SSL application. |
| Add icon | This column provides icons to add, edit, and remove SSL application objects.<br>To add an object, click the **Add** icon at the top of the column.<br>To edit an object, click the **Edit** icon next to the object.<br>To delete an object, click the **Remove** icon next to the object. |

## 44.2.1 Creating/Editing a Web-based SSL Application Object

A web-based application allows remote users to access an application via standard web browsers.

To configure a web-based application, click the **Add** or **Edit** button in the **SSL Application** screen and select **Web Application** in the **Type** field to display the configuration screen as shown.

**Figure 489** Object > SSL Application > Add/Edit: Web Application




The following table describes the labels in this screen.

**Table 234** Object > SSL Application > Add/Edit: Web Application

| LABEL | DESCRIPTION |
|---|---|
| Object | |
| Type | Select **Web Application** from the drop-down list box. |

**Table 234** Object > SSL Application > Add/Edit: Web Application

| LABEL | DESCRIPTION |
|---|---|
| Web Application | Click **Advanced** to display more configuration fields and edit the details of your SSL application setup. Click **Basic** to display fewer fields. |
| Server Type | Specify the type of service for this SSL application.<br><br>Select **Web Server** to allow access to the specified web site hosted on the local network.<br><br>Select **OWA** (Outlook Web Access) to allow users to access e-mails, contacts, calenders via Microsoft Outlook-like interface using supported web browsers. The ZyWALL supports one OWA object.<br><br>Select **VNC** to allow users to manage LAN computers that have Virtual Network Computing remote desktop server software installed.<br><br>Select **RDP** to allow users to manage LAN computers that have Remote Desktop Protocol remote desktop server software installed. |
| Name | Enter a descriptive name to identify this object. You can enter up to 31 characters (“0-9”, “a-z”, “A-Z”, “-” and “_”). Spaces are not allowed. |
| URL | This field displays if the **Server Type** is set to **Web Server** or **OWA**.<br><br>Enter the Fully-Qualified Domain Name (FQDN) or IP address of the application server.<br><br>Note: You must enter the “http://” or “https://” prefix.<br><br>Remote users are restricted to access only files in this directory. For example, if you enter “\remote\” in this field, emote users can only access files in the “remote” directory.<br><br>If a link contains a file that is not within this domain, then remote users cannot access it. |
| Preview | This field displays if the **Server Type** is set to **Web Server** or **OWA**.<br><br>Click **Preview** to access the URL you specified in a new IE web browser. |
| Entry Point | This field displays if the **Server Type** is set to **Web Server** or **OWA**.<br><br>This field is optional. You only need to configure this field if you need to specify the name of the directory or file on the local server as the home page or home directory on the user screen. |
| Server Address(es) | This field displays if the **Server Type** is set to **RDP** or **VNC**.<br><br>Specify the IP address or Fully-Qualified Domain Name (FQDN) of the computer(s) that you want to allow the remote users to manage. |
| Starting Port<br><br>Ending Port | This field displays if the **Server Type** is set to **RDP** or **VNC**.<br><br>Specify the listening ports of the LAN computer(s) running remote desktop server software. The ZyWALL uses a port number from this range to send traffic to the LAN computer that is being remotely managed. |
| Program Path | This field displays if the **Server Type** is set to **RDP**.<br><br>You can specify an application to open when a remote user logs into the remote desktop application. |
| Web Page Encryption | Select this option to prevent users from saving the web content. |

**Table 234** Object > SSL Application > Add/Edit: Web Application

| LABEL | DESCRIPTION |
|---|---|
| Ok | Click **Ok** to save the changes and return to the main **SSL Application Configuration** screen. |
| Cancel | Click **Cancel** to discard the changes and return to the main **SSL Application Configuration** screen. |

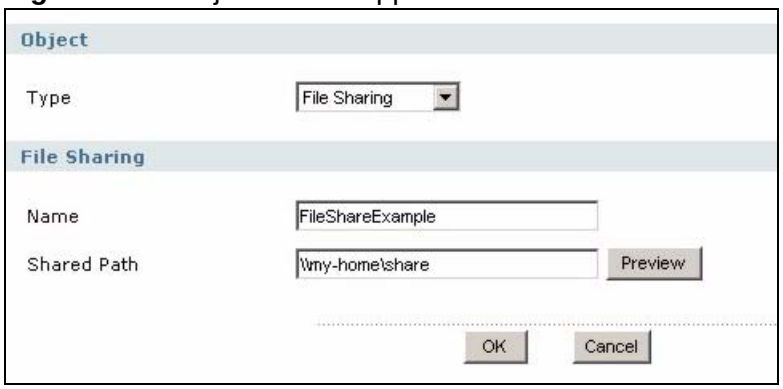
## 44.2.2 Creating/Editing a File Sharing SSL Application Object

You can specify the name of a folder on a file server (Linux or Windows) which remote users can access. Remote users can access files using a standard web browser and files are displayed as links on the screen.

To configure a file share, click the **Add** or **Edit** button in the **SSL Application** screen and select **File Sharing** in the **Type** field. The configuration screen displays as shown.

Note: You must also configure the shared folder on the file server for remote access. Refer to the document that comes with your file server.

**Figure 490** Object > SSL Application > Add/Edit: File Sharing




The following table describes the labels in this screen.

**Table 235** Object > SSL Application > Add/Edit: File Sharing

| LABEL | DESCRIPTION |
|---|---|
| Object | |
| Type | Select File Sharing to create a file share application for VPN SSL. |
| File Sharing | |
| Name | Enter a descriptive name to identify this object. You can enter up to 31 characters (“0-9”, “a-z”, “A-Z”, “-” and “_”). Spaces are not allowed. |

**Table 235** Object > SSL Application > Add/Edit: File Sharing

| LABEL | DESCRIPTION |
|---|---|
| Shared Path | Specify the IP address, domain name or NetBIOS name (computer name) of the file server and the name of the share to which you want to allow user access. Enter the path in one of the following formats.<br>"\\<IP address>\<share name>"<br>"\\<domain name>\<share name>"<br>"\\<computer name>\<share name>"<br>For example, if you enter "\\my-server\Tmp", this allows remote users to access all files and/or folders in the "\Tmp" share on the "my-server" computer. |
| Preview | Click **Preview** to display the file share in a new web browser. |
| Ok | Click **Ok** to save the changes and return to the main **SSL Application Configuration** screen. |
| Cancel | Click **Cancel** to discard the changes and return to the main **SSL Application Configuration** screen. |

# PART IX
# System

# 45

# System

## 45.1 Overview

Use the system screens to configure general ZyWALL settings.

### 45.1.1 What You Can Do In The System Screens

- Use the **System > Host Name** screen (see Section 45.2 on page 732) to configure a unique name for the ZyWALL in your network.
- Use the **System > Date/Time** screen (see Section 45.3 on page 732) to configure the date and time for the ZyWALL.
- Use the **System > Console Speed** screen (see Section 45.4 on page 737) to configure the console port speed when you connect to the ZyWALL via the console port using a terminal emulation program.
- Use the **System > DNS** screen (see Section 45.5 on page 737) to configure the DNS (Domain Name System) server used for mapping a domain name to its corresponding IP address and vice versa.
- Use the **System > WWW** screens (see Section 45.6 on page 744) to configure settings for HTTP or HTTPS access to the ZyWALL and how the login and access user screens look.
- Use the **System > SSH** screen (see Section 45.7 on page 762) to configure SSH (Secure SHell) used to securely access the ZyWALL's command line interface. You can specify which zones allow SSH access and from which IP address the access can come.
- Use the **System > TELNET** screen (see Section 45.8 on page 767) to configure Telnet to access the ZyWALL's command line interface. Specify which zones allow Telnet access and from which IP address the access can come.
- Use the **System > FTP** screen (see Section 45.9 on page 768) to specify from which zones FTP can be used to access the ZyWALL. You can also specify from which IP addresses the access can come. You can upload and download the ZyWALL's firmware and configuration files using FTP. Please also see Chapter 46 on page 781 for more information about firmware and configuration files.
- Your ZyWALL can act as an SNMP agent, which allows a manager station to manage and monitor the ZyWALL through the network. Use the **System > SNMP** screen (see Section 45.10 on page 770) to configure SNMP settings, including from which zones SNMP can be used to access the ZyWALL. You can also specify from which IP addresses the access can come.

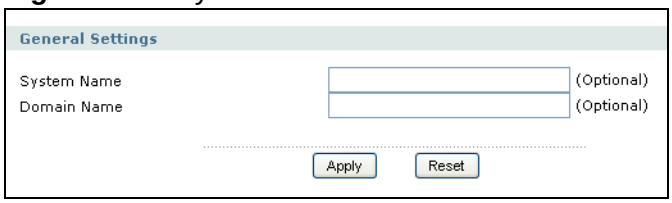
- Connect an external serial modem to the **AUX** port to provide a management connection in case the ZyWALL's other WAN connections are down. Use the **System > Dial-in Mgmt.** screen (see Section 45.11 on page 774) to configure the external serial modem.
- Vantage CNM (Centralized Network Management) is a browser-based global management tool that allows an administrator to manage ZyXEL devices. Use the **System > Vantage CNM** screen (see Section 45.12 on page 776) to allow your ZyWALL to be managed by the Vantage CNM server.
- Use the **System > Language** screen (see Section 45.13 on page 777) to set a language for the ZyWALL's Web Configurator screens.

Note: See each section for related background information and term definitions.

# 45.2 Host Name

A host name is the unique name by which a device is known on a network. Click **System > Host Name** to open the **Host Name** screen.

**Figure 491** System > Host Name




The following table describes the labels in this screen.

**Table 236** System > Host Name

| LABEL | DESCRIPTION |
|---|---|
| System Name | Choose a descriptive name to identify your ZyWALL device. This name can be up to 64 alphanumeric characters long. Spaces are not allowed, but dashes "-" are accepted. |
| Domain Name | Enter the domain name (if you know it) here. This name is propagated to DHCP clients connected to interfaces with the DHCP server enabled. This name can be up to 254 alphanumeric characters long. Spaces are not allowed, but dashes "-" are accepted. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

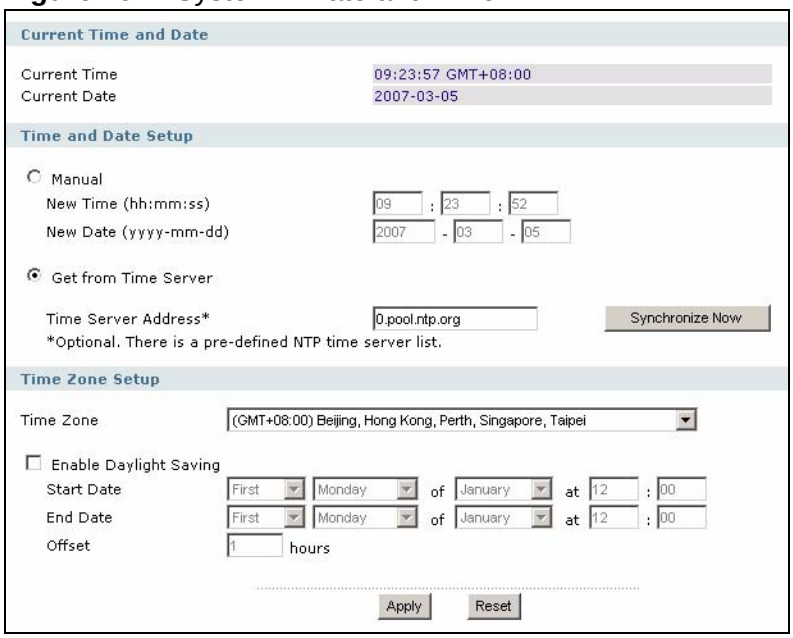
# 45.3 Date and Time

For effective scheduling and logging, the ZyWALL system time must be accurate. The ZyWALL's Real Time Chip (RTC) keeps track of the time and date. There is

also a software mechanism to set the time manually or get the current time and date from an external server.

To change your ZyWALL's time based on your local time zone and date, click **System > Date/Time**. The screen displays as shown. You can manually set the ZyWALL's time and date or have the ZyWALL get the date and time from a time server.

**Figure 492** System > Date and Time




The following table describes the labels in this screen.

**Table 237** System > Date and Time

| LABEL | DESCRIPTION |
|---|---|
| Current Time and Date | |
| Current Time | This field displays the present time of your ZyWALL. |
| Current Date | This field displays the present date of your ZyWALL. |
| Time and Date Setup | |
| Manual | Select this radio button to enter the time and date manually. If you configure a new time and date, time zone and daylight saving at the same time, the time zone and daylight saving will affect the new time and date you entered. When you enter the time settings manually, the ZyWALL uses the new setting once you click **Apply**. |
| New Time (hh-mm-ss) | This field displays the last updated time from the time server or the last time configured manually.<br>When you set **Time and Date Setup** to **Manual**, enter the new time in this field and then click **Apply**. |

**Table 237** System > Date and Time (continued)

| LABEL | DESCRIPTION |
|---|---|
| New Date (yyyy-mm-dd) | This field displays the last updated date from the time server or the last date configured manually.<br>When you set **Time and Date Setup** to **Manual**, enter the new date in this field and then click **Apply**. |
| Get from Time Server | Select this radio button to have the ZyWALL get the time and date from the time server you specify below. The ZyWALL requests time and date settings from the time server under the following circumstances.<br>• When the ZyWALL starts up.<br>• When you click **Apply** or **Synchronize Now** in this screen.<br>• 24-hour intervals after starting up. |
| Time Server Address | Enter the IP address or URL of your time server. Check with your ISP/ network administrator if you are unsure of this information. |
| Synchronize Now | Click this button to have the ZyWALL get the time and date from a time server (see the **Time Server Address** field). This also saves your changes (except the daylight saving settings). |
| Time Zone Setup | |
| Time Zone | Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT). |
| Enable Daylight Saving | Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.<br>Select this option if you use Daylight Saving Time. |
| Start Date | Configure the day and time when Daylight Saving Time starts if you selected **Enable Daylight Saving**. The **at** field uses the 24 hour format. Here are a couple of examples:<br>Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Second**, **Sunday**, **March** and type 2 in the **at** field.<br>Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **March**. The time you type in the **at** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1). |

**Table 237** System > Date and Time (continued)

| LABEL | DESCRIPTION |
|---|---|
| End Date | Configure the day and time when Daylight Saving Time ends if you selected **Enable Daylight Saving**. The **at** field uses the 24 hour format. Here are a couple of examples:<br><br>Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **First**, **Sunday**, **November** and type 2 in the **at** field.<br><br>Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **October**. The time you type in the **at** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1). |
| Offset | Specify how much the clock changes when daylight saving begins and ends.<br><br>Enter a number from 1 to 5.5 (by 0.5 increments).<br><br>For example, if you set this field to 3.5, a log occurred at 6 P.M. in local official time will appear as if it had occurred at 10:30 P.M. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 45.3.1 Pre-defined NTP Time Servers List

When you turn on the ZyWALL for the first time, the date and time start at 2003-01-01 00:00:00. The ZyWALL then attempts to synchronize with one of the following pre-defined list of Network Time Protocol (NTP) time servers.

The ZyWALL continues to use the following pre-defined list of NTP time servers if you do not specify a time server or it cannot synchronize with the time server you specified.

**Table 238** Default Time Servers

| |
|---|
| 0.pool.ntp.org |
| 1.pool.ntp.org |
| 2.pool.ntp.org |

When the ZyWALL uses the pre-defined list of NTP time servers, it randomly selects one server and tries to synchronize with it. If the synchronization fails, then the ZyWALL goes through the rest of the list in order from the first one tried until either it is successful or all the pre-defined NTP time servers have been tried.

## 45.3.2 Time Server Synchronization

Click the **Synchronize Now** button to get the time and date from the time server you specified in the **Time Server Address** field.

When the **Please Wait...** screen appears, you may have to wait up to one minute.

**Figure 493** Synchronization in Process


The **Current Time** and **Current Date** fields will display the appropriate settings if the synchronization is successful.

If the synchronization was not successful, a log displays in the **View Log** screen. Try reconfiguring the **Date/Time** screen.

To manually set the ZyWALL date and time.

1 Click **System > Date/Time**.

2 Select **Manual** under **Time and Date Setup**.

3 Enter the ZyWALL's time in the **New Time** field.

4 Enter the ZyWALL's date in the **New Date** field.

5 Under **Time Zone Setup**, select your **Time Zone** from the list.

6 As an option you can select the **Enable Daylight Saving** check box to adjust the ZyWALL clock for daylight savings.

7 Click **Apply**.

To get the ZyWALL date and time from a time server

1 Click **System > Date/Time**.

2 Select **Get from Time Server** under **Time and Date Setup**.

3 Under **Time Zone Setup**, select your **Time Zone** from the list.

4 As an option you can select the **Enable Daylight Saving** check box to adjust the ZyWALL clock for daylight savings.

5 Under **Time and Date Setup**, enter a **Time Server Address** (Table 238 on page 735).

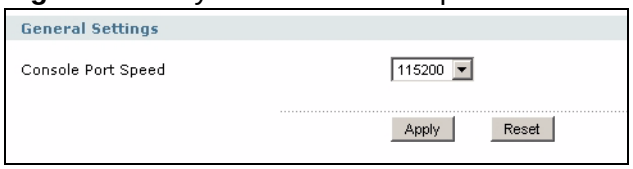
6 Click **Apply**.

# 45.4 Console Port Speed

This section shows you how to set the console port speed when you connect to the ZyWALL via the console port using a terminal emulation program. See Table 2 on page 33 for default console port settings.

Click **System > Console Speed** to open the **Console Speed** screen.

**Figure 494** System > Console Speed




The following table describes the labels in this screen.

**Table 239** System > Console Speed

| LABEL | DESCRIPTION |
|---|---|
| Console Port Speed | Use the drop-down list box to change the speed of the console port. Your ZyWALL supports 9600, 19200, 38400, 57600, and 115200 bps (default) for the console port.<br><br>The **Console Port Speed** applies to a console port connection using terminal emulation software and NOT the **Console** in the ZyWALL Web Configurator **Status** screen. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# 45.5 DNS Overview

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it.

## 45.5.1 DNS Server Address Assignment

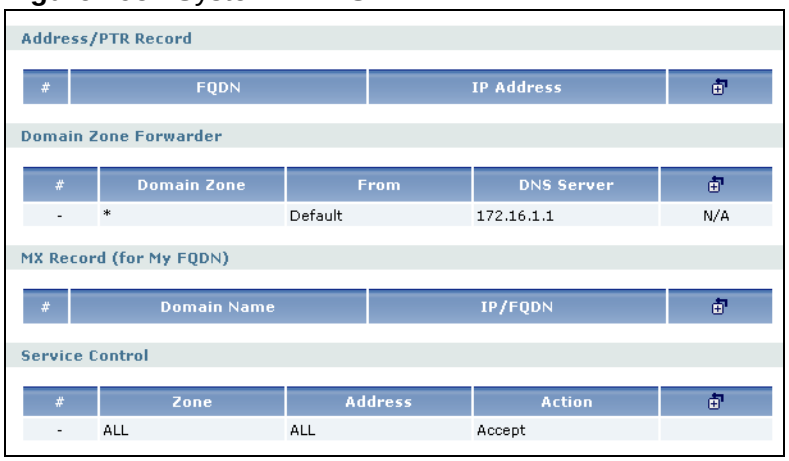
The ZyWALL can get the DNS server addresses in the following ways.

- The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, manually enter them in the DNS server fields.
- If your ISP dynamically assigns the DNS server IP addresses (along with the ZyWALL's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.
- You can manually enter the IP addresses of other DNS servers.

## 45.5.2 Configuring the DNS Screen

Click **System > DNS** to change your ZyWALL's DNS settings. Use the **DNS** screen to configure the ZyWALL to use a DNS server to resolve domain names for ZyWALL system features like VPN, DDNS and the time server. You can also configure the ZyWALL to accept or discard DNS queries. Use the **Network > Interface** screens to configure the DNS server information that the ZyWALL sends to the specified DHCP client devices.

**Figure 495** System > DNS




The following table describes the labels in this screen.

**Table 240** System > DNS

| LABEL | DESCRIPTION |
|---|---|
| Address/PTR Record | This record specifies the mapping of a Fully-Qualified Domain Name (FQDN) to an IP address. An FQDN consists of a host and domain name. For example, www.zyxel.com.tw is a fully qualified domain name, where "www" is the host, "zyxel" is the third-level domain, "com" is the second-level domain, and "tw" is the top level domain. |
| # | This is the index number of the address/PTR record. |
| FQDN | This is a host's fully qualified domain name. |
| IP Address | This is the IP address of a host. |

**Table 240** System > DNS (continued)

| LABEL | DESCRIPTION |
|---|---|
| Add icon | Click the **Add** icon in the heading row to open a screen where you can add a new address/PTR record. Refer to Table 241 on page 741 for information on the fields.<br><br>Click the **Edit** icon to go to the screen where you can edit the record.<br><br>Click the **Delete** icon to remove an existing record. A window display asking you to confirm that you want to delete the record. Note that subsequent records move up by one when you take this action. |
| Domain Zone Forwarder | This specifies a DNS server's IP address. The ZyWALL can query the DNS server to resolve domain zones for features like VPN, DDNS and the time server.<br><br>When the ZyWALL needs to resolve a domain zone, it checks it against the domain zone forwarder entries in the order that they appear in this list. |
| # | This is the index number of the domain zone forwarder record. The ordering of your rules is important as rules are applied in sequence.<br><br>A hyphen (-) displays for the default domain zone forwarder record. The default record is not configurable. The ZyWALL uses this default record if the domain zone that needs to be resolved does not match any of the other domain zone forwarder records. |
| Domain Zone | A domain zone is a fully qualified domain name without the host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name.<br><br>A "*" means all domain zones. |
| From | This displays whether the DNS server IP address is assigned by the ISP dynamically through a specified interface or configured manually. |
| DNS Server | This is the IP address of a DNS server. This field displays **N/A** if you have the ZyWALL get a DNS server IP address from the ISP dynamically but the specified interface is not active. |
| Add icon | Click the **Add** icon in the heading row to open a screen where you can add a new domain zone forwarder record. Refer to Table 242 on page 742 for information on the fields.<br><br>Click the **Edit** icon to go to the screen where you can edit the record.<br><br>Click the **Add** icon in an entry to add a record below the current entry.<br><br>Click the **Delete** icon to remove an existing record. A window display asking you to confirm that you want to delete the record. Note that subsequent records move up by one when you take this action.<br><br>Click the **Move to N** icon to display a field to type a number for where you want to put that record and press [ENTER] to move the record to the number that you typed. |
| MX Record (for My FQDN) | A MX (Mail eXchange) record identifies a mail server that handles the mail for a particular domain. |
| # | This is the index number of the MX record. |
| Domain Name | This is the domain name where the mail is destined for. |

**Table 240** System > DNS (continued)

| LABEL | DESCRIPTION |
|---|---|
| IP/FQDN | This is the IP address or Fully-Qualified Domain Name (FQDN) of a mail server that handles the mail for the domain specified in the field above. |
| Add icon | Click the **Add** icon in the heading row to open a screen where you can add a new MX record. Refer to Table 243 on page 743 for information on the fields.<br><br>Click the **Edit** icon to go to the screen where you can edit the record.<br><br>Click the **Delete** icon to remove an existing record. A window display asking you to confirm that you want to delete the record. Note that subsequent records move up by one when you take this action. |
| Service Control | This specifies from which computers and zones you can send DNS queries to the ZyWALL. |
| # | This the index number of the service control rule. The ordering of your rules is important as rules are applied in sequence.<br><br>The entry with a hyphen (-) instead of a number is the ZyWALL's (non-configurable) default policy. The ZyWALL applies this to traffic that does not match any other configured rule. It is not an editable rule. To apply other behavior, configure a rule that traffic will match so the ZyWALL will not have to use the default policy. |
| Zone | This is the zone on the ZyWALL the user is allowed or denied to access. |
| Address | This is the object name of the IP address(es) with which the computer is allowed or denied to send DNS queries. |
| Action | This displays whether the ZyWALL accepts DNS queries from the computer with the IP address specified above through the specified zone (**Accept**) or discards them (**Deny**). |
| Add icon | Click the **Add** icon in the heading row to open a screen where you can add a new rule. Refer to Table 244 on page 744 for information on the fields.<br><br>Click the **Edit** icon to go to the screen where you can edit the rule.<br><br>Click the **Add** icon in an entry to add a rule below the current entry.<br><br>Click the **Delete** icon to remove an existing rule. A window display asking you to confirm that you want to delete the rule. Note that subsequent rules move up by one when you take this action.<br><br>Click the **Move to N** icon to display a field to type a number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed. |

## 45.5.3 Address Record

An address record contains the mapping of a Fully-Qualified Domain Name (FQDN) to an IP address. An FQDN consists of a host and domain name. For example, www.zyxel.com is a fully qualified domain name, where "www" is the host, "zyxel" is the second-level domain, and "com" is the top level domain. mail.myZyXEL.com.tw is also a FQDN, where "mail" is the host, "myZyXEL" is the

third-level domain, “com” is the second-level domain, and “tw” is the top level domain.

The ZyWALL allows you to configure address records about the ZyWALL itself or another device. This way you can keep a record of DNS names and addresses that people on your network may use frequently. If the ZyWALL receives a DNS query for an FQDN for which the ZyWALL has an address record, the ZyWALL can send the IP address in a DNS response without having to query a DNS name server.

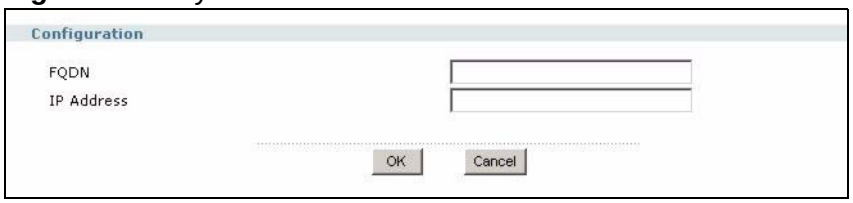
## 45.5.4 PTR Record

A PTR (pointer) record is also called a reverse record or a reverse lookup record. It is a mapping of an IP address to a domain name.

## 45.5.5 Adding an Address/PTR Record

Click the **Add** icon in the **Address/PTR Record** table to add an address/PTR record.

**Figure 496** System > DNS > Address/PTR Record Edit




The following table describes the labels in this screen.

**Table 241** System > DNS > Address/PTR Record Edit

| LABEL | DESCRIPTION |
|---|---|
| FQDN | Type a Fully-Qualified Domain Name (FQDN) of a server. An FQDN starts with a host name and continues all the way up to the top-level domain name. For example, www.zyxel.com.tw is a fully qualified domain name, where “www” is the host, “zyxel” is the third-level domain, “com” is the second-level domain, and “tw” is the top level domain. Underscores are not allowed. |
| IP Address | Enter the IP address of the host in dotted decimal notation. |
| OK | Click **OK** to save your customized settings and exit this screen. |
| Cancel | Click **Cancel** to exit this screen without saving |

## 45.5.6 Domain Zone Forwarder

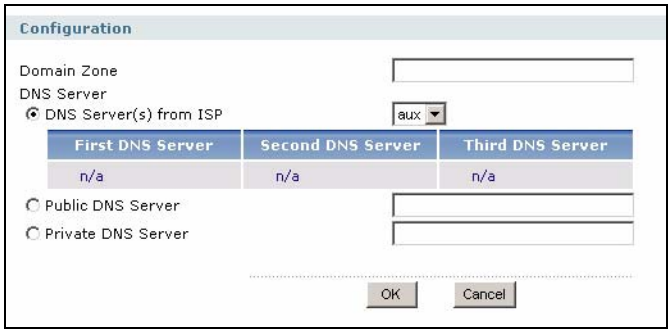
A domain zone forwarder contains a DNS server’s IP address. The ZyWALL can query the DNS server to resolve domain zones for features like VPN, DDNS and the time server. A domain zone is a fully qualified domain name without the host.

For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name.

## 45.5.7 Adding a Domain Zone Forwarder

Click the **Add** icon in the **Domain Zone Forwarder** table to add a domain zone forwarder record.

**Figure 497** System > DNS > Domain Zone Forwarder Add




The following table describes the labels in this screen.

**Table 242** System > DNS > Domain Zone Forwarder Add

| LABEL | DESCRIPTION |
|---|---|
| Domain Zone | A domain zone is a fully qualified domain name without the host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name. For example, whenever the ZyWALL receives needs to resolve a zyxel.com.tw domain name, it can send a query to the recorded name server IP address.<br><br>Enter * if all domain zones are served by the specified DNS server(s). |
| DNS Server | Select **DNS Server(s) from ISP** if your ISP dynamically assigns DNS server information. You also need to select an interface through which the ISP provides the DNS server IP address(es). The interface should be activated and set to be a DHCP client. The fields below display the (read-only) DNS server IP address(es) that the ISP assigns. **N/A** displays for any DNS server IP address fields for which the ISP does not assign an IP address.<br><br>Select **Public DNS Server** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. The ZyWALL must be able to connect to the DNS server without using a VPN tunnel. The DNS server could be on the Internet or one of the ZyWALL's local networks. You cannot use 0.0.0.0.<br><br>Select **Private DNS Server** if you have the IP address of a DNS server to which the ZyWALL connects through a VPN tunnel. Enter the DNS server's IP address in the field to the right. You cannot use 0.0.0.0. |
| OK | Click **OK** to save your customized settings and exit this screen. |
| Cancel | Click **Cancel** to exit this screen without saving |

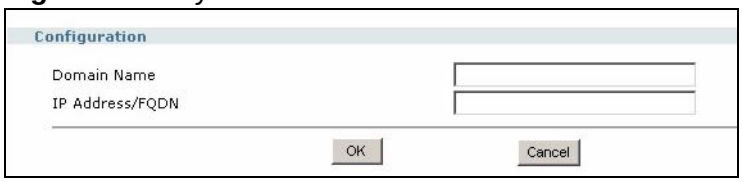
## 45.5.8 MX Record

A MX (Mail eXchange) record indicates which host is responsible for the mail for a particular domain, that is, controls where mail is sent for that domain. If you do not configure proper MX records for your domain or other domain, external e-mail from other mail servers will not be able to be delivered to your mail server and vice versa. Each host or domain can have only one MX record, that is, one domain is mapping to one host.

## 45.5.9 Adding a MX Record

Click the **Add** icon in the **MX Record** table to add a MX record.

**Figure 498** System > DNS > MX Record Add




The following table describes the labels in this screen.

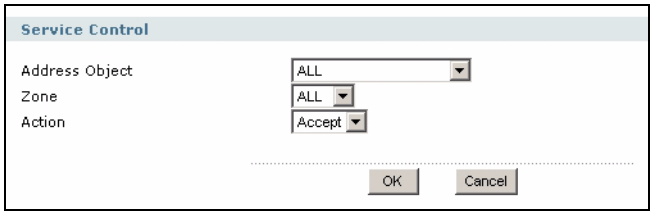
**Table 243** System > DNS > MX Record Add

| LABEL | DESCRIPTION |
|---|---|
| Domain Name | Enter the domain name where the mail is destined for. |
| IP Address/ FQDN | Enter the IP address or Fully-Qualified Domain Name (FQDN) of a mail server that handles the mail for the domain specified in the field above. |
| OK | Click **OK** to save your customized settings and exit this screen. |
| Cancel | Click **Cancel** to exit this screen without saving |

## 45.5.10 Adding a DNS Service Control Rule

Click the **Add** icon in the **Service Control** table to add a service control rule.

**Figure 499** System > DNS > Service Control Rule Add



The following table describes the labels in this screen.

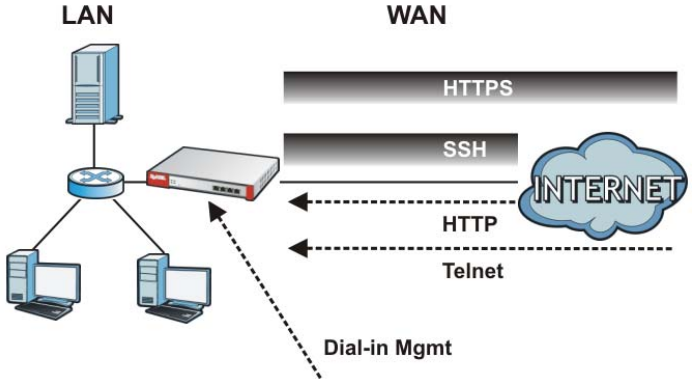
**Table 244** System > DNS > Service Control Rule Add

| LABEL | DESCRIPTION |
|---|---|
| Address Object | Select **ALL** to allow or deny any computer to send DNS queries to the ZyWALL.<br><br>Select a predefined address object to just allow or deny the computer with the IP address that you specified to send DNS queries to the ZyWALL. |
| Zone | Select **ALL** to allow or prevent DNS queries through any zones.<br><br>Select a predefined zone on which a DNS query to the ZyWALL is allowed or denied. |
| Action | Select **Accept** to have the ZyWALL allow the DNS queries from the specified computer.<br><br>Select **Deny** to have the ZyWALL reject the DNS queries from the specified computer. |
| OK | Click **OK** to save your customized settings and exit this screen. |
| Cancel | Click **Cancel** to exit this screen without saving |

# 45.6 WWW Overview

The following figure shows secure and insecure management of the ZyWALL coming in from the WAN. HTTPS and SSH access are secure. HTTP, Telnet, and dial-in management access are not secure.

**Figure 500** Secure and Insecure Service Access From the WAN




- See Section 5.6.1 on page 97 for related information on these screens.

Note: To allow the ZyWALL to be accessed from a specified computer using a service, make sure you do not have a service control rule or to-ZyWALL firewall rule to block that traffic.

- See To-ZyWALL Rules on page 345 for more on To-ZyWALL firewall rules.

- See Section 6.7 on page 134 for an example of configuring service control to block administrator HTTPS access from all zones except the LAN.

To stop a service from accessing the ZyWALL, clear **Enable** in the corresponding service screen.

## 45.6.1 Service Access Limitations

A service cannot be used to access the ZyWALL when:

1. You have disabled that service in the corresponding screen.
2. The allowed IP address (address object) in the **Service Control** table does not match the client IP address (the ZyWALL disallows the session).
3. The IP address (address object) in the **Service Control** table is not in the allowed zone or the action is set to **Deny**.
4. There is a firewall rule that blocks it.

## 45.6.2 System Timeout

There is a lease timeout for administrators. The ZyWALL automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling.

Each user is also forced to log in the ZyWALL for authentication again when the reauthentication time expires.

You can change the timeout settings in the **User / Group** screens.

## 45.6.3 HTTPS

You can set the ZyWALL to use HTTP or HTTPS (HTTPS adds security) for Web Configurator sessions. Specify which zones allow Web Configurator access and from which IP address the access can come.

HTTPS (HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a web protocol that encrypts and decrypts web pages. Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data by ensuring confidentiality (an unauthorized party cannot read the transferred data), authentication (one party can identify the other party) and data integrity (you know if data has been changed).

It relies upon certificates, public keys, and private keys (see Chapter 43 on page 699 for more information).

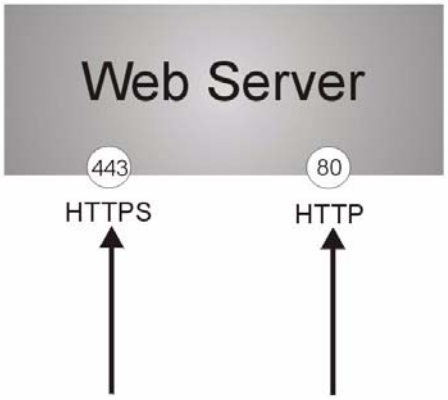
HTTPS on the ZyWALL is used so that you can securely access the ZyWALL using the Web Configurator. The SSL protocol specifies that the HTTPS server (the ZyWALL) must always authenticate itself to the HTTPS client (the computer which requests the HTTPS connection with the ZyWALL), whereas the HTTPS client only should authenticate itself when the HTTPS server requires it to do so (select **Authenticate Client Certificates** in the **WWW** screen). **Authenticate Client Certificates** is optional and if selected means the HTTPS client must send the ZyWALL a certificate. You must apply for a certificate for the browser from a CA that is a trusted CA on the ZyWALL.

Please refer to the following figure.

1 HTTPS connection requests from an SSL-aware web browser go to port 443 (by default) on the ZyWALL's web server.

2 HTTP connection requests from a web browser go to port 80 (by default) on the ZyWALL's web server.

**Figure 501** HTTP/HTTPS Implementation



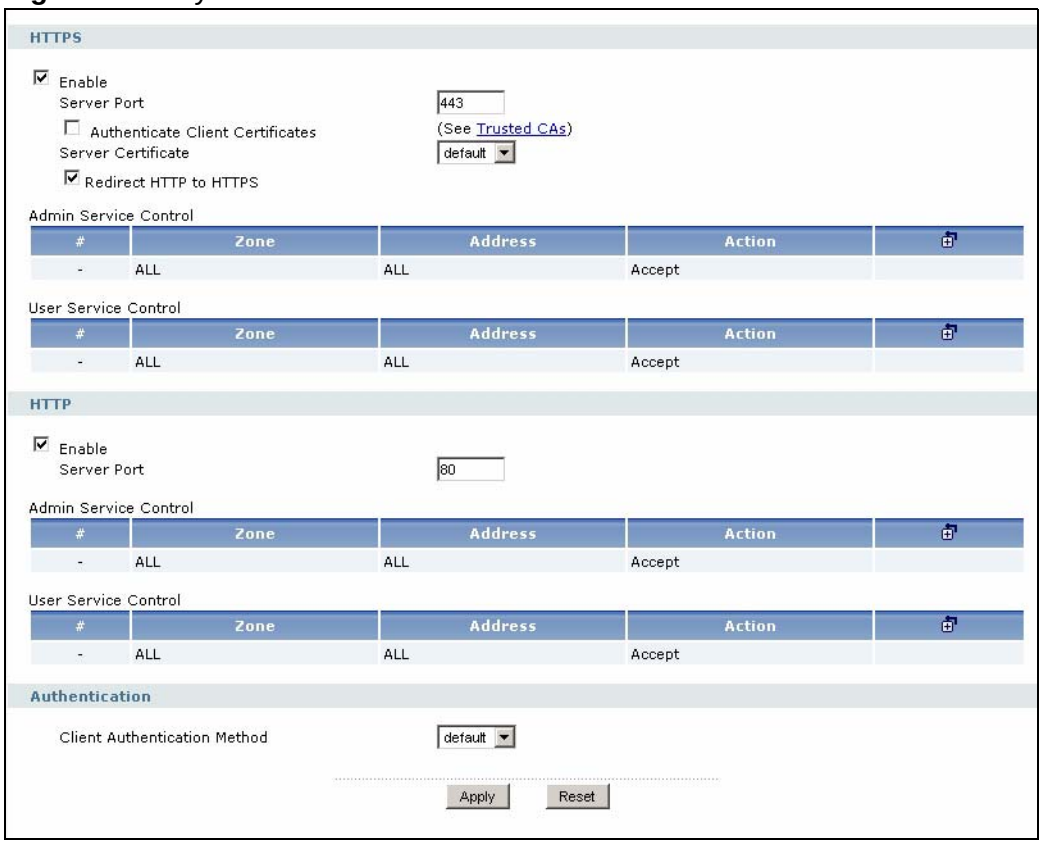

Note: If you disable **HTTP** in the **WWW** screen, then the ZyWALL blocks all HTTP connection attempts.

## 45.6.4 Configuring WWW Service Control

Click **System > WWW** to open the **WWW** screen. Use this screen to specify from which zones you can access the ZyWALL using HTTP or HTTPS. You can also specify which IP addresses the access can come from.

Note: **Admin Service Control** deals with management access (to the Web Configurator).
**User Service Control** deals with user access to the ZyWALL (logging into SSL VPN for example).

**Figure 502** System > WWW > Service Control




The following table describes the labels in this screen.

**Table 245** System > WWW > Service Control

| LABEL | DESCRIPTION |
|---|---|
| HTTPS | |
| Enable | Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the **Service Control** table to access the ZyWALL Web Configurator using secure HTTPs connections. |
| Server Port | The HTTPS server listens on port 443 by default. If you change the HTTPS server port to a different number on the ZyWALL, for example 8443, then you must notify people who need to access the ZyWALL Web Configurator to use "https://ZyWALL IP Address:**8443**" as the URL. |
| Authenticate Client Certificates | Select **Authenticate Client Certificates** (optional) to require the SSL client to authenticate itself to the ZyWALL by sending the ZyWALL a certificate. To do that the SSL client must have a CA-signed certificate from a CA that has been imported as a trusted CA on the ZyWALL (see Section 45.6.7.5 on page 757 on importing certificates for details). |

**Table 245** System > WWW > Service Control (continued)

| LABEL | DESCRIPTION |
|---|---|
| Server Certificate | Select a certificate the HTTPS server (the ZyWALL) uses to authenticate itself to the HTTPS client. You must have certificates already configured in the **My Certificates** screen. |
| Redirect HTTP to HTTPS | To allow only secure Web Configurator access, select this to redirect all HTTP connection requests to the HTTPS server. |
| Admin/User Service Control | **Admin Service Control** specifies from which zones an administrator can use HTTPS to manage the ZyWALL (using the Web Configurator). You can also specify the IP addresses from which the administrators can manage the ZyWALL.<br><br>**User Service Control** specifies from which zones a user can use HTTPS to log into the ZyWALL (to log into SSL VPN for example). You can also specify the IP addresses from which the users can access the ZyWALL. |
| # | This is the index number of the service control rule.<br><br>The entry with a hyphen (-) instead of a number is the ZyWALL's (non-configurable) default policy. The ZyWALL applies this to traffic that does not match any other configured rule. It is not an editable rule. To apply other behavior, configure a rule that traffic will match so the ZyWALL will not have to use the default policy. |
| Zone | This is the zone on the ZyWALL the user is allowed or denied to access. |
| Address | This is the object name of the IP address(es) with which the computer is allowed or denied to access. |
| Action | This displays whether the computer with the IP address specified above can access the ZyWALL zone(s) configured in the **Zone** field (**Accept**) or not (**Deny**). |
| Add icon | Click the **Add** icon in the heading row to open a screen where you can add a new rule. Refer to Table 246 on page 750 for information on the fields.<br><br>Click the **Edit** icon to go to the screen where you can edit the rule.<br><br>Click the **Add** icon in an entry to add a rule below the current entry.<br><br>Click the **Delete** icon to remove an existing rule. A window display asking you to confirm that you want to delete the rule. Note that subsequent rules move up by one when you take this action.<br><br>Click the **Move to N** icon to display a field to type a number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed. |
| HTTP | |
| Enable | Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the **Service Control** table to access the ZyWALL Web Configurator using HTTP connections. |
| Server Port | You may change the server port number for a service if needed, however you must use the same port number in order to use that service to access the ZyWALL. |

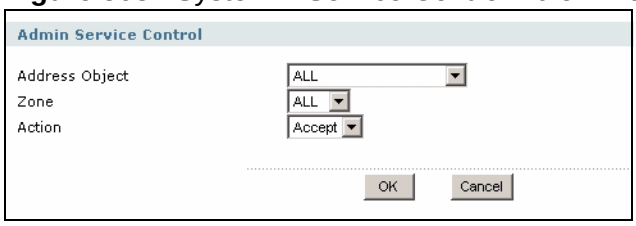
**Table 245** System > WWW > Service Control (continued)

| LABEL | DESCRIPTION |
|---|---|
| Admin/User Service Control | **Admin Service Control** specifies from which zones an administrator can use HTTP to manage the ZyWALL (using the Web Configurator). You can also specify the IP addresses from which the administrators can manage the ZyWALL.<br><br>**User Service Control** specifies from which zones a user can use HTTP to log into the ZyWALL (to log into SSL VPN for example). You can also specify the IP addresses from which the users can access the ZyWALL. |
| # | This is the index number of the service control rule.<br><br>The entry with a hyphen (-) instead of a number is the ZyWALL's (non-configurable) default policy. The ZyWALL applies this to traffic that does not match any other configured rule. It is not an editable rule. To apply other behavior, configure a rule that traffic will match so the ZyWALL will not have to use the default policy. |
| Zone | This is the zone on the ZyWALL the user is allowed or denied to access. |
| Address | This is the object name of the IP address(es) with which the computer is allowed or denied to access. |
| Action | This displays whether the computer with the IP address specified above can access the ZyWALL zone(s) configured in the **Zone** field (**Accept**) or not (**Deny**). |
| Add icon | Click the **Add** icon in the heading row to open a screen where you can add a new rule. Refer to Table 246 on page 750 for information on the fields.<br><br>Click the **Edit** icon to go to the screen where you can edit the rule.<br><br>Click the **Add** icon in an entry to add a rule below the current entry.<br><br>Click the **Delete** icon to remove an existing rule. A window display asking you to confirm that you want to delete the rule. Note that subsequent rules move up by one when you take this action.<br><br>Click the **Move to N** icon to display a field to type a number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed. |
| Authentication | |
| Client Authentication Method | Select a method the HTTPS or HTTP server uses to authenticate a client.<br><br>You must have configured the authentication methods in the **Auth. method** screen. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 45.6.5 Service Control Rules

Click **Add** or **Edit** in the **Service Control** table in a **WWW**, **SSH**, **Telnet**, **FTP** or **SNMP** screen to add a service control rule.

**Figure 503** System > Service Control Rule > Edit




The following table describes the labels in this screen.

**Table 246** System > Service Control Rule > Edit

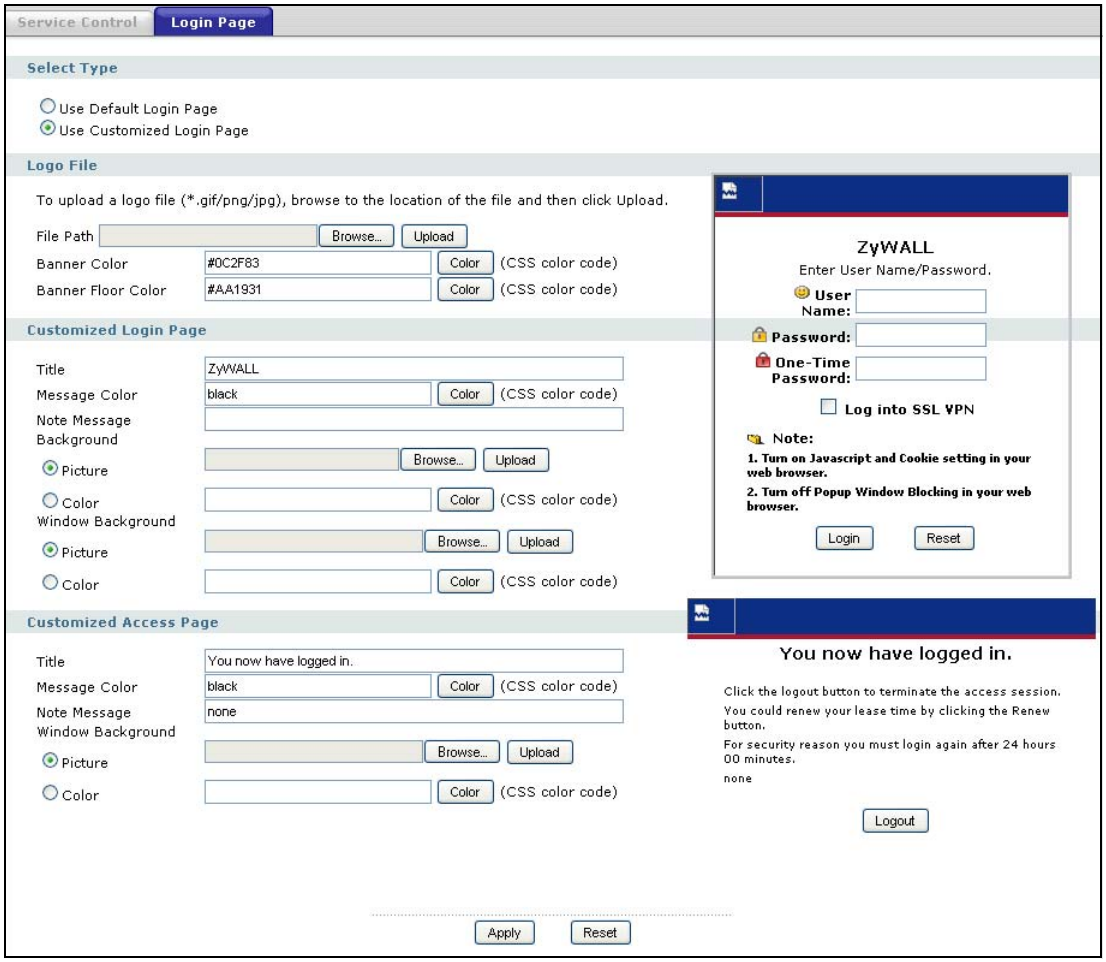
| LABEL | DESCRIPTION |
|---|---|
| Address Object | Select **ALL** to allow or deny any computer to communicate with the ZyWALL using this service.<br><br>Select a predefined address object to just allow or deny the computer with the IP address that you specified to access the ZyWALL using this service. |
| Zone | Select **ALL** to allow or prevent any ZyWALL zones from being accessed using this service.<br><br>Select a predefined ZyWALL zone on which a incoming service is allowed or denied. |
| Action | Select **Accept** to allow the user to access the ZyWALL from the specified computers.<br><br>Select **Deny** to block the user's access to the ZyWALL from the specified computers. |
| OK | Click **OK** to save your customized settings and exit this screen. |
| Cancel | Click **Cancel** to exit this screen without saving |

## 45.6.6 Customizing the WWW Login Page

Click **System > WWW > Login Page** to open the **Login Page** screen. Use this screen to customize the Web Configurator login screen. You can also customize the page that displays after an access user logs into the Web Configurator to

access network services like the Internet. See Chapter 37 on page 649 for more on access user accounts.

**Figure 504** System > WWW > Login Page



The following figures identify the parts you can customize in the login and access pages.

**Figure 505** Login Page Customization

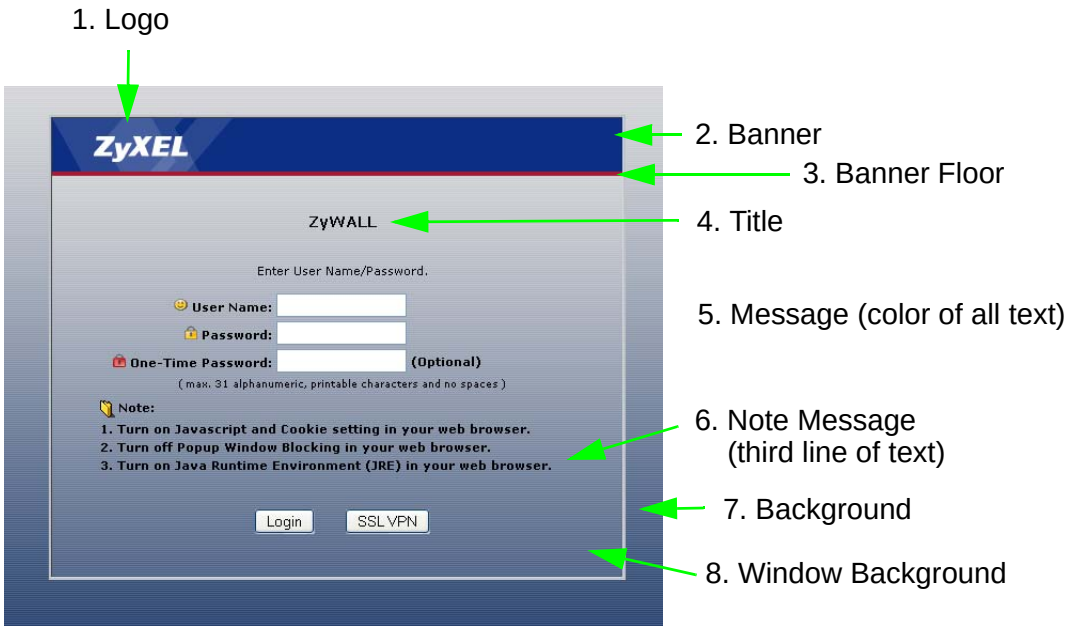



**Figure 506** Access Page Customization


You can specify colors in one of the following ways:

- Click **Color** to display a screen of web-safe colors from which to choose.
- Enter the name of the desired color.
- Enter a pound sign (#) followed by the six-digit hexadecimal number that represents the desired color. For example, use “#000000” for black.
- Enter “rgb” followed by red, green, and blue values in parenthesis and separate by commas. For example, use “rgb(0,0,0)” for black.

Your desired color should display in the preview screen on the right after you click in another field, click **Apply**, or press [ENTER]. If your desired color does not display, your browser may not support it. Try selecting another color.

The following table describes the labels in the screen.

**Table 247** System > WWW > Login Page

| LABEL | DESCRIPTION |
|---|---|
| Select Type | Select whether the Web Configurator uses the default login screen or one that you customize in the rest of this screen. |
| Logo File | You can upload a graphic logo to be displayed on the upper left corner of the Web Configurator login screen and access page.<br>Specify the location and file name of the logo graphic or click **Browse** to locate it.<br>Note: Use a GIF, JPG, or PNG of 100 kilobytes or less. |
| Browse | Click **Browse** to locate the graphic file on your computer. |
| Upload | Click **Upload** to transfer the specified graphic file from your computer to the ZyWALL. |
| Banner Color | Specify the color of the banner across the top of the login screen and access page. |
| Banner Floor Color | Specify the color of the line below the banner that goes across the top of the login screen and access page. |
| Customized Login Page | Use this section to set how the Web Configurator login screen looks. |
| Title | Enter the title for the top of the screen. Use up to 64 printable ASCII characters. Spaces are allowed. |
| Message Color | Specify the color of the screen's text. |
| Note Message | Enter a note to display at the bottom of the screen. Use up to 64 printable ASCII characters. Spaces are allowed. |
| Background | Set how the screen background looks.<br>To use a graphic, select **Picture** and upload a graphic. Specify the location and file name of the logo graphic or click **Browse** to locate it.<br>Note: Use a GIF, JPG, or PNG of 100 kilobytes or less.<br>To use a color, select **Color** and specify the color. |
| Window Background | Set how the window's background looks.<br>To use a graphic, select **Picture** and upload a graphic. Specify the location and file name of the logo graphic or click **Browse** to locate it.<br>Note: Use a GIF, JPG, or PNG of 100 kilobytes or less.<br>To use a color, select **Color** and specify the color. |
| Customized Access Page | Use this section to customize the page that displays after an access user logs into the Web Configurator to access network services like the Internet. |

**Table 247** System > WWW > Login Page

| LABEL | DESCRIPTION |
|---|---|
| Title | Enter the title for the top of the screen. Use up to 64 printable ASCII characters. Spaces are allowed. |
| Message Color | Specify the color of the screen's text. |
| Note Message | Enter a note to display below the title. Use up to 64 printable ASCII characters. Spaces are allowed. |
| Window Background | Set how the window's background looks.<br>To use a graphic, select **Picture** and upload a graphic. Specify the location and file name of the logo graphic or click **Browse** to locate it.<br>Note: Use a GIF, JPG, or PNG of 100 kilobytes or less.<br>To use a color, select **Color** and specify the color. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 45.6.7 HTTPS Example

If you haven't changed the default HTTPS port on the ZyWALL, then in your browser enter "https://ZyWALL IP Address/" as the web site address where "ZyWALL IP Address" is the IP address or domain name of the ZyWALL you wish to access.

### 45.6.7.1 Internet Explorer Warning Messages

When you attempt to access the ZyWALL HTTPS server, a Windows dialog box pops up asking if you trust the server certificate. Click **View Certificate** if you want to verify that the certificate is from the ZyWALL.

You see the following **Security Alert** screen in Internet Explorer. Select **Yes** to proceed to the Web Configurator login screen; if you select **No**, then Web Configurator access is blocked.

**Figure 507** Security Alert Dialog Box (Internet Explorer)


## 45.6.7.2 Netscape Navigator Warning Messages

When you attempt to access the ZyWALL HTTPS server, a **Website Certified by an Unknown Authority** screen pops up asking if you trust the server certificate. Click **Examine Certificate** if you want to verify that the certificate is from the ZyWALL.

If **Accept this certificate temporarily for this session** is selected, then click **OK** to continue in Netscape.

Select **Accept this certificate permanently** to import the ZyWALL's certificate into the SSL client.

**Figure 508** Security Certificate 1 (Netscape)


**Figure 509** Security Certificate 2 (Netscape)


## 45.6.7.3 Avoiding Browser Warning Messages

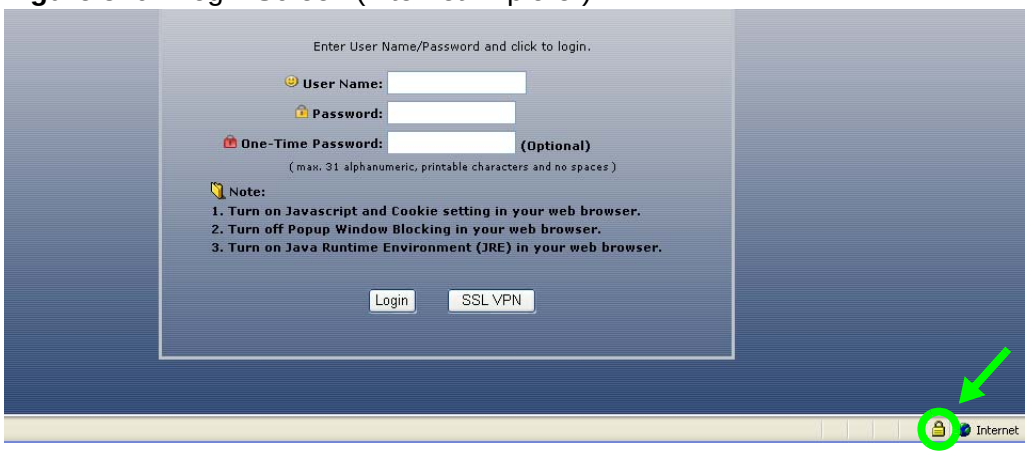
Here are the main reasons your browser displays warnings about the ZyWALL's HTTPS server certificate and what you can do to avoid seeing the warnings:

- The issuing certificate authority of the ZyWALL's HTTPS server certificate is not one of the browser's trusted certificate authorities. The issuing certificate authority of the ZyWALL's factory default certificate is the ZyWALL itself since the certificate is a self-signed certificate.
- For the browser to trust a self-signed certificate, import the self-signed certificate into your operating system as a trusted certificate.
- To have the browser trust the certificates issued by a certificate authority, import the certificate authority's certificate into your operating system as a trusted certificate. Refer to Appendix D on page 915 for details.

### 45.6.7.4 Login Screen

After you accept the certificate, the ZyWALL login screen appears. The lock displayed in the bottom of the browser status bar denotes a secure connection.

**Figure 510** Login Screen (Internet Explorer)



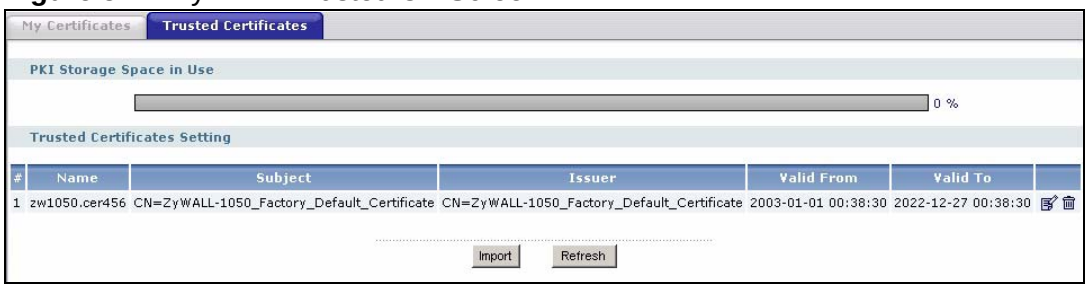

### 45.6.7.5 Enrolling and Importing SSL Client Certificates

The SSL client needs a certificate if **Authenticate Client Certificates** is selected on the ZyWALL.

You must have imported at least one trusted CA to the ZyWALL in order for the **Authenticate Client Certificates** to be active (see the Certificates chapter for details).

Apply for a certificate from a Certification Authority (CA) that is trusted by the ZyWALL (see the ZyWALL's **Trusted CA** Web Configurator screen).

**Figure 511** ZyWALL Trusted CA Screen

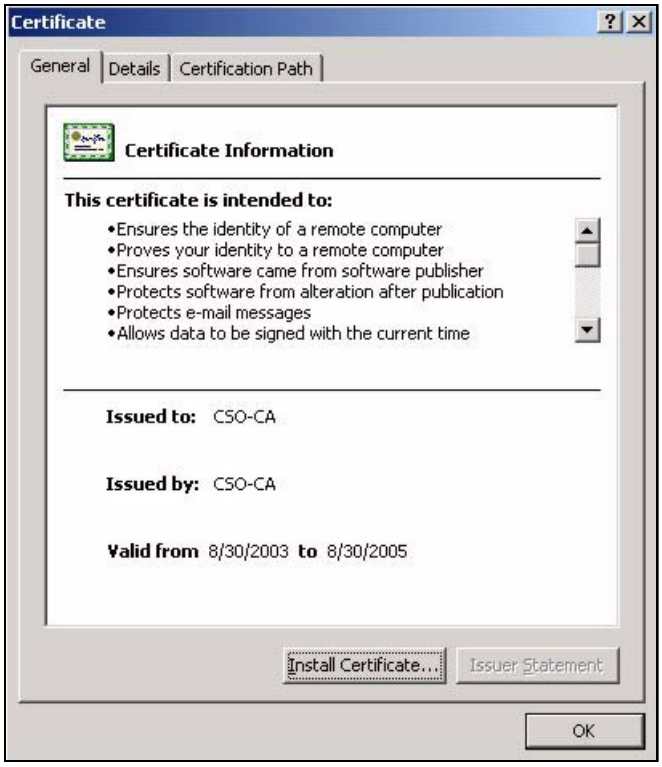



The CA sends you a package containing the CA's trusted certificate(s), your personal certificate(s) and a password to install the personal certificate(s).

#### *45.6.7.5.1 Installing the CA's Certificate*

1 Double click the CA's trusted certificate to produce a screen similar to the one shown next.

**Figure 512** CA Certificate Example




2 Click **Install Certificate** and follow the wizard as shown earlier in this appendix.

#### *45.6.7.5.2 Installing Your Personal Certificate(s)*

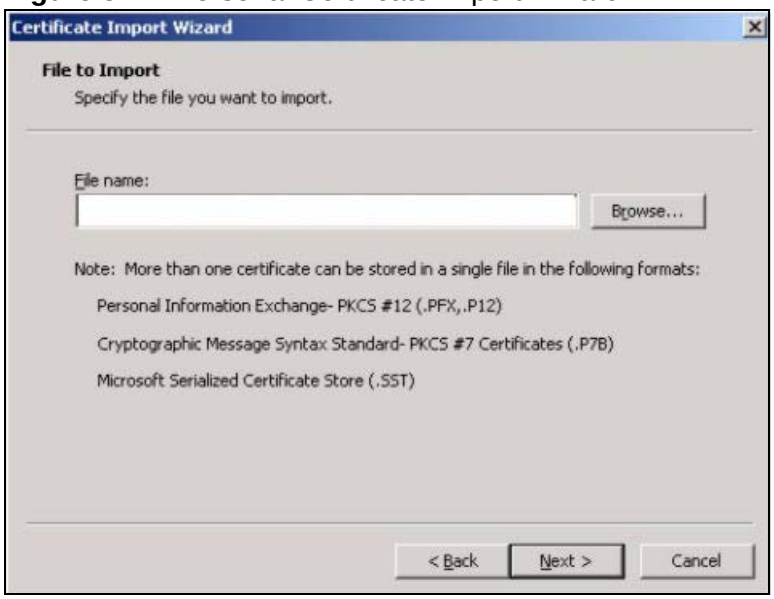
You need a password in advance. The CA may issue the password or you may have to specify it during the enrollment. Double-click the personal certificate given to you by the CA to produce a screen similar to the one shown next

1 Click **Next** to begin the wizard.

**Figure 513** Personal Certificate Import Wizard 1


2 The file name and path of the certificate you double-clicked should automatically appear in the **File name** text box. Click **Browse** if you wish to import a different certificate.

**Figure 514** Personal Certificate Import Wizard 2

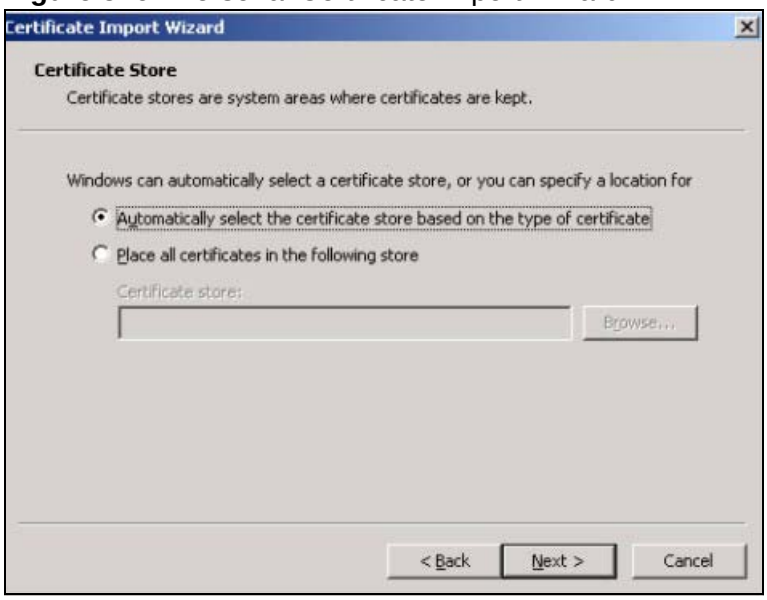


3 Enter the password given to you by the CA.

**Figure 515** Personal Certificate Import Wizard 3

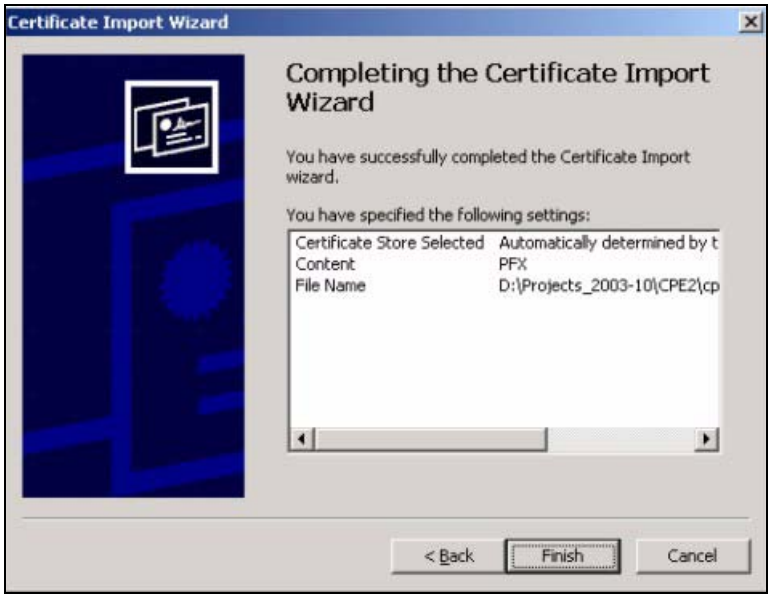

4 Have the wizard determine where the certificate should be saved on your computer or select **Place all certificates in the following store** and choose a different location.

**Figure 516** Personal Certificate Import Wizard 4



5 Click **Finish** to complete the wizard and begin the import process.

**Figure 517** Personal Certificate Import Wizard 5




6 You should see the following screen when the certificate is correctly installed on your computer.

**Figure 518** Personal Certificate Import Wizard 6


## 45.6.7.6 Using a Certificate When Accessing the ZyWALL Example

Use the following procedure to access the ZyWALL via HTTPS.

1 Enter 'https://ZyWALL IP Address/ in your browser's web address field.

**Figure 519** Access the ZyWALL Via HTTPS

2 When **Authenticate Client Certificates** is selected on the ZyWALL, the following screen asks you to select a personal certificate to send to the ZyWALL. This screen displays even if you only have a single certificate as in the example.

**Figure 520** SSL Client Authentication


3 You next see the Web Configurator login screen.

**Figure 521** Secure Web Configurator Login Screen


# 45.7 SSH

You can use SSH (Secure SHell) to securely access the ZyWALL's command line interface. Specify which zones allow SSH access and from which IP address the access can come.

SSH is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an

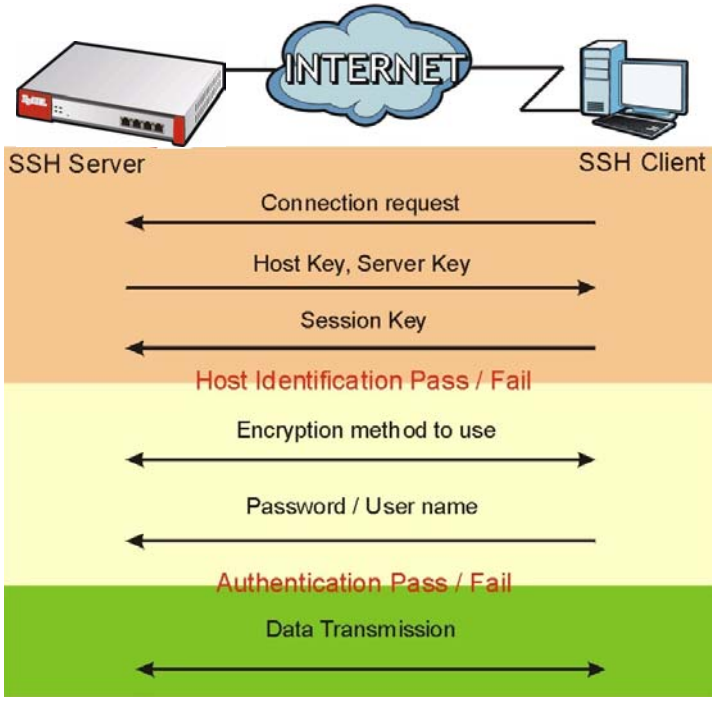
unsecured network. In the following figure, computer A on the Internet uses SSH to securely connect to the WAN port of the ZyWALL for a management session.

**Figure 522** SSH Communication Over the WAN Example


## 45.7.1 How SSH Works

The following figure is an example of how a secure connection is established between two remote hosts using SSH v1.

**Figure 523** How SSH v1 Works Example




1 Host Identification

The SSH client sends a connection request to the SSH server. The server identifies itself with a host key. The client encrypts a randomly generated session key with the host key and server key and sends the result back to the server.

The client automatically saves any new server public keys. In subsequent connections, the server public key is checked against the saved version on the client computer.

2 Encryption Method

Once the identification is verified, both the client and server must agree on the type of encryption method to use.

3 Authentication and Data Transmission

After the identification is verified and data encryption activated, a secure tunnel is established between the client and the server. The client then sends its authentication information (user name and password) to the server to log in to the server.

## 45.7.2 SSH Implementation on the ZyWALL

Your ZyWALL supports SSH versions 1 and 2 using RSA authentication and four encryption methods (AES, 3DES, Archfour, and Blowfish). The SSH server is implemented on the ZyWALL for management using port 22 (by default).

## 45.7.3 Requirements for Using SSH

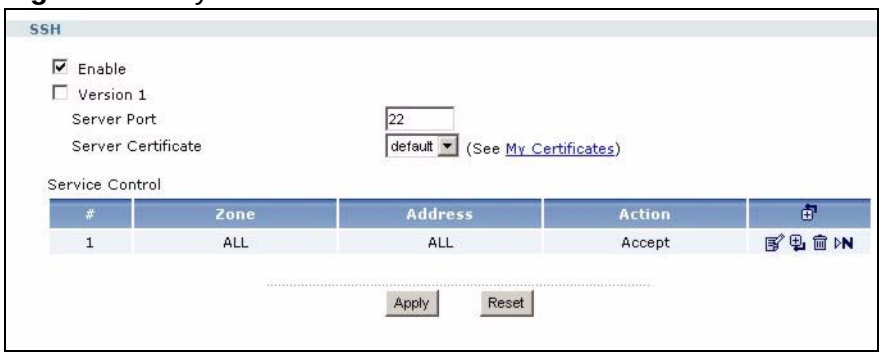
You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to the ZyWALL over SSH.

## 45.7.4 Configuring SSH

Click **System > SSH** to change your ZyWALL's Secure Shell settings. Use this screen to specify from which zones SSH can be used to manage the ZyWALL. You can also specify from which IP addresses the access can come.

Note: It is recommended that you disable Telnet and FTP when you configure SSH for secure connections.

**Figure 524** System > SSH



The following table describes the labels in this screen.

**Table 248** System > SSH

| LABEL | DESCRIPTION |
|---|---|
| Enable | Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the **Service Control** table to access the ZyWALL CLI using this service. |
| Version 1 | Select the check box to have the ZyWALL use both SSH version 1 and version 2 protocols. If you clear the check box, the ZyWALL uses only SSH version 2 protocol. |
| Server Port | You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management. |
| Server Certificate | Select the certificate whose corresponding private key is to be used to identify the ZyWALL for SSH connections. You must have certificates already configured in the **My Certificates** screen (Click **My Certificates** and see Chapter 43 on page 699 for details). |
| Service Control | This specifies from which computers you can access which ZyWALL zones. |
| # | This the index number of the service control rule. |
| Zone | This is the zone on the ZyWALL the user is allowed or denied to access. |
| Address | This is the object name of the IP address(es) with which the computer is allowed or denied to access. |
| Action | This displays whether the computer with the IP address specified above can access the ZyWALL zone(s) configured in the **Zone** field (**Accept**) or not (**Deny**). |
| Add icon | Click the **Add** icon in the heading row to open a screen where you can add a new rule. Refer to Table 246 on page 750 for information on the fields.<br>Click the **Edit** icon to go to the screen where you can edit the rule.<br>Click the **Add** icon in an entry to add a rule below the current entry.<br>Click the **Delete** icon to remove an existing rule. A window display asking you to confirm that you want to delete the rule. Note that subsequent rules move up by one when you take this action.<br>Click the **Move to N** icon to display a field to type a number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 45.7.5 Secure Telnet Using SSH Examples

This section shows two examples using a command interface and a graphical interface SSH client program to remotely access the ZyWALL. The configuration and connection steps are similar for most SSH client programs. Refer to your SSH client program user's guide.

### 45.7.5.1 Example 1: Microsoft Windows

This section describes how to access the ZyWALL using the Secure Shell Client program.

1 Launch the SSH client and specify the connection information (IP address, port number) for the ZyWALL.

2 Configure the SSH client to accept connection using SSH version 1.

3 A window displays prompting you to store the host key in you computer. Click **Yes** to continue.

**Figure 525** SSH Example 1: Store Host Key


Enter the password to log in to the ZyWALL. The CLI screen displays next.

### 45.7.5.2 Example 2: Linux

This section describes how to access the ZyWALL using the OpenSSH client program that comes with most Linux distributions.

1 Test whether the SSH service is available on the ZyWALL.

Enter "`telnet 192.168.1.1 22`" at a terminal prompt and press [ENTER]. The computer attempts to connect to port 22 on the ZyWALL (using the default IP address of 192.168.1.1).

A message displays indicating the SSH protocol version supported by the ZyWALL.

**Figure 526** SSH Example 2: Test

```
$ telnet 192.168.1.1 22
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.
SSH-1.5-1.0.0
```

2 Enter “ssh –1 192.168.1.1”. This command forces your computer to connect to the ZyWALL using SSH version 1. If this is the first time you are connecting to the ZyWALL using SSH, a message displays prompting you to save the host information of the ZyWALL. Type “yes” and press [ENTER].

Then enter the password to log in to the ZyWALL.

**Figure 527** SSH Example 2: Log in

```
$ ssh –1 192.168.1.1
The authenticity of host '192.168.1.1 (192.168.1.1)' can't be established.
RSA1 key fingerprint is 21:6c:07:25:7e:f4:75:80:ec:af:bd:d4:3d:80:53:d1.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.1' (RSA1) to the list of known hosts.
Administrator@192.168.1.1's password:
```

3 The CLI screen displays next.

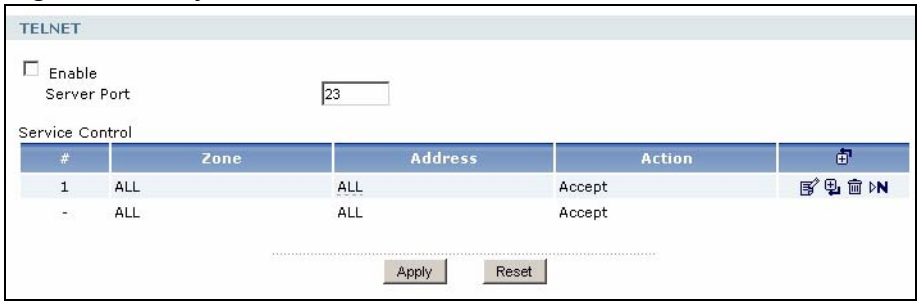
# 45.8 Telnet

You can use Telnet to access the ZyWALL’s command line interface. Specify which zones allow Telnet access and from which IP address the access can come.

## 45.8.1 Configuring Telnet

Click **System > TELNET** to configure your ZyWALL for remote Telnet access. Use this screen to specify from which zones Telnet can be used to manage the ZyWALL. You can also specify from which IP addresses the access can come.

**Figure 528** System > Telnet



The following table describes the labels in this screen.

**Table 249** System > Telnet

| LABEL | DESCRIPTION |
|---|---|
| Enable | Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the **Service Control** table to access the ZyWALL CLI using this service. |
| Server Port | You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management. |
| Service Control | This specifies from which computers you can access which ZyWALL zones. |
| # | This the index number of the service control rule.<br><br>The entry with a hyphen (-) instead of a number is the ZyWALL's (non-configurable) default policy. The ZyWALL applies this to traffic that does not match any other configured rule. It is not an editable rule. To apply other behavior, configure a rule that traffic will match so the ZyWALL will not have to use the default policy. |
| Zone | This is the zone on the ZyWALL the user is allowed or denied to access. |
| Address | This is the object name of the IP address(es) with which the computer is allowed or denied to access. |
| Action | This displays whether the computer with the IP address specified above can access the ZyWALL zone(s) configured in the **Zone** field (**Accept**) or not (**Deny**). |
| Add icon | Click the **Add** icon in the heading row to open a screen where you can add a new rule. Refer to Table 246 on page 750 for information on the fields.<br><br>Click the **Edit** icon to go to the screen where you can edit the rule.<br><br>Click the **Add** icon in an entry to add a rule below the current entry.<br><br>Click the **Delete** icon to remove an existing rule. A window display asking you to confirm that you want to delete the rule. Note that subsequent rules move up by one when you take this action.<br><br>Click the **Move to N** icon to display a field to type a number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

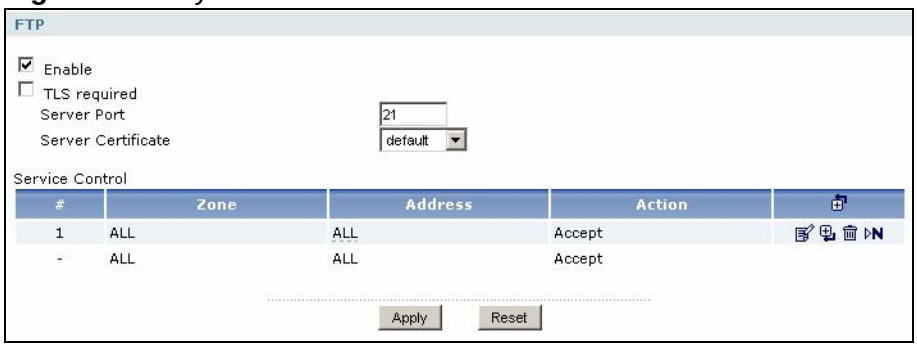
# 45.9 FTP

You can upload and download the ZyWALL's firmware and configuration files using FTP. To use this feature, your computer must have an FTP client. Please see Chapter 46 on page 781 for more information about firmware and configuration files.

## 45.9.1 Configuring FTP

To change your ZyWALL's FTP settings, click **System > FTP** tab. The screen appears as shown. Use this screen to specify from which zones FTP can be used to access the ZyWALL. You can also specify from which IP addresses the access can come.

**Figure 529** System > FTP




The following table describes the labels in this screen.

**Table 250** System > FTP

| LABEL | DESCRIPTION |
|---|---|
| Enable | Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the **Service Control** table to access the ZyWALL using this service. |
| TLS required | Select the check box to use FTP over TLS (Transport Layer Security) to encrypt communication.<br><br>This implements TLS as a security mechanism to secure FTP clients and/or servers. |
| Server Port | You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management. |
| Server Certificate | Select the certificate whose corresponding private key is to be used to identify the ZyWALL for FTP connections. You must have certificates already configured in the **My Certificates** screen (Click **My Certificates** and see Chapter 43 on page 699 for details). |
| Service Control | This specifies from which computers you can access which ZyWALL zones. |
| # | This the index number of the service control rule.<br><br>The entry with a hyphen (-) instead of a number is the ZyWALL's (non-configurable) default policy. The ZyWALL applies this to traffic that does not match any other configured rule. It is not an editable rule. To apply other behavior, configure a rule that traffic will match so the ZyWALL will not have to use the default policy. |
| Zone | This is the zone on the ZyWALL the user is allowed or denied to access. |
| Address | This is the object name of the IP address(es) with which the computer is allowed or denied to access. |

**Table 250** System > FTP (continued)

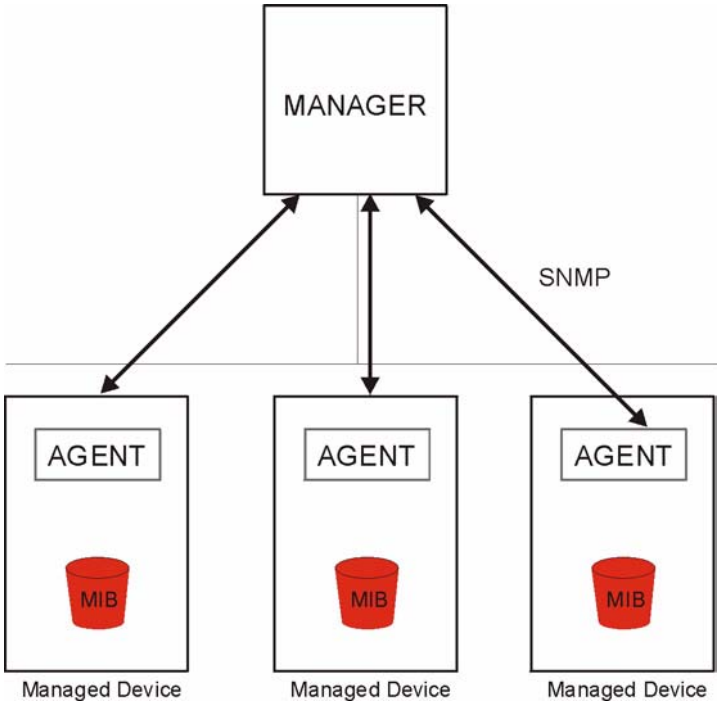
| LABEL | DESCRIPTION |
|---|---|
| Action | This displays whether the computer with the IP address specified above can access the ZyWALL zone(s) configured in the **Zone** field (**Accept**) or not (**Deny**). |
| Add icon | Click the **Add** icon in the heading row to open a screen where you can add a new rule. Refer to Table 246 on page 750 for information on the fields.<br><br>Click the **Edit** icon to go to the screen where you can edit the rule.<br><br>Click the **Add** icon in an entry to add a rule below the current entry.<br><br>Click the **Delete** icon to remove an existing rule. A window display asking you to confirm that you want to delete the rule. Note that subsequent rules move up by one when you take this action.<br><br>Click the **Move to N** icon to display a field to type a number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# 45.10 SNMP

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. Your ZyWALL supports SNMP agent functionality, which allows a manager station to manage and monitor the ZyWALL through the network. The ZyWALL supports SNMP version one (SNMPv1)

and version two (SNMPv2c). The next figure illustrates an SNMP management operation.

**Figure 530** SNMP Management Model




An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the ZyWALL). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.

- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

## 45.10.1 Supported MIBs

The ZyWALL supports MIB II that is defined in RFC-1213 and RFC-1215. The ZyWALL also supports private MIBs (zywall.mib and zyxel-zywall-ZLD-Common.mib) to collect information about CPU and memory usage and VPN total throughput. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance. You can download the ZyWALL's MIBs from www.zyxel.com.

## 45.10.2 SNMP Traps

The ZyWALL will send traps to the SNMP manager when any one of the following events occurs.

**Table 251** SNMP Traps

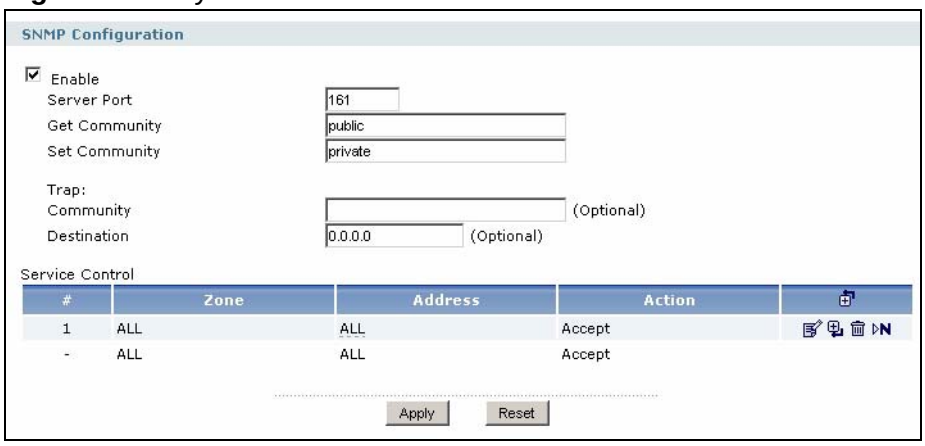
| OBJECT LABEL | OBJECT ID | DESCRIPTION |
|---|---|---|
| Cold Start | 1.3.6.1.6.3.1.1.5.1 | This trap is sent when the ZyWALL is turned on or an agent restarts. |
| linkDown | 1.3.6.1.6.3.1.1.5.3 | This trap is sent when the Ethernet link is down. |
| linkUp | 1.3.6.1.6.3.1.1.5.4 | This trap is sent when the Ethernet link is up. |
| authenticationFailure | 1.3.6.1.6.3.1.1.5.5 | This trap is sent when an SNMP request comes from non-authenticated hosts. |

## 45.10.3 Configuring SNMP

To change your ZyWALL's SNMP settings, click **System > SNMP** tab. The screen appears as shown. Use this screen to configure your SNMP settings, including

from which zones SNMP can be used to access the ZyWALL. You can also specify from which IP addresses the access can come.

**Figure 531** System > SNMP




The following table describes the labels in this screen.

**Table 252** System > SNMP

| LABEL | DESCRIPTION |
|---|---|
| Enable | Select the check box to allow or disallow the computer with the IP address that matches the IP address(es) in the **Service Control** table to access the ZyWALL using this service. |
| Server Port | You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management. |
| Get Community | Enter the **Get Community**, which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests. |
| Set Community | Enter the **Set community**, which is the password for incoming Set requests from the management station. The default is private and allows all requests. |
| Trap | |
| Community | Type the trap community, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests. |
| Destination | Type the IP address of the station to send your SNMP traps to. |
| Service Control | This specifies from which computers you can access which ZyWALL zones. |
| # | This the index number of the service control rule.<br><br>The entry with a hyphen (-) instead of a number is the ZyWALL's (non-configurable) default policy. The ZyWALL applies this to traffic that does not match any other configured rule. It is not an editable rule. To apply other behavior, configure a rule that traffic will match so the ZyWALL will not have to use the default policy. |
| Zone | This is the zone on the ZyWALL the user is allowed or denied to access. |
| Address | This is the object name of the IP address(es) with which the computer is allowed or denied to access. |

**Table 252** System > SNMP (continued)

| LABEL | DESCRIPTION |
|---|---|
| Action | This displays whether the computer with the IP address specified above can access the ZyWALL zone(s) configured in the **Zone** field (**Accept**) or not (**Deny**). |
| Add icon | Click the **Add** icon in the heading row to open a screen where you can add a new rule. Refer to Table 246 on page 750 for information on the fields.<br><br>Click the **Edit** icon to go to the screen where you can edit the rule.<br><br>Click the **Add** icon in an entry to add a rule below the current entry.<br><br>Click the **Delete** icon to remove an existing rule. A window display asking you to confirm that you want to delete the rule. Note that subsequent rules move up by one when you take this action.<br><br>Click the **Move to N** icon to display a field to type a number for where you want to put that rule and press [ENTER] to move the rule to the number that you typed. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# 45.11 Dial-in Management

Connect an external serial modem to the **AUX** port to provide a management connection in case the ZyWALL's other WAN connections are down. This is like an auxiliary interface, except it is used for management connections coming into the ZyWALL instead of as a backup WAN connection.

### AT Command Strings

For regular telephone lines, the default Dial string tells the modem that the line uses tone dialing. ATDT is the command for a switch that requires tone dialing. If your switch requires pulse dialing, change the string to ATDP.

### DTR Signal

The majority of WAN devices default to hanging up the current call when the DTR (Data Terminal Ready) signal is dropped by the DTE. When the Drop DTR When Hang Up check box is selected, the ZyWALL uses this hardware signal to force the WAN device to hang up, in addition to issuing the drop command ATH.

### Response Strings

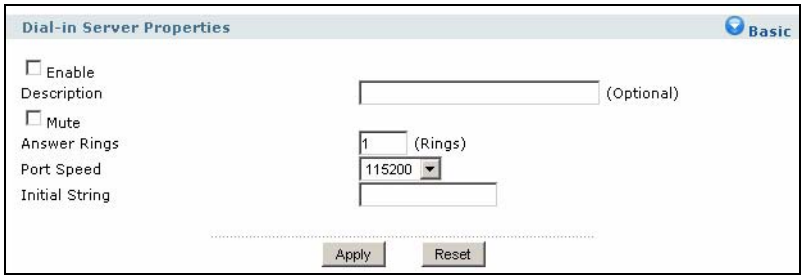
The response strings tell the ZyWALL the tags, or labels, immediately preceding the various call parameters sent from the serial modem. The response strings

have not been standardized; please consult the documentation of your serial modem to find the correct tags.

## 45.11.1 Configuring Dial-in Mgmt

Click **System** > **Dial-in Mgmt** to display the following screen. Configure this screen for dial-in management connections.

**Figure 532** System > Dial-in Mgmt




The following table describes the labels in this screen.

**Table 253** System > Dial-in Mgmt

| LABEL | DESCRIPTION |
|---|---|
| Dial-in Server Properties | Click **Advanced** to display more configuration fields and edit the details of your dial-in management setup. Click **Basic** to display fewer fields. |
| Enable | Select this check box to turn on dial-in management. |
| Description | Enter some information about this connection. |
| Mute | Select this check box to stop the external serial modem from making audible sounds during a dial-in management session. |
| Answer Rings | Set how many times the ZyWALL lets the incoming dial-in management session ring before processing it. |
| Port Speed | Use the drop-down list box to select the speed of the connection between the ZyWALL's auxiliary port and the external modem. Available speeds are: **9600**, **19200**, **38400**, **57600**, or **115200** bps. |
| Initial String | Type the AT command string that the ZyWALL returns to the external serial modem connected to the ZyWALL's auxiliary port during connection initialization.<br><br>Note: Consult the manual of your external serial modem connected to your ZyWALL's auxiliary port for specific AT commands. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# 45.12 Vantage CNM

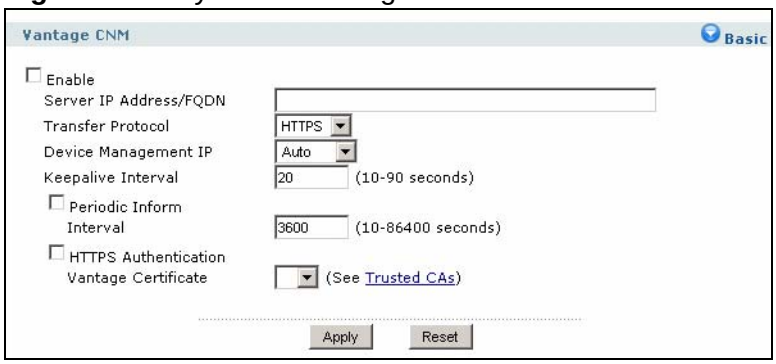
Vantage CNM (Centralized Network Management) is a browser-based global management solution that allows an administrator from any location to easily configure, manage, monitor and troubleshoot ZyXEL devices located worldwide. See the Vantage CNM User's Guide for details.

If you allow your ZyWALL to be managed by the Vantage CNM server, then you should not do any configurations directly to the ZyWALL (using either the Web Configurator or commands) without notifying the Vantage CNM administrator.

## 45.12.1 Configuring Vantage CNM

Vantage CNM is disabled on the device by default. Click **System > Vantage CNM** to configure your device's Vantage CNM settings.

**Figure 533** System > Vantage CNM




The following table describes the labels in this screen.

**Table 254** System > Vantage CNM

| LABEL | DESCRIPTION |
|---|---|
| Vantage CNM | Click **Advanced** to display more configuration fields or click **Basic** to display fewer fields. |
| Enable | Select this check box to allow Vantage CNM to manage your ZyWALL. |
| Server IP Address/FQDN | Enter the IP address or fully qualified domain name of the Vantage server.<br><br>If the Vantage CNM server is on a different subnet to the ZyWALL and is behind a NAT router, enter the WAN IP address of the NAT router here and configure the NAT router to forward UDP port 11864 traffic to the Vantage CNM server.<br><br>If the Vantage CNM server is behind a firewall, you may have to create a rule on the firewall to allow UDP port 11864 traffic through to the Vantage CNM server (most (new) ZyXEL firewalls automatically allow this). |

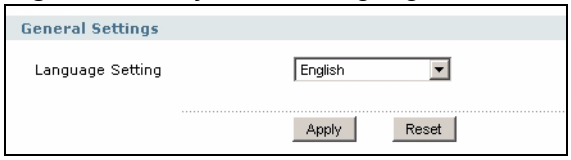
**Table 254** System > Vantage CNM (continued)

| LABEL | DESCRIPTION |
|---|---|
| Transfer Protocol | Select whether the Vantage CNM sessions should use regular HTTP connections or secure HTTPS connections.<br><br>Note: HTTPS is recommended.<br><br>The Vantage CNM server must use the same setting. |
| Device Management IP | Select **Auto** to have the ZyWALL allow Vantage CNM sessions to connect to any of the ZyWALL's IP addresses.<br><br>Select **Custom** to specify the ZyWALL's IP address that allows Vantage CNM sessions. Configure the **Custom IP** field if you select this. You might for example need to specify the IP address when using a WAN trunk that uses multiple WAN IP addresses. |
| Custom IP | Specify the ZyWALL's IP address that allows Vantage CNM sessions. This field applies when you select **Custom** in the **Device Management IP** field. |
| Keepalive Interval | Set how often the ZyWALL sends a keep alive packet to the Vantage CNM server if there is no other traffic. The keep alive packets maintain the Vantage CNM server's control session. |
| Periodic Inform Interval | Select this option to have the ZyWALL periodically send "Inform" messages to the Vantage CNM server. |
| HTTPS Authentication | When you are using HTTPs, select this option to have the ZyWALL authenticate the Vantage CNM server's certificate. In order to do this you need to import the Vantage CNM server's public key (certificate) into the ZyWALL's trusted certificates. |
| Vantage Certificate | Select the Vantage CNM server's certificate. This applies when you enable HTTPS authentication. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# 45.13 Language Screen

Click **System > Language** to open the following screen. Use this screen to select a display language for the ZyWALL's Web Configurator screens.

**Figure 534** System > Language



The following table describes the labels in this screen.

**Table 255** System > Language

| LABEL | DESCRIPTION |
|---|---|
| Language Setting | Select a display language for the ZyWALL's Web Configurator screens. You also need to open a new browser session to display the screens in the new language. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# PART X
# Maintenance, Troubleshooting, & Specifications

# 46

# File Manager

## 46.1 Overview

Configuration files define the ZyWALL's settings. Shell scripts are files of commands that you can store on the ZyWALL and run when you need them. You can apply a configuration file or run a shell script without the ZyWALL restarting. You can store multiple configuration files and shell script files on the ZyWALL. You can edit configuration files or shell scripts in a text editor and upload them to the ZyWALL. Configuration files use a .conf extension and shell scripts use a .zysh extension.

### 46.1.1 What You Can Do in the File Manager Screens

- Use the **Configuration File** screen (see Section 46.2 on page 784) to store and name configuration files. You can also download configuration files from the ZyWALL to your computer and upload configuration files from your computer to the ZyWALL.
- Use the **Firmware Package** screen (see Section 46.3 on page 788) to check your current firmware version and upload firmware to the ZyWALL.
- Use the **Shell Script** screen (see Section 46.4 on page 790) to store, name, download, upload and run shell script files.

### 46.1.2 What you Need to Know About the File Manager

#### Configuration Files and Shell Scripts

When you apply a configuration file, the ZyWALL uses the factory default settings for any features that the configuration file does not include. When you run a shell script, the ZyWALL only applies the commands that it contains. Other settings do not change.

These files have the same syntax, which is also identical to the way you run CLI commands manually. An example is shown below.

**Figure 535** Configuration File / Shell Script: Example

```
# enter configuration mode
configure terminal
# change administrator password
username admin password 4321 user-type admin
# configure ge3
interface ge3
ip address 172.23.37.240 255.255.255.0
ip gateway 172.23.37.254 metric 1
exit
# create address objects for remote management / to-ZyWALL firewall rules
# use the address group in case we want to open up remote management later
address-object TW_SUBNET 172.23.37.0/24
object-group address TW_TEAM
address-object TW_SUBNET
exit
# enable Telnet access (not enabled by default, unlike other services)
ip telnet server
# open WAN-to-ZyWALL firewall for TW_TEAM for remote management
firewall WAN ZyWALL insert 4
sourceip TW_TEAM
service TELNET
action allow
exit
write
```

While configuration files and shell scripts have the same syntax, the ZyWALL applies configuration files differently than it runs shell scripts. This is explained below.

**Table 256** Configuration Files and Shell Scripts in the ZyWALL

| Configuration Files (.conf) | Shell Scripts (.zysh) |
|---|---|
| • Resets to default configuration.<br>• Goes into CLI **Configuration** mode.<br>• Runs the commands in the configuration file. | • Goes into CLI **Privilege** mode.<br>• Runs the commands in the shell script. |

You have to run the example in Figure 535 on page 782 as a shell script because the first command is run in **Privilege** mode. If you remove the first command, you have to run the example as a configuration file because the rest of the commands are executed in **Configuration** mode.

## Comments in Configuration Files or Shell Scripts

In a configuration file or shell script, use "#" or "!" as the first character of a command line to have the ZyWALL treat the line as a comment.

Your configuration files or shell scripts can use “exit” or a command line consisting of a single “!” to have the ZyWALL exit sub command mode.

Note: “exit” or “!”' must follow sub commands if it is to make the ZyWALL exit sub command mode.

Line 3 in the following example exits sub command mode.

```
interface ge1
ip address dhcp
!
```

Lines 1 and 3 in the following example are comments and line 4 exits sub command mode.

```
!
interface ge1
# this interface is a DHCP client
!
```

Lines 1 and 2 are comments. Line 5 exits sub command mode.

```
! this is from Joe
# on 2008/04/05
interface ge1
ip address dhcp
!
```

### Errors in Configuration Files or Shell Scripts

When you apply a configuration file or run a shell script, the ZyWALL processes the file line-by-line. The ZyWALL checks the first line and applies the line if no errors are detected. Then it continues with the next line. If the ZyWALL finds an error, it stops applying the configuration file or shell script and generates a log.

You can change the way a configuration file or shell script is applied. Include `setenv stop-on-error off` in the configuration file or shell script. The ZyWALL ignores any errors in the configuration file or shell script and applies all of the valid commands. The ZyWALL still generates a log for any errors.

# 46.2 The Configuration File Screen

Click **Maintenance > File Manager > Configuration File** to open the **Configuration File** screen. Use the **Configuration File** screen to store, run, and name configuration files. You can also download configuration files from the ZyWALL to your computer and upload configuration files from your computer to the ZyWALL.

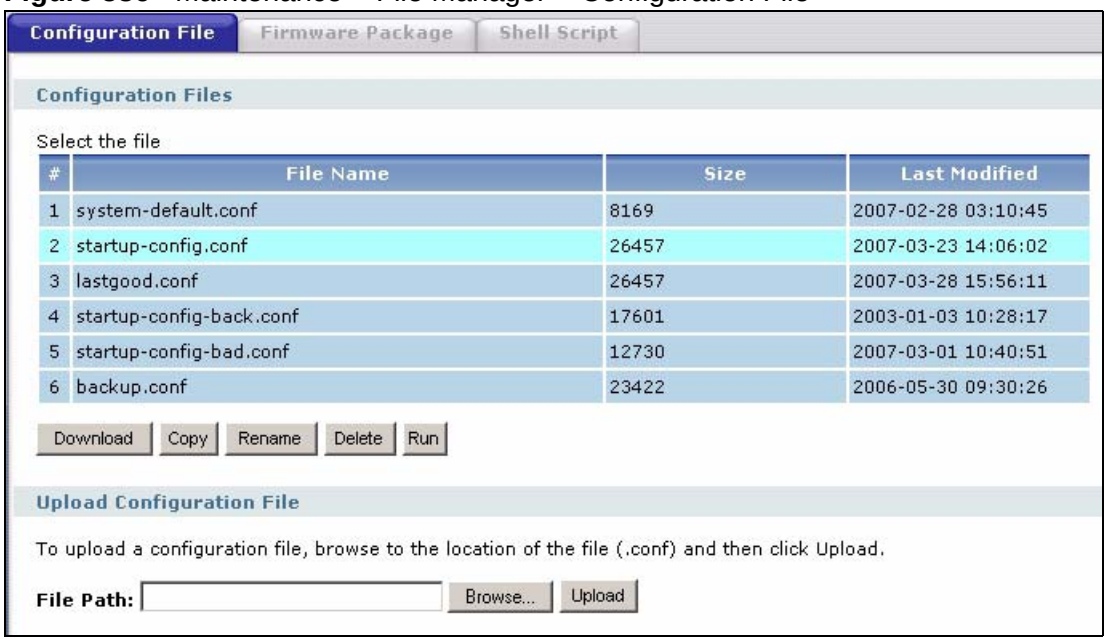
Once your ZyWALL is configured and functioning properly, it is highly recommended that you back up your configuration file before making further configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

### Configuration File Flow at Restart

- If there is not a **startup-config.conf** when you restart the ZyWALL (whether through a management interface or by physically turning the power off and back on), the ZyWALL uses the **system-default.conf** configuration file with the ZyWALL's default settings.
- If there is a **startup-config.conf**, the ZyWALL checks it for errors and applies it. If there are no errors, the ZyWALL uses it and copies it to the **lastgood.conf** configuration file as a back up file. If there is an error, the ZyWALL generates a log and copies the **startup-config.conf** configuration file to the **startup-config-bad.conf** configuration file and tries the existing **lastgood.conf** configuration file. If there isn't a **lastgood.conf** configuration file or it also has an error, the ZyWALL applies the **system-default.conf** configuration file.

- You can change the way the **startup-config.conf** file is applied. Include the `setenv-startup stop-on-error off` command. The ZyWALL ignores any errors in the **startup-config.conf** file and applies all of the valid commands. The ZyWALL still generates a log for any errors.

**Figure 536** Maintenance > File Manager > Configuration File




**Do not turn off the ZyWALL while configuration file upload is in progress.**

The following table describes the labels in this screen.

**Table 257** Maintenance > File Manager > Configuration File

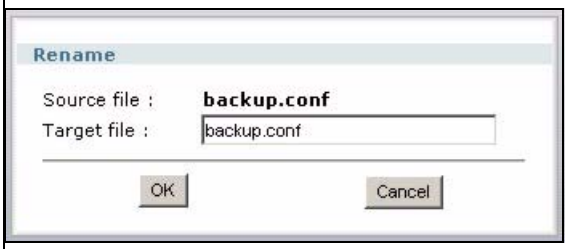
| LABEL | DESCRIPTION |
|---|---|
| Download | Click a configuration file's row to select it and click **Download** to save the configuration to your computer. |
| Copy | Use this button to save a duplicate of a configuration file on the ZyWALL.<br>Click a configuration file's row to select it and click **Copy** to open the **Copy File** screen.<br>**Figure 537** Maintenance > File Manager > Configuration File > Copy<br>  <br>Specify a name for the duplicate configuration file. Use up to 25 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-).<br>Click **OK** to save the duplicate or click **Cancel** to close the screen without saving a duplicate of the configuration file. |
| Rename | Use this button to change the label of a configuration file on the ZyWALL. You can only rename manually saved configuration files. You cannot rename the **lastgood.conf**, **system-default.conf** and **startup-config.conf** files.<br>You cannot rename a configuration file to the name of another configuration file in the ZyWALL.<br>Click a configuration file's row to select it and click **Rename** to open the **Rename File** screen.<br>**Figure 538** Maintenance > File Manager > Configuration File > Rename<br>  <br>Specify the new name for the configuration file. Use up to 25 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-).<br>Click **OK** to save the duplicate or click **Cancel** to close the screen without saving a duplicate of the configuration file. |

**Table 257** Maintenance > File Manager > Configuration File (continued)

| LABEL | DESCRIPTION |
|---|---|
| Delete | Click a configuration file's row to select it and click **Delete** to remove the configuration file from the ZyWALL. You can only delete manually saved configuration files. You cannot delete the **system-default.conf**, **startup-config.conf** and **lastgood.conf** files.<br><br>A pop-up window asks you to confirm that you want to delete the configuration file. Click **OK** to delete the configuration file or click **Cancel** to close the screen without deleting the configuration file. |
| Run | Use this button to have the ZyWALL use a specific configuration file.<br><br>Click a configuration file's row to select it and click **Run** to have the ZyWALL use that configuration file. The ZyWALL does not have to restart in order to use a different configuration file, although you will need to wait for a few minutes while the system reconfigures. |
| # | This column displays the number for each configuration file entry. The total number of configuration files that you can save depends on the sizes of the configuration files and the available flash storage space. |
| File Name | This column displays the label that identifies a configuration file.<br><br>You cannot delete the following configuration files or change their file names.<br><br>The **system-default.conf** file contains the ZyWALL's default settings. Select this file and click **Apply** to reset all of the ZyWALL settings to the factory defaults. This configuration file is included when you upload a firmware package.<br><br>The **startup-config.conf** file is the configuration file that the ZyWALL is currently using. If you make and save changes during your management session, the changes are applied to this configuration file. The ZyWALL applies configuration changes made in the Web Configurator to the configuration file when you click **Apply** or **OK**. It applies configuration changes made via commands when you use the `write` command.<br><br>The **lastgood.conf** is the most recently used (valid) configuration file that was saved when the device last restarted. If you upload and apply a configuration file with an error, you can apply lastgood.conf to return to a valid configuration. |
| Size | This column displays the size (in KB) of a configuration file. |
| Last Modified | This column displays the date and time that the individual configuration files were last changed or saved. |
| Upload Configuration File | The bottom part of the screen allows you to upload a new or previously saved configuration file from your computer to your ZyWALL<br><br>You cannot upload a configuration file named **system-default.conf** or **lastgood.conf**.<br><br>If you upload **startup-config.conf**, it will replace the current configuration and immediately apply the new settings. |
| File Path | Type in the location of the file you want to upload in this field or click **Browse ...** to find it. |

**Table 257** Maintenance > File Manager > Configuration File (continued)

| LABEL | DESCRIPTION |
|---|---|
| Browse... | Click **Browse...** to find the .conf file you want to upload. The configuration file must use a ".conf" filename extension. You will receive an error message if you try to upload a fie of a different format. Remember that you must decompress compressed (.zip) files before you can upload them. |
| Upload | Click **Upload** to begin the upload process. This process may take up to two minutes. |

# 46.3 The Firmware Package Screen

Click **Maintenance > File Manager > Firmware Package** to open the **Firmware Package** screen. Use the **Firmware Package** screen to check your current firmware version and upload firmware to the ZyWALL.

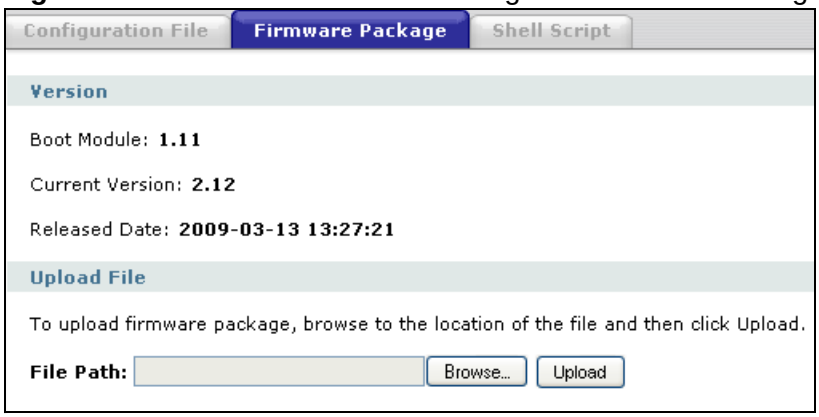
Note: The Web Configurator is the recommended method for uploading firmware. You only need to use the command line interface if you need to recover the firmware. See the CLI Reference Guide for how to determine if you need to recover the firmware and how to recover it.

Find the firmware package at www.zyxel.com in a file that (usually) uses the system model name with a .bin extension, for example, "zywall.bin".

The ZyWALL's firmware package cannot go through the ZyWALL when you enable the anti-virus **Destroy compressed files that could not be decompressed** option. The ZyWALL classifies the firmware package as not being able to be decompressed and deletes it. You can upload the firmware package to the ZyWALL with the option enabled, so you only need to clear the **Destroy compressed files that could not be decompressed** option while you download the firmware package. See Section 30.2.1 on page 511 for more on the anti-virus **Destroy compressed files that could not be decompressed** option.

**The firmware update can take up to five minutes. Do not turn off or reset the ZyWALL while the firmware update is in progress!**

**Figure 539** Maintenance > File Manager > Firmware Package



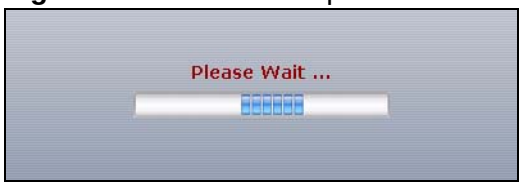

The following table describes the labels in this screen.

**Table 258** Maintenance > File Manager > Firmware Package

| LABEL | DESCRIPTION |
|---|---|
| Boot Module | This is the version of the boot module that is currently on the ZyWALL. |
| Current Version | This is the firmware version and the date created. |
| Released Date | This is the date that the version of the firmware was created. |
| File Path | Type in the location of the file you want to upload in this field or click **Browse ...** to find it. |
| Browse... | Click **Browse...** to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them. |
| Upload | Click **Upload** to begin the upload process. This process may take up to two minutes. |

After you see the **Firmware Upload in Process** screen, wait two minutes before logging into the ZyWALL again.

**Figure 540** Firmware Upload In Process




Note: The ZyWALL automatically reboots after a successful upload.

The ZyWALL automatically restarts causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

**Figure 541** Network Temporarily Disconnected


After five minutes, log in again and check your new firmware version in the **HOME** screen.

If the upload was not successful, the following message appears in the status bar at the bottom of the screen.

**Figure 542** Firmware Upload Error

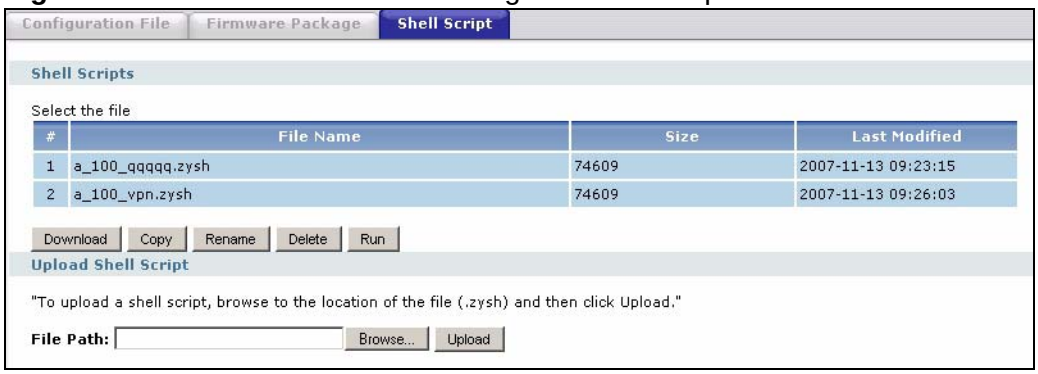

# 46.4 The Shell Script Screen

Use shell script files to have the ZyWALL use commands that you specify. Use a text editor to create the shell script files. They must use a ".zysh" filename extension.

Click **Maintenance > File Manager > Shell Script** to open the **Shell Script** screen. Use the **Shell Script** screen to store, name, download, upload and run shell script files. You can store multiple shell script files on the ZyWALL at the same time.

Note: You should include `write` commands in your scripts. If you do not use the `write` command, the changes will be lost when the ZyWALL restarts. You could use multiple `write` commands in a long script.

**Figure 543** Maintenance > File Manager > Shell Script



Each field is described in the following table.

**Table 259** Maintenance > File Manager > Shell Script

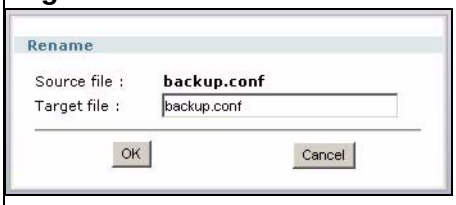
| LABEL | DESCRIPTION |
|---|---|
| Download | Click a shell script file's row to select it and click **Download** to save the configuration to your computer. |
| Copy | Use this button to save a duplicate of a shell script file on the ZyWALL.<br><br>Click a shell script file's row to select it and click **Copy** to open the **Copy File** screen.<br><br>**Figure 544** Maintenance > File Manager > Shell Script > Copy<br>  <br><br><br>Specify a name for the duplicate file. Use up to 25 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-).<br><br>Click **OK** to save the duplicate or click **Cancel** to close the screen without saving a duplicate of the configuration file. |
| Rename | Use this button to change the label of a shell script file on the ZyWALL.<br><br>You cannot rename a shell script to the name of another shell script in the ZyWALL.<br><br>Click a shell script's row to select it and click **Rename** to open the **Rename File** screen.<br><br>**Figure 545** Maintenance > File Manager > Shell Script > Rename<br>  <br><br><br>Specify the new name for the shell script file. Use up to 25 characters (including a-zA-Z0-9;'~!@#$%^&()_+[]{}',.=-).<br><br>Click **OK** to save the duplicate or click **Cancel** to close the screen without saving a duplicate of the configuration file. |
| Delete | Click a shell script file's row to select it and click **Delete** to delete the shell script file from the ZyWALL.<br><br>A pop-up window asks you to confirm that you want to delete the shell script file. Click **OK** to delete the shell script file or click **Cancel** to close the screen without deleting the shell script file. |
| Run | Use this button to have the ZyWALL use a specific shell script file.<br><br>Click a shell script file's row to select it and click **Run** to have the ZyWALL use that shell script file. You may need to wait awhile for the ZyWALL to finish applying the commands. |
| # | This column displays the number for each shell script file entry. |

**Table 259** Maintenance > File Manager > Shell Script (continued)

| LABEL | DESCRIPTION |
|---|---|
| File Name | This column displays the label that identifies a shell script file. |
| Size | This column displays the size (in KB) of a shell script file. |
| Last Modified | This column displays the date and time that the individual shell script files were last changed or saved. |
| Upload Shell Script | The bottom part of the screen allows you to upload a new or previously saved shell script file from your computer to your ZyWALL. |
| File Path | Type in the location of the file you want to upload in this field or click **Browse ...** to find it. |
| Browse... | Click **Browse...** to find the .zysh file you want to upload. |
| Upload | Click **Upload** to begin the upload process. This process may take up to several minutes. |

# 47

# Logs

## 47.1 Overview

This chapter provides general information about the ZyWALL's log feature.

Note: When a log reaches the maximum number of log messages, new log messages automatically overwrite existing log messages, starting with the oldest existing log message first.

- For individual log descriptions, see Appendix A on page 845.
- For the maximum number of log messages in the ZyWALL, see Chapter 52 on page 835.

## 47.2 What You Can Do In The Log Screens

- Use the **Maintenance** > **View Log** screen (Section 47.3 on page 793) to view current log messages. You can change the way the log is displayed, you can e-mail the log, and you can also clear the log in this screen.
- Use the **Maintenance** > **Log Settings** screen (Section 47.4 on page 796) to specify which log messages are e-mailed, where they are e-mailed, and how often they are e-mailed.

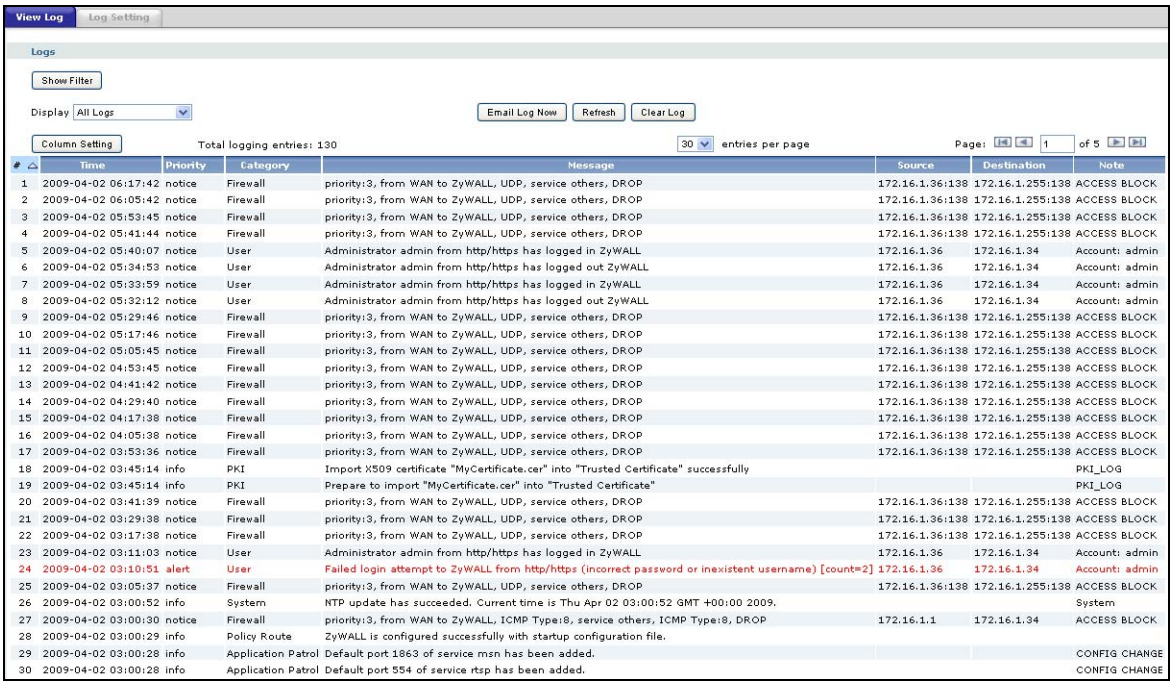
## 47.3 View Log Screen

Log messages are stored in two separate logs, one for regular log messages and one for debugging messages. In the regular log, you can look at all the log messages by selecting **All Logs**, or you can select a specific category of log messages (for example, firewall or user). You can also look at the debugging log by selecting **Debug Log**. All debugging messages have the same priority.

To access this screen, click **Maintenance** > **View Log**. The log is displayed in the following screen.

Events that generate an alert (as well as a log message) display in red. Regular logs display in black. Click a column's heading cell to sort the table entries by that column's criteria. Click the heading cell again to reverse the sort order.

**Figure 546** Maintenance > Log > View Log




The following table describes the labels in this screen.

**Table 260** Maintenance > Log > View Log

| LABEL | DESCRIPTION |
|---|---|
| Show Filter / Hide Filter | Click this button to show or hide the filter settings.<br><br>If the filter settings are hidden, the **Display**, **Email Log Now**, **Refresh**, and **Clear Log** fields are available.<br><br>If the filter settings are shown, the **Display**, **Priority**, **Source Address**, **Destination Address**, **Service**, **Keyword**, and **Search** fields are available. |
| Display | Select the log category you want to view. |
| (Filter Hidden) | These fields and buttons display when you hide the filter. |
| Email Log Now | Click this button to send log message(s) to the **Active** e-mail address(es) specified in the **Send Log To** field on the **Log Settings** page. (See Section 47.4.1 on page 797 or Section 47.4.2 on page 798 for more information about these fields.) |
| Refresh | Click this button to update the information on the log screen. |
| Clear Log | Click this button to clear the whole log, regardless of what is currently displayed on the screen. |
| Display | Select the log message(s) you want to view. You can also view **All Logs** at one time, or you can view the **Debug Log**. |

**Table 260** Maintenance > Log > View Log (continued)

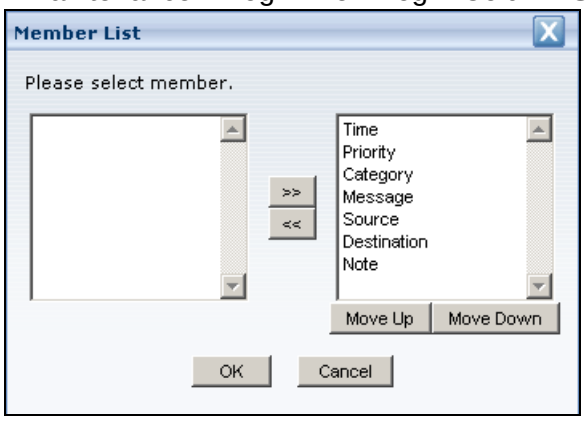
| LABEL | DESCRIPTION |
|---|---|
| Priority | Select the priority of log messages to display. The log displays the log messages with this priority or higher. Choices are: **any**, **emerg**, **alert**, **crit**, **error**, **warn**, **notice**, and **info**, from highest priority to lowest priority. This field is read-only if the **Category** is **Debug Log**. |
| Source Address | Type the source IP address of the incoming packet that generated the log message. Do not include the port in this filter. |
| Destination Address | Type the IP address of the destination of the incoming packet when the log message was generated. Do not include the port in this filter. |
| Service | Select the service whose log messages you would like to see. The Web Configurator uses the protocol and destination port number(s) of the service to select which log messages you see. |
| Keyword | Type a keyword to look for in the **Message**, **Source**, **Destination** and **Note** fields. If a match is found in any field, the log message is displayed. You can use up to 63 alphanumeric characters and the underscore, as well as punctuation marks ()' ,.:;?! +-*/= #$% @ ; the period, double quotes, and brackets are not allowed. |
| Search | Click this button to update the log using the current filter settings. |
| Column Setting | Click this icon to open a screen where you can configure how the columns in the log table display.<br><br>Select the titles of any columns you don't want to display and use the left-arrow button to move them to the left column to hide them. Select titles and use the **Move Up** and **Move Down** buttons to arrange their display sequence.<br><br>**Figure 547** Maintenance > Log > View Log > Column Setting<br>  |
| Total Logging Entries | This is the number of logs recorded in the ZyWALL. |
| entries per page | Select the number of log messages you would like to see on one screen. Choices are: **30**, **50**, and **80**. |
| Page x of x | This is the currently displayed log entries' page number and the total number of pages. Type a page number to go to or use the arrows to navigate to the pages of entries. |
| # | This field is a sequential value, and it is not associated with a specific log message. |

**Table 260** Maintenance > Log > View Log (continued)

| LABEL | DESCRIPTION |
|---|---|
| Time | This field displays the time the log message was recorded. |
| Priority | This field displays the priority of the log message. It has the same range of values as the **Priority** field above. |
| Category | This field displays the log that generated the log message. It is the same value used in the **Display** and (other) **Category** fields. |
| Message | This field displays the reason the log message was generated. The text "[count=*x*]", where *x* is a number, appears at the end of the **Message** field if log consolidation is turned on (see **Log Consolidation** in Table 262 on page 800) and multiple entries were aggregated to generate into this one. |
| Source | This field displays the source IP address and the port number in the event that generated the log message. |
| Destination | This field displays the destination IP address and the port number of the event that generated the log message. |
| Note | This field displays any additional information about the log message. |

The Web Configurator saves the filter settings if you leave the **View Log** screen and return to it later.

# 47.4 Log Setting Screens

The **Log Setting** screens control log messages and alerts. A log message stores the information for viewing (for example, in the **View Log** tab) or regular e-mailing later, and an alert is e-mailed immediately. Usually, alerts are used for events that require more serious attention, such as system errors and attacks.

The ZyWALL provides a system log and supports e-mail profiles and remote syslog servers. The system log is available on the **View Log** tab, the e-mail profiles are used to mail log messages to the specified destinations, and the other four logs are stored on specified syslog servers.

The **Log Setting** tab also controls what information is saved in each log. For the system log, you can also specify which log messages are e-mailed, where they are e-mailed, and how often they are e-mailed.

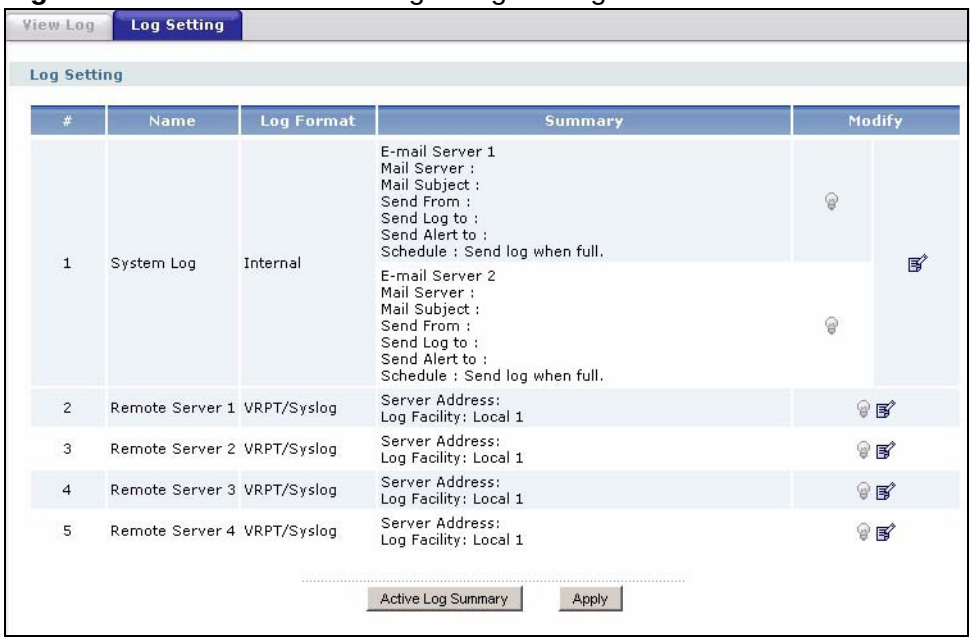
For alerts, the **Log Settings** tab controls which events generate alerts and where alerts are e-mailed.

The **Log Settings Summary** screen provides a summary of all the settings. You can use the **Log Settings Edit** screen to maintain the detailed settings (such as log categories, e-mail addresses, server names, etc.) for any log. Alternatively, if you want to edit what events is included in each log, you can also use the **Active Log Summary** screen to edit this information for all logs at the same time.

## 47.4.1 Log Setting Summary

To access this screen, click **Maintenance** > **Log** > **Log Setting**.

**Figure 548** Maintenance > Log > Log Setting




The following table describes the labels in this screen.

**Table 261** Maintenance > Log > Log Setting

| LABEL | DESCRIPTION |
|---|---|
| # | This field is a sequential value, and it is not associated with a specific log. |
| Name | This field displays the name of the log (system log or one of the remote servers). |
| Log Format | This field displays the format of the log.<br>**Internal** - system log; you can view the log on the **View Log** tab.<br>**VRPT/Syslog** - ZyXEL's Vantage Report, syslog-compatible format.<br>**CEF/Syslog** - Common Event Format, syslog-compatible format. |
| Summary | This field is a summary of the settings for each log. Please see Section 47.4.2 on page 798 for more information. |
| Modify | This column provides icons to activate or deactivate logs and to modify the settings.<br>To activate or deactivate a log, click the **Active** icon. Make sure you click **Apply** to save and apply the change.<br>To edit the settings, click the **Edit** icon next to the associated log. The **Log Settings Edit** screen appears. |

**Table 261** Maintenance > Log > Log Setting (continued)

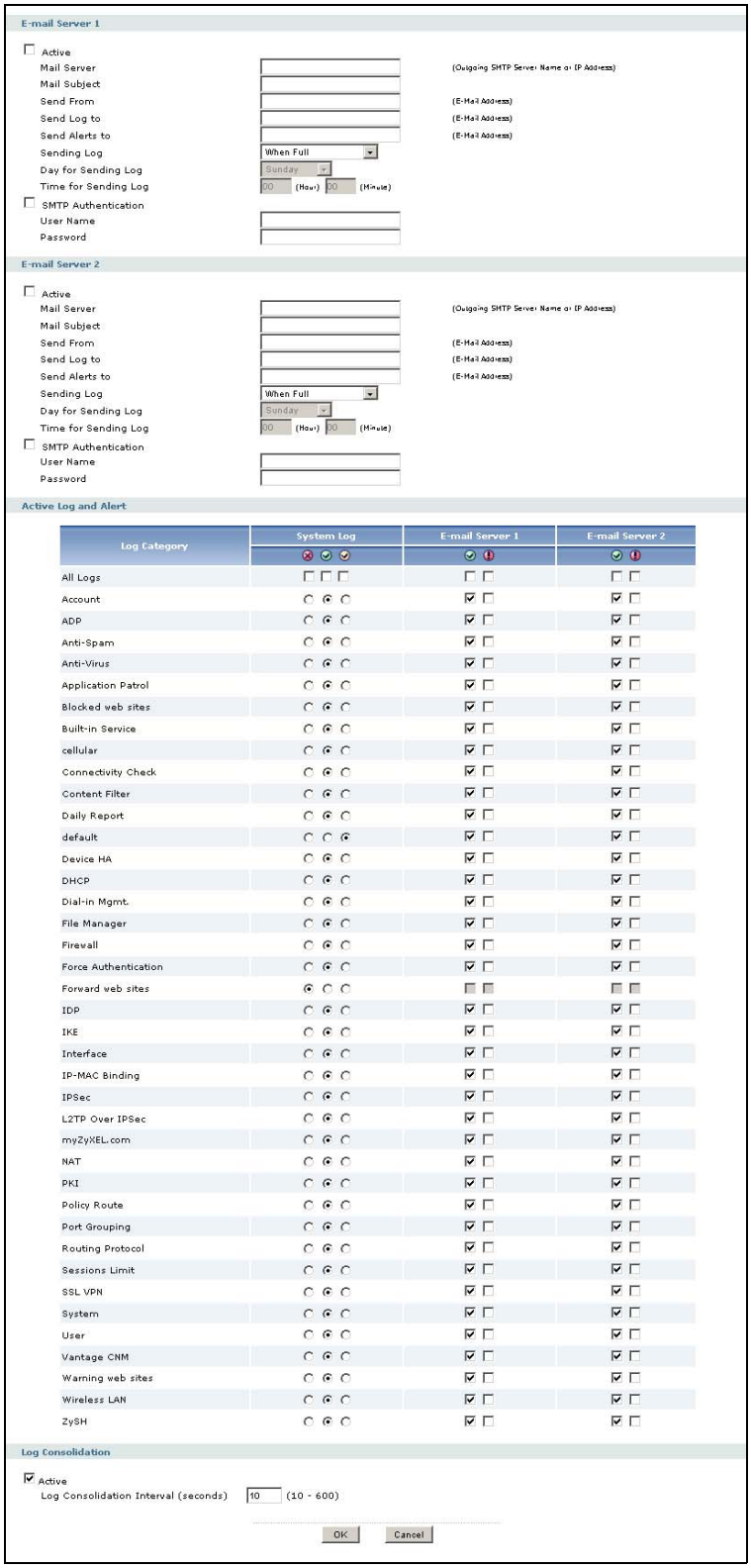
| LABEL | DESCRIPTION |
|---|---|
| Active Log Summary | Click this button to open the **Active Log Summary Edit** screen. |
| Apply | Click this button to save your changes (activate and deactivate logs) and make them take effect. |

## 47.4.2 Edit System Log Settings

The **Log Settings Edit** screen controls the detailed settings for each log in the system log (which includes the e-mail profiles). Go to the **Log Settings**

**Summary** screen (see Section 47.4.1 on page 797), and click the system log **Edit** icon.

**Figure 549** Maintenance > Log > Log Setting > Edit (System Log)



The following table describes the labels in this screen.

**Table 262** Maintenance > Log > Log Setting > Edit (System Log)

| LABEL | DESCRIPTION |
|---|---|
| E-Mail Server 1/2 | |
| Active | Select this to send log messages and alerts according to the information in this section. You specify what kinds of log messages are included in log information and what kinds of log messages are included in alerts in the **Active Log and Alert** section. |
| Mail Server | Type the name or IP address of the outgoing SMTP server. |
| Mail Subject | Type the subject line for the outgoing e-mail. |
| Send From | Type the e-mail address from which the outgoing e-mail is delivered. This address is used in replies. |
| Send Log To | Type the e-mail address to which the outgoing e-mail is delivered. |
| Send Alerts To | Type the e-mail address to which alerts are delivered. |
| Sending Log | Select how often log information is e-mailed. Choices are: **When Full**, **Hourly and When Full**, **Daily and When Full**, and **Weekly and When Full**. |
| Day for Sending Log | This field is available if the log is e-mailed weekly. Select the day of the week the log is e-mailed. |
| Time for Sending Log | This field is available if the log is e-mailed weekly or daily. Select the time of day (hours and minutes) when the log is e-mailed. Use 24-hour notation. |
| SMTP Authentication | Select this check box if it is necessary to provide a user name and password to the SMTP server. |
| User Name | This box is effective when you select the **SMTP Authentication** check box. Type the user name to provide to the SMTP server when the log is e-mailed. |
| Password | This box is effective when you select the **SMTP Authentication** check box. Type the password to provide to the SMTP server when the log is e-mailed. |
| Active Log and Alert | |
| Log Category | This field displays each category of messages. It is the same value used in the **Display** and **Category** fields in the **View Log** tab. The **Default** category includes debugging messages generated by open source software. |

**Table 262** Maintenance > Log > Log Setting > Edit (System Log) (continued)

| LABEL | DESCRIPTION |
|---|---|
| System log | Select which events you want to log by **Log Category** (except **All Logs**; see below). There are three choices:<br><br>**disable all logs** (red X) - do not log any information from this category<br><br>**enable normal logs** (green checkmark) - create log messages and alerts from this category<br><br>**enable normal logs and debug logs** (yellow checkmark) - create log messages, alerts, and debugging information from this category; the ZyWALL does not e-mail debugging information, however, even if this setting is selected.<br><br>If you select one of the check boxes for **All Logs**, it affects the settings for every category. |
| E-mail Server 1 | Select whether this category of events should be included in the log messages when it is e-mailed (green checkmark) and/or in alerts (yellow exclamation point) for the e-mail settings specified in **E-Mail Server 1**. The ZyWALL does not e-mail debugging information, even if it is recorded in the **System log**. |
| E-mail Server 2 | Select whether this category of events should be included in log messages when it is e-mailed (green checkmark) and/or in alerts (yellow exclamation point) for the e-mail settings specified in **E-Mail Server 2**. The ZyWALL does not e-mail debugging information, even if it is recorded in the **System log**. |
| Log Consolidation | |
| Active | Select this to activate log consolidation. Log consolidation aggregates multiple log messages that arrive within the specified **Log Consolidation Interval**. In the **View Log** tab, the text "[count=*x*]", where *x* is the number of original log messages, is appended at the end of the **Message** field, when multiple log messages were aggregated. |
| Log Consolidation Interval | Type how often, in seconds, to consolidate log information. If the same log message appears multiple times, it is aggregated into one log message with the text "[count=*x*]", where *x* is the number of original log messages, appended at the end of the **Message** field. |
| OK | Click this to save your changes and return to the previous screen. |
| Cancel | Click this to return to the previous screen without saving your changes. |

## 47.4.3 Edit Remote Server Log Settings

The **Log Settings Edit** screen controls the detailed settings for each log in the remote server (syslog). Go to the **Log Settings Summary** screen (see Section 47.4.1 on page 797), and click a remote server **Edit** icon.

**Figure 550** Maintenance > Log > Log Setting > Edit (Remote Server)

The following table describes the labels in this screen.

**Table 263** Maintenance > Log > Log Setting > Edit (Remote Server)

| LABEL | DESCRIPTION |
|---|---|
| Log Settings for Remote Server 1 | |
| Active | Select this check box to send log information according to the information in this section. You specify what kinds of messages are included in log information in the **Active Log** section. |
| Log Format | This field displays the format of the log information. It is read-only.<br>**VRPT/Syslog** - ZyXEL's Vantage Report, syslog-compatible format.<br>**CEF/Syslog** - Common Event Format, syslog-compatible format. |
| Server Address | Type the server name or the IP address of the syslog server to which to send log information. |
| Log Facility | Select a log facility. The log facility allows you to log the messages to different files in the syslog server. Please see the documentation for your syslog program for more information. |
| Active Log | |
| Log Category | This field displays each category of messages. It is the same value used in the **Display** and **Category** fields in the **View Log** tab. The **Default** category includes debugging messages generated by open source software. |
| Selection | Select what information you want to log from each **Log Category** (except **All Logs**; see below). Choices are:<br>**disable all logs** (red X) - do not log any information from this category<br>**enable normal logs** (green checkmark) - log regular information and alerts from this category<br>**enable normal logs and debug logs** (yellow checkmark) - log regular information, alerts, and debugging information from this category<br>If you check one of the check boxes for **All Logs**, it affects the settings for every category. |
| OK | Click this to save your changes and return to the previous screen. |
| Cancel | Click this to return to the previous screen without saving your changes. |

## 47.4.4 Active Log Summary Screen

The **Active Log Summary** screen allows you to view and to edit what information is included in the system log, e-mail profiles, and remote servers at the same time. It does not let you change other log settings (for example, where and how often log information is e-mailed or remote server names).To access this screen,

go to the **Log Settings Summary** screen (see Section 47.4.1 on page 797), and click the **Active Log Summary** button.

**Figure 551** Active Log Summary


This screen provides a different view and a different way of indicating which messages are included in each log and each alert. Please see Section 47.4.2 on page 798, where this process is discussed. (The **Default** category includes debugging messages generated by open source software.)

The following table describes the fields in this screen.

**Table 264** Maintenance > Log > Log Setting > Active Log Summary

| LABEL | DESCRIPTION |
|---|---|
| Active Log Summary | |
| Log Category | This field displays each category of messages. It is the same value used in the **Display** and **Category** fields in the **View Log** tab. The **Default** category includes debugging messages generated by open source software. |
| Selection | Select what information you want to log from each **Log Category** (except **All Logs**; see below). Choices are:<br>**disable all logs** (red X) - do not log any information from this category<br>**enable normal logs** (green checkmark) - log regular information and alerts from this category<br>**enable all logs** (yellow checkmark) - log regular information, alerts, and debugging information from this category<br>If you check one of the check boxes for **All Logs**, it affects the settings for every category. |
| OK | Click this to save your changes and return to the previous screen. |
| Cancel | Click this to return to the previous screen without saving your changes. |

# 48

# Reports

## 48.1 Overview

This chapter provides information about the report screens. Use the **Report** screens to start or stop data collection and view various statistics about traffic passing through your ZyWALL.

Note: Data collection may decrease the ZyWALL's traffic throughput rate.

### 48.1.1 What You Can Do in the Report Screens

- Use the **Traffic Statistics** screen (see Section 48.2 on page 807) to start or stop data collection and view statistics.
- Use the **Session** screen (see Section 48.3 on page 810) to view sessions by user or service.
- Use the **Anti-Virus** screen (see Section 48.4 on page 813) to start or stop data collection and view virus statistics.
- Use the **IDP** screen (Section 48.5 on page 815) to start or stop data collection and view IDP statistics.
- Use the **Content Filter** screen (Section 48.6 on page 817) to start or stop data collection and view content filter statistics.
- Use the **Anti-Spam** screen (Section 48.7 on page 819) to start or stop data collection and view spam statistics.
- Use the **Email Daily Report** screen (Section 48.8 on page 822) to configure where and how to send daily reports and what reports to send.

## 48.2 The Traffic Statistics Screen

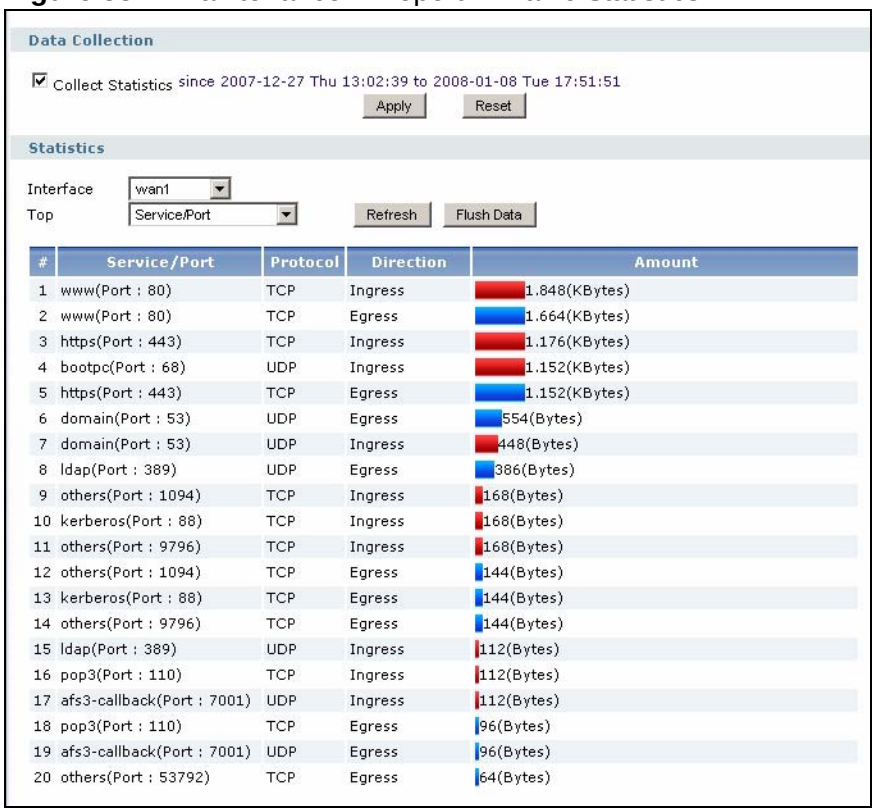
Click **Maintenance > Report > Traffic Statistics** to display the **Traffic Statistics** screen. This screen provides basic information about the following for example:

- Most-visited Web sites and the number of times each one was visited. This count may not be accurate in some cases because the ZyWALL counts HTTP GET packets. Please see Table 265 on page 808 for more information.

- Most-used protocols or service ports and the amount of traffic on each one
- LAN IP with heaviest traffic and how much traffic has been sent to and from each one

You use the **Traffic Statistics** screen to tell the ZyWALL when to start and when to stop collecting information for these reports. You cannot schedule data collection; you have to start and stop it manually in the **Traffic Statistics** screen.

**Figure 552** Maintenance > Report > Traffic Statistics




There is a limit on the number of records shown in the report. Please see Table 266 on page 810 for more information. The following table describes the labels in this screen.

**Table 265** Maintenance > Report > Traffic Statistics

| LABEL | DESCRIPTION |
|---|---|
| Data Collection | |
| Collect Statistics | Select this to have the ZyWALL collect data for the report. If the ZyWALL has already been collecting data, the collection period displays to the right. The progress is not tracked here real-time, but you can click the **Refresh** button to update it. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |
| Statistics | |

**Table 265** Maintenance > Report > Traffic Statistics (continued)

| LABEL | DESCRIPTION |
|---|---|
| Interface | Select the interface from which to collect information. You can collect information from Ethernet, VLAN, bridge, PPPoE/PPTP, and auxiliary interfaces. |
| Traffic Type | Select the type of report to display. Choices are:<br>**Host IP Address/User** - displays the IP addresses or users with the most traffic and how much traffic has been sent to and from each one.<br>**Service/Port** - displays the most-used protocols or service ports and the amount of traffic for each one.<br>**Web Site Hits** - displays the most-visited Web sites and how many times each one has been visited.<br>Each type of report has different information in the report (below). |
| Refresh | Click this button to update the report display. |
| Flush Data | Click this button to discard all of the screen's statistics and update the report display. |
| | These fields are available when the **Traffic Type** is **Host IP Address/User**. |
| # | This field is the rank of each record. The IP addresses and users are sorted by the amount of traffic. |
| IP Address/User | This field displays the IP address or user in this record. The maximum number of IP addresses or users in this report is indicated in Table 266 on page 810. |
| Direction | This field indicates whether the IP address or user is sending or receiving traffic. **Ingress**- traffic is coming from the IP address or user to the ZyWALL.<br>**Egress** - traffic is going from the ZyWALL to the IP address or user. |
| Amount | This field displays how much traffic was sent or received from the indicated IP address or user. If the **Direction** is **Ingress**, a red bar is displayed; if the **Direction** is **Egress**, a blue bar is displayed. The unit of measure is bytes, Kbytes, Mbytes or Gbytes, depending on the amount of traffic for the particular IP address or user. The count starts over at zero if the number of bytes passes the byte count limit. See Table 266 on page 810. |
| | These fields are available when the **Traffic Type** is **Service/Port**. |
| # | This field is the rank of each record. The protocols and service ports are sorted by the amount of traffic. |
| Service/Port | This field displays the service and port in this record. The maximum number of services and service ports in this report is indicated in Table 266 on page 810. |
| Protocol | This field indicates what protocol the service was using. |
| Direction | This field indicates whether the indicated protocol or service port is sending or receiving traffic.<br>**Incoming** - traffic is coming into the router through the interface<br>**Outgoing** - traffic is going out from the router through the interface |

**Table 265** Maintenance > Report > Traffic Statistics (continued)

| LABEL | DESCRIPTION |
|---|---|
| Amount | This field displays how much traffic was sent or received from the indicated service / port. If the **Direction** is **Ingress**, a red bar is displayed; if the **Direction** is **Egress**, a blue bar is displayed. The unit of measure is bytes, Kbytes, Mbytes, Gbytes, or Tbytes, depending on the amount of traffic for the particular protocol or service port. The count starts over at zero if the number of bytes passes the byte count limit. See Table 266 on page 810. |
| | These fields are available when the **Traffic Type** is **Web Site Hits**. |
| # | This field is the rank of each record. The domain names are sorted by the number of hits. |
| Web Site | This field displays the domain names most often visited. The ZyWALL counts each page viewed on a Web site as another hit. The maximum number of domain names in this report is indicated in Table 266 on page 810. |
| Hits | This field displays how many hits the Web site received. The ZyWALL counts hits by counting HTTP GET packets. Many Web sites have HTTP GET references to other Web sites, and the ZyWALL counts these as hits too. The count starts over at zero if the number of hits passes the hit count limit. See Table 266 on page 810. |

The following table displays the maximum number of records shown in the report, the byte count limit, and the hit count limit.

**Table 266** Maximum Values for Reports

| LABEL | DESCRIPTION |
|---|---|
| Maximum Number of Records | 20 |
| Byte Count Limit | $2^{64}$ bytes; this is just less than 17 million terabytes. |
| Hit Count Limit | $2^{64}$ hits; this is over $1.8 \times 10^{19}$ hits. |

# 48.3 The Session Monitor Screen

The **Session Monitor** screen displays information about active sessions for debugging or statistical analysis. It is not possible to manage sessions in this screen. The following information is displayed.

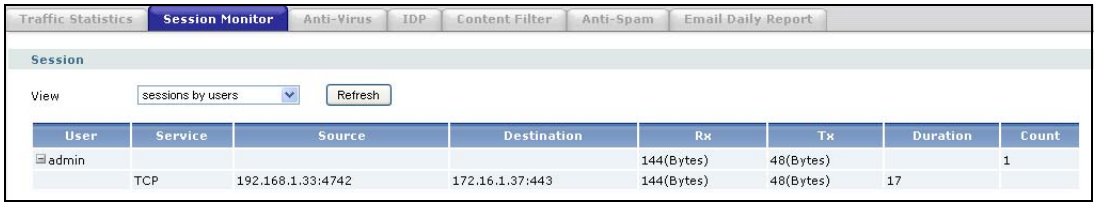
- User who started the session
- Protocol or service port used
- Source address
- Destination address
- Number of bytes received (so far)

- Number of bytes transmitted (so far)
- Duration (so far)

You can look at all the active sessions by user, service, source IP address, or destination IP address. You can also filter the information by user, protocol / service or service group, source address, and/or destination address and view it by user.

Click **Maintenance** > **Report** > **Session Monitor** to display the following screen.

**Figure 553** Maintenance > Report > Session Monitor




The following table describes the labels in this screen.

**Table 267** Maintenance > Report > Session Monitor

| LABEL | DESCRIPTION |
|---|---|
| View | Select how you want the information to be displayed. Choices are:<br>**sessions by users** - display all active sessions grouped by user<br>**sessions by services** - display all active sessions grouped by service or protocol<br>**sessions by source IP** - display all active sessions grouped by source IP address<br>**sessions by destination IP** - display all active sessions grouped by destination IP address<br>**all sessions** - filter the active sessions by the **User**, **Service**, **Source Address**, and **Destination Address**, and display each session individually (sorted by user). |
| Refresh | Click this button to update the information on the screen. The screen also refreshes automatically when you open and close the screen. |
| | The **User**, **Service**, **Source Address**, and **Destination Address** fields display if you view all sessions. Select your desired filter criteria and click the **Search** button to filter the list of sessions. |
| User | This field displays when **View** is set to **all sessions**. Type the user whose sessions you want to view. It is not possible to type part of the user name or use wildcards in this field; you must enter the whole user name. |
| Service | This field displays when **View** is set to **all sessions**. Select the service or service group whose sessions you want to view. The ZyWALL identifies the service by comparing the protocol and destination port of each packet to the protocol and port of each services that is defined. (See Chapter 39 on page 671 for more information about services.) |

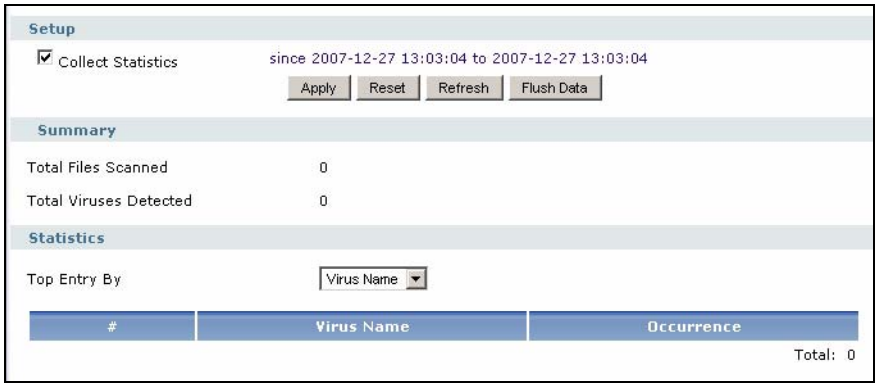
**Table 267** Maintenance > Report > Session Monitor (continued)

| LABEL | DESCRIPTION |
|---|---|
| Source Address | This field displays when **View** is set to **all sessions**. Type the source IP address whose sessions you want to view. You cannot include the source port. |
| Destination Address | This field displays when **View** is set to **all sessions**. Type the destination IP address whose sessions you want to view. You cannot include the destination port. |
| Search | This button displays when **View** is set to **all sessions**. Click this button to update the information on the screen using the filter criteria in the **User**, **Service**, **Source Address**, and **Destination Address** fields. |
| Active Sessions | This is the total number of active sessions that matched the search criteria. |
| sessions per page | Select the number of active sessions displayed on each page. You can use the arrow keys on the right to change pages. |
| User | This field displays the user in each active session.<br>If you are looking at the **sessions by users** (or **all sessions**) report, click **+** or **-** to display or hide details about a user's sessions. |
| Service | This field displays the protocol used in each active session.<br>If you are looking at the **sessions by services** report, click **+** or **-** to display or hide details about a protocol's sessions. |
| Source | This field displays the source IP address and port in each active session.<br>If you are looking at the **sessions by source IP** report, click **+** or **-** to display or hide details about a source IP address's sessions. |
| Destination | This field displays the destination IP address and port in each active session.<br>If you are looking at the **sessions by destination IP** report, click **+** or **-** to display or hide details about a destination IP address's sessions. |
| Rx | This field displays the amount of information received by the source in the active session. |
| Tx | This field displays the amount of information transmitted by the source in the active session. |
| Duration | This field displays the length of the active session in seconds. |
| Count | This field displays the number of active sessions for each user, service, or IP address. This field does not display when you are viewing **all sessions** (since each session is displayed individually). |

# 48.4 The Anti-Virus Report Screen

Click **Maintenance > Report > Anti-Virus** to display the following screen. This screen displays anti-virus statistics.

**Figure 554** Maintenance > Report > Anti-Virus: Virus Name




The following table describes the labels in this screen.

**Table 268** Maintenance > Report > Anti-Virus

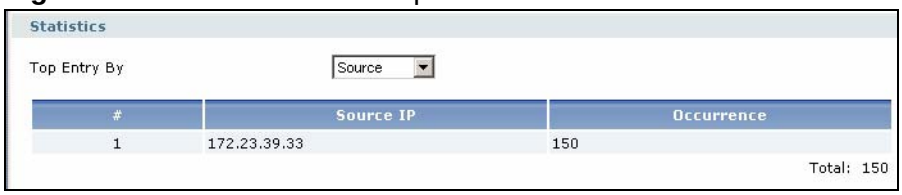
| LABEL | DESCRIPTION |
|---|---|
| Collect Statistics | Select this check box to have the ZyWALL collect anti-virus statistics.<br><br>The collection starting time displays after you click **Apply**. All of the statistics in this screen are for the time period starting at the time displayed here. The format is year, month, day and hour, minute, second. All of the statistics are erased if you restart the ZyWALL or click **Flush Data**. Collecting starts over and a new collection start time displays. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |
| Refresh | Click this button to update the report display. |
| Flush Data | Click this button to discard all of the screen's statistics and update the report display. |
| Total Viruses Detected | This field displays the number of different viruses that the ZyWALL has detected. |
| Infected Files Detected | This field displays the number of files in which the ZyWALL has detected a virus. |
| Top Entry By | Use this field to have the following (read-only) table display the top anti-virus entries by **Virus Name**, **Source** or **Destination**.<br><br>Select **Virus Name** to list the most common viruses that the ZyWALL has detected.<br><br>Select **Source** to list the source IP addresses from which the ZyWALL has detected the most virus-infected files.<br><br>Select **Destination** to list the most common destination IP addresses for virus-infected files that ZyWALL has detected. |
| # | This field displays the entry's rank in the list of the top entries. |

**Table 268** Maintenance > Report > Anti-Virus (continued)

| LABEL | DESCRIPTION |
|---|---|
| Virus name | This column displays when you display the entries by **Virus Name**. This displays the name of a detected virus. |
| Source IP | This column displays when you display the entries by **Source.** It shows the source IP address of virus-infected files that the ZyWALL has detected. |
| Destination IP | This column displays when you display the entries by **Destination.** It shows the destination IP address of virus-infected files that the ZyWALL has detected. |
| Occurrences | This field displays how many times the ZyWALL has detected the event described in the entry. |
| Total | This field displays the sum of the occurrences of the events in the entries. |

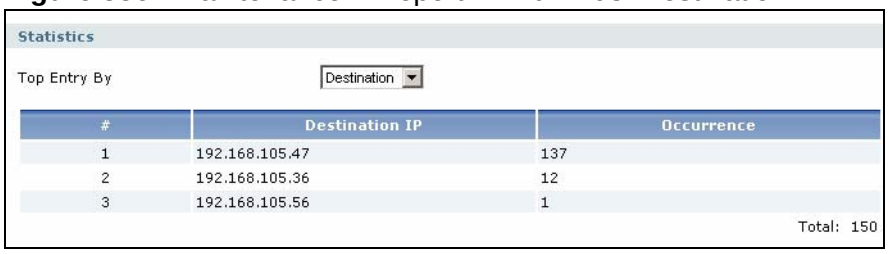
The statistics display as follows when you display the top entries by source.

**Figure 555** Maintenance > Report > Anti-Virus: Source




The statistics display as follows when you display the top entries by destination.

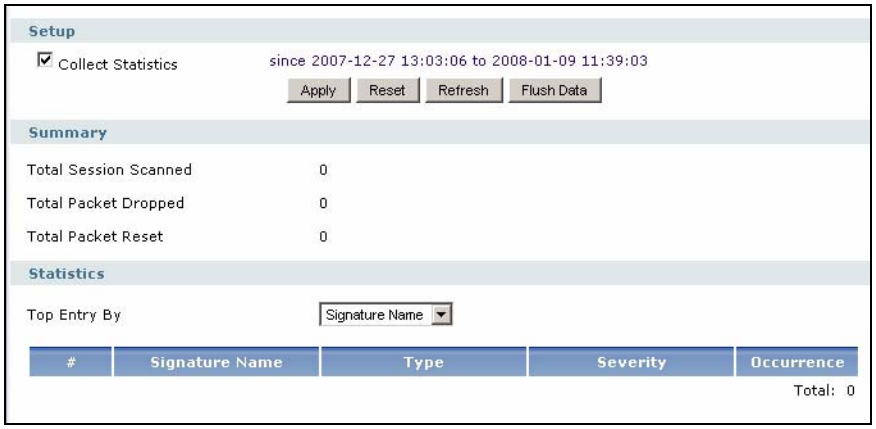
**Figure 556** Maintenance > Report > Anti-Virus: Destination



# 48.5 The IDP Report Screen

Click **Maintenance > Report > IDP** to display the following screen. This screen displays IDP (Intrusion Detection and Prevention) statistics.

**Figure 557** Maintenance > Report > IDP: Signature Name




The following table describes the labels in this screen.

**Table 269** Maintenance > Report > IDP

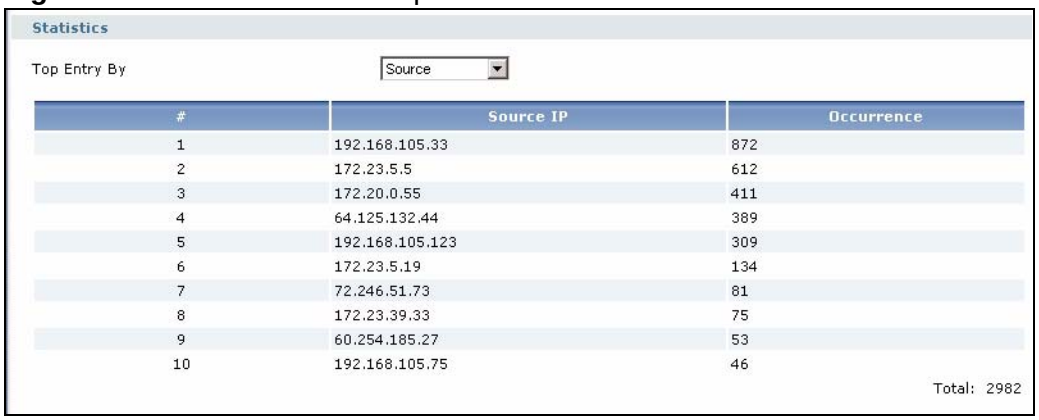
| LABEL | DESCRIPTION |
|---|---|
| Collect Statistics | Select this check box to have the ZyWALL collect IDP statistics.<br>The collection starting time displays after you click **Apply**. All of the statistics in this screen are for the time period starting at the time displayed here. The format is year, month, day and hour, minute, second. All of the statistics are erased if you restart the ZyWALL or click **Flush Data**. Collecting starts over and a new collection start time displays. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |
| Refresh | Click this button to update the report display. |
| Flush Data | Click this button to discard all of the screen's statistics and update the report display. |
| Total Sessions Scanned | This field displays the number of sessions that the ZyWALL has checked for intrusion characteristics. |
| Total Packet Dropped | The ZyWALL can detect and drop malicious packets from network traffic. This field displays the number of packets that the ZyWALL has dropped. |
| Total Packet Reset | The ZyWALL can detect and drop malicious packets from network traffic. This field displays the number of packets that the ZyWALL has reset. |

**Table 269** Maintenance > Report > IDP (continued)

| LABEL | DESCRIPTION |
|---|---|
| Top Entry By | Use this field to have the following (read-only) table display the top IDP entries by **Signature Name**, **Source** or **Destination**.<br><br>Select **Signature Name** to list the most common signatures that the ZyWALL has detected.<br><br>Select **Source** to list the source IP addresses from which the ZyWALL has detected the most intrusion attempts.<br><br>Select **Destination** to list the most common destination IP addresses for intrusion attempts that the ZyWALL has detected. |
| # | This field displays the entry's rank in the list of the top entries. |
| Signature Name | This column displays when you display the entries by **Signature Name**. The signature name identifies a specific intrusion pattern. Click the hyperlink for more detailed information on the intrusion. |
| Type | This column displays when you display the entries by **Signature Name**. It shows the categories of intrusions. See Table 164 on page 533 for more information. |
| Severity | This column displays when you display the entries by **Signature Name**. It shows the level of threat that the intrusions may pose. See Table 163 on page 531 for more information. |
| Source IP | This column displays when you display the entries by **Source.** It shows the source IP address of the intrusion attempts. |
| Destination IP | This column displays when you display the entries by **Destination.** It shows the destination IP address at which intrusion attempts were targeted. |
| Occurrences | This field displays how many times the ZyWALL has detected the event described in the entry. |
| Total | This field displays the sum of the occurrences of the events in the entries. |

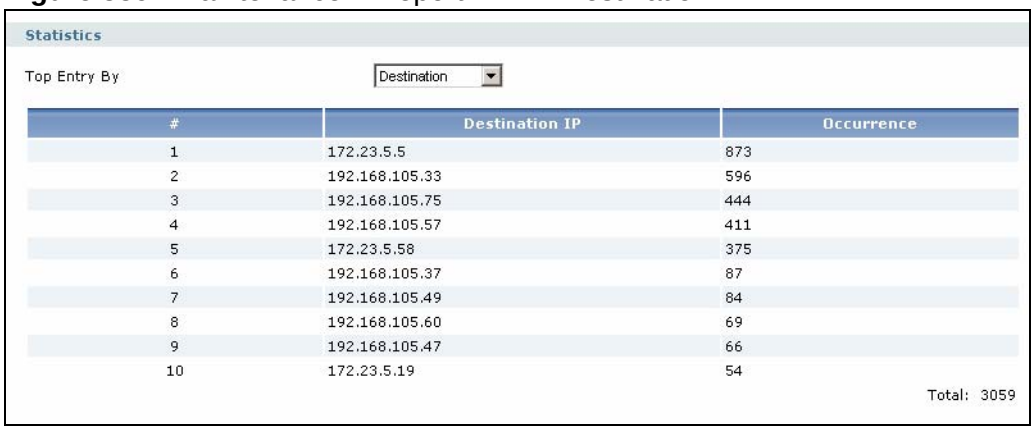
The statistics display as follows when you display the top entries by source.

**Figure 558** Maintenance > Report > IDP: Source



The statistics display as follows when you display the top entries by destination.

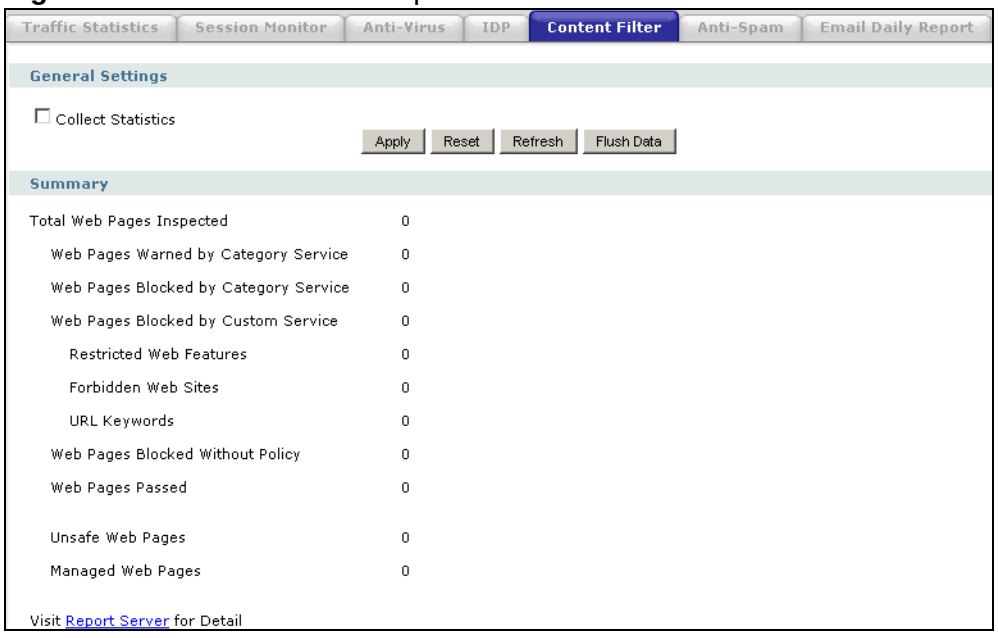
**Figure 559** Maintenance > Report > IDP: Destination




# 48.6 The Content Filter Report Screen

Click **Maintenance > Report > Content Filter** to display the following screen. This screen displays content filter statistics.

**Figure 560** Maintenance > Report > Content Filter



The following table describes the labels in this screen.

**Table 270** Maintenance > Report > Content Filter

| LABEL | DESCRIPTION |
|---|---|
| Collect Statistics | Select this check box to have the ZyWALL collect content filtering statistics.<br><br>The collection starting time displays after you click **Apply**. All of the statistics in this screen are for the time period starting at the time displayed here. The format is year, month, day and hour, minute, second. All of the statistics are erased if you restart the ZyWALL or click **Flush Data**. Collecting starts over and a new collection start time displays. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |
| Refresh | Click this button to update the report display. |
| Flush Data | Click this button to discard all of the screen's statistics and update the report display. |
| Total Web Pages Inspected | This field displays the number of web pages that the ZyWALL's content filter feature has checked. |
| Web Pages Warned by Category Service | This is the number of web pages that matched an external database content filtering category selected in the ZyWALL and for which the ZyWALL displayed a warning before allowing users access. |
| Web Pages Blocked by Category Service | This is the number of web pages to which the ZyWALL did not allow access because they matched an external database content filtering category to which the ZyWALL was configured to block access. |
| Web Pages Blocked by Custom Service | This is the number of web pages to which the ZyWALL did not allow access due to the content filtering custom service configuration. |
| Restricted Web Features | This is the number of web pages to which the ZyWALL did not allow access due to the content filtering custom service's restricted web features configuration. |
| Forbidden Web Sites | This is the number of web pages to which the ZyWALL did not allow access because they matched the content filtering custom service's forbidden web sites list. |
| URL Keywords | This is the number of web pages to which the ZyWALL did not allow access because they contained one of the content filtering custom service's list of forbidden keywords. |
| Web Pages Blocked Without Policy | This is the number of web pages to which the ZyWALL did not allow access because they were not rated by the external database content filtering service. |
| Web Pages Passed | This is the number of web pages to which the ZyWALL allowed access. |
| Unsafe Web Pages | This is the number of requested web pages that the ZyWALL's content filtering service identified as posing a threat to users. |

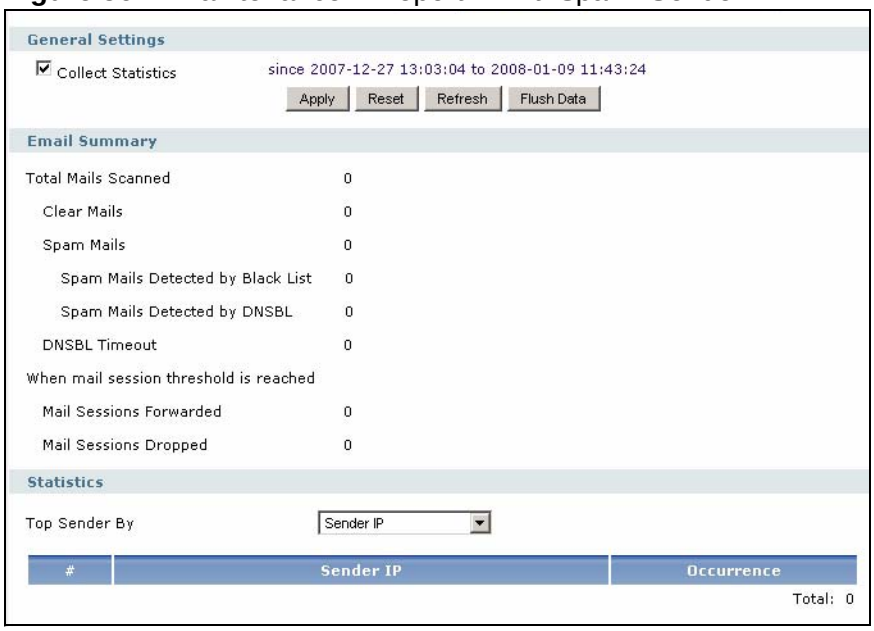
**Table 270** Maintenance > Report > Content Filter (continued)

| LABEL | DESCRIPTION |
|---|---|
| Managed Web Pages | This is the number of requested web pages that the ZyWALL's content filtering service identified as belonging to a category that was selected to be managed. |
| Report Server | Click this link to go to http://www.myZyXEL.com where you can view content filtering reports after you have activated the category-based content filtering subscription service. |

# 48.7 The Anti-Spam Report Screen

Click **Maintenance > Report > Anti-Spam** to display the following screen. This screen displays spam statistics.

**Figure 561** Maintenance > Report > Anti-Spam: Sender IP




The following table describes the labels in this screen.

**Table 271** Maintenance > Report > Anti-Spam

| LABEL | DESCRIPTION |
|---|---|
| Collect Statistics | Select this check box to have the ZyWALL collect anti-spam statistics.<br><br>The collection starting time displays after you click **Apply**. All of the statistics in this screen are for the time period starting at the time displayed here. The format is year, month, day and hour, minute, second. All of the statistics are erased if you restart the ZyWALL or click **Flush Data**. Collecting starts over and a new collection start time displays. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

**Table 271** Maintenance > Report > Anti-Spam (continued)

| LABEL | DESCRIPTION |
|---|---|
| Refresh | Click this button to update the report display. |
| Flush Data | Click this button to discard all of the screen's statistics and update the report display. |
| Total Mails Scanned | This field displays the number of e-mails that the ZyWALL's anti-spam feature has checked. |
| Clear Mails | This is the number of e-mails that the ZyWALL has determined to not be spam. |
| Spam Mails | This is the number of e-mails that the ZyWALL has determined to be spam. |
| Spam Mails Detected by Black List | This is the number of e-mails that matched an entry in the ZyWALL's anti-spam black list. |
| Spam Mails Detected by DNSBL | The ZyWALL can check the sender and relay IP addresses in an e-mail's header against DNS (Domain Name Service)-based spam Black Lists (DNSBLs). This is the number of e-mails that had a sender or relay IP address in the header which matched one of the DNSBLs that the ZyWALL uses. |
| DSNBL Timeout | This is how many queries that were sent to the ZyWALL's configured list of DNSBL domains and did not receive a response in time. |
| Mail Sessions Forwarded | This is how many e-mail sessions the ZyWALL allowed because they exceeded the maximum number of e-mail sessions that the anti-spam feature can check at a time.<br>You can see the ZyWALL's threshold of concurrent e-mail sessions in the **Anti-Spam > Status** screen.<br>Use the **Anti-Spam > General** screen to set whether the ZyWALL forwards or drops sessions that exceed this threshold. |
| Mail Sessions Dropped | This is how many e-mail sessions the ZyWALL dropped because they exceeded the maximum number of e-mail sessions that the anti-spam feature can check at a time.<br>You can see the ZyWALL's threshold of concurrent e-mail sessions in the **Anti-Spam > Status** screen.<br>Use the **Anti-Spam > General** screen to set whether the ZyWALL forwards or drops sessions that exceed this threshold. |
| Top Sender By | Use this field to list the top e-mail or IP addresses from which the ZyWALL has detected the most spam.<br>Select **Sender IP** to list the source IP addresses from which the ZyWALL has detected the most spam.<br>Select **Sender Email Address** to list the top e-mail addresses from which the ZyWALL has detected the most spam. |
| # | This field displays the entry's rank in the list of the top entries. |
| Sender IP | This column displays when you display the entries by **Sender IP**. It shows the source IP address of spam e-mails that the ZyWALL has detected. |

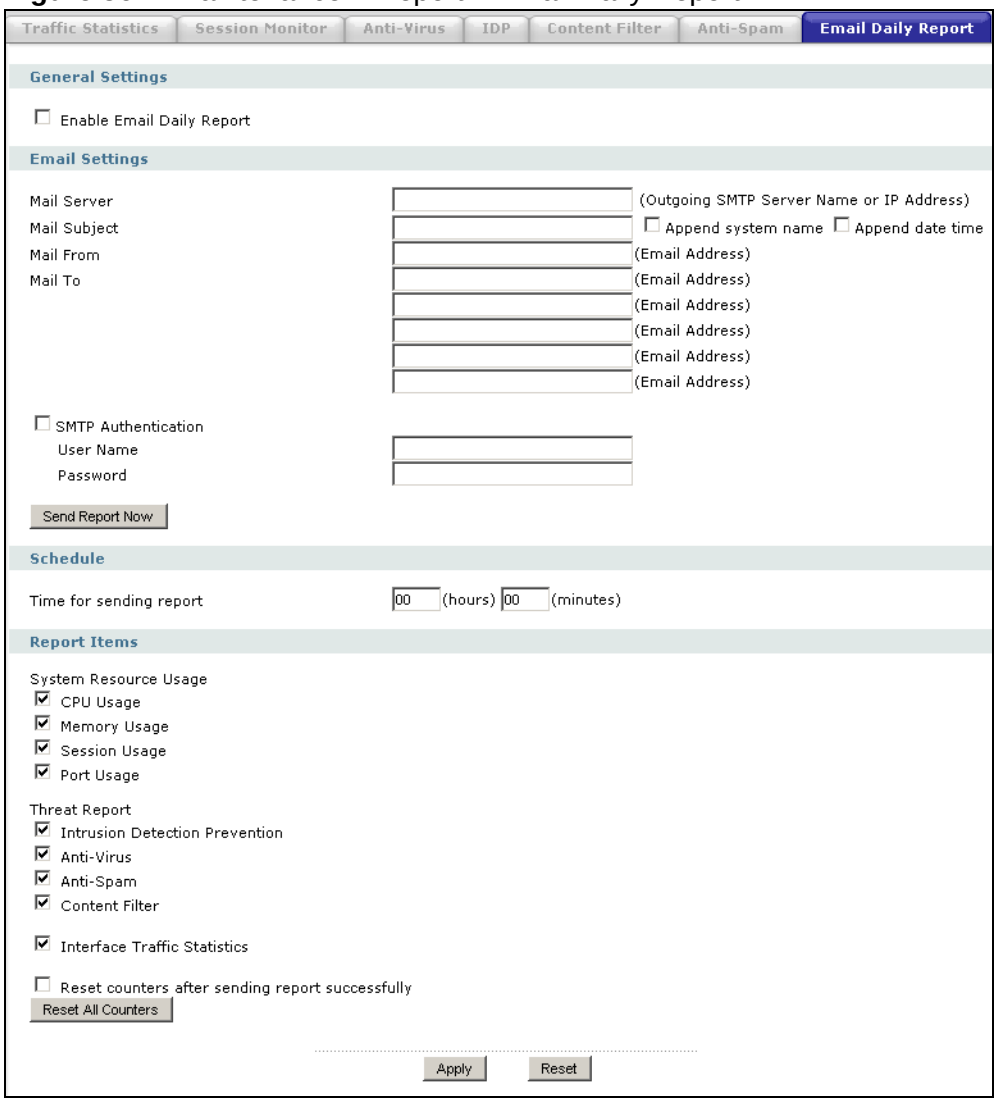
**Table 271** Maintenance > Report > Anti-Spam (continued)

| LABEL | DESCRIPTION |
|---|---|
| Sender Mail Address | This column displays when you display the entries by **Sender Mail Address**. This column displays the e-mail addresses from which the ZyWALL has detected the most spam. |
| Occurrence | This field displays how many spam e-mails the ZyWALL detected from the sender. |
| Total | This field displays the sum of the occurrences of the events in the entries. |

# 48.8 The Email Daily Report Screen

Click **Maintenance > Report > Email Daily Report** to display the following screen. Configure this screen to have the ZyWALL e-mail you system statistics every day.

**Figure 562** Maintenance > Report > Email Daily Report




The following table describes the labels in this screen.

**Table 272** Maintenance > Report > Email Daily Report

| LABEL | DESCRIPTION |
|---|---|
| Enable Email Daily Report | Select this to send reports by e-mail every day. |
| Mail Server | Type the name or IP address of the outgoing SMTP server. |

**Table 272** Maintenance > Report > Email Daily Report (continued)

| LABEL | DESCRIPTION |
|---|---|
| Mail Subject | Type the subject line for the outgoing e-mail. Select **Append system name** to add the ZyWALL's system name to the subject. Select **Append date time** to add the ZyWALL's system date and time to the subject. |
| Mail From | Type the e-mail address from which the outgoing e-mail is delivered. This address is used in replies. |
| Mail To | Type the e-mail address (or addresses) to which the outgoing e-mail is delivered. |
| SMTP Authentication | Select this check box if it is necessary to provide a user name and password to the SMTP server. |
| User Name | This box is effective when you select the **SMTP Authentication** check box. Type the user name to provide to the SMTP server when the log is e-mailed. |
| Password | This box is effective when you select the **SMTP Authentication** check box. Type the password to provide to the SMTP server when the log is e-mailed. |
| Send Report Now | Click this button to have the ZyWALL send the daily e-mail report immediately. |
| Time for sending report | Select the time of day (hours and minutes) when the log is e-mailed. Use 24-hour notation. |
| Report Items | Select the information to include in the report. Select **Reset counters after sending report successfully** if you only want to see statistics for a 24 hour period. |
| Reset All Counters | Click this to discard all report data and start all of the counters over at zero. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# 49

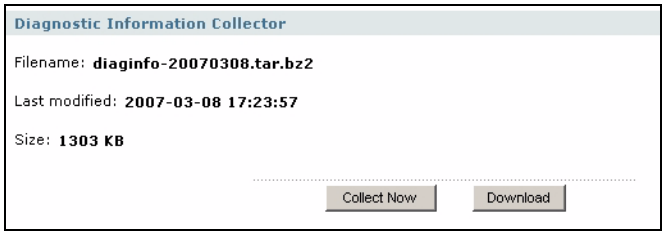
# Diagnostics

## 49.1 The Diagnostics Screen

The **Diagnostics** screen provides an easy way for you to generate a file containing the ZyWALL's configuration and diagnostic information. You may need to generate this file and send it to customer support during troubleshooting.

Click **Maintenance > Diagnostics** to open the **Diagnostics** screen.

**Figure 563** Maintenance > Diagnostics




The following table describes the labels in this screen.

**Table 273** Maintenance > Diagnostics

| LABEL | DESCRIPTION |
|---|---|
| Filename | This is the name of the most recently created diagnostic file. |
| Last modified | This is the date and time that the last diagnostic file was created. The format is yyyy-mm-dd hh:mm:ss. |
| Size | This is the size of the most recently created diagnostic file. |
| Collect Now | Click this to have the ZyWALL create a new diagnostic file. |
| Download | Click this to save the most recent diagnostic file to a computer. |

# 50 Reboot

## 50.1 Overview

Use this to restart the device (for example, if the device begins behaving erratically). See also Section 1.4 on page 34 for information on different ways to start and stop the ZyWALL.

### 50.1.1 What You Need To Know About Reboot

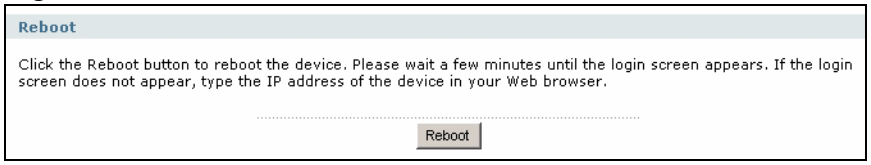
If you applied changes in the Web configurator, these were saved automatically and do not change when you reboot. If you made changes in the CLI, however, you have to use the `write` command to save the configuration before you reboot. Otherwise, the changes are lost when you reboot.

Reboot is different to reset; (see Section 51.1 on page 831) reset returns the device to its default configuration.

## 50.2 The Reboot Screen

The **Reboot** screen is part of the Web configurator so that remote users can restart the device. To access this screen, click **Maintenance** > **Reboot**.

**Figure 564** Maintenance > Reboot




Click the **Reboot** button to restart the ZyWALL. Wait a few minutes until the login screen appears. If the login screen does not appear, type the IP address of the device in your Web browser.

You can also use the CLI command `reboot` to restart the ZyWALL.

# 51

# Troubleshooting

This chapter offers some suggestions to solve problems you might encounter.

- You can also refer to the logs (see Chapter 51 on page 829).
- For individual log descriptions, Appendix A on page 845.

For the order in which the ZyWALL applies its features and checks, see Section 2.2 on page 37. I cannot set up an IPSec VPN tunnel to another device.

If the IPSec tunnel does not build properly, the problem is likely a configuration error at one of the IPSec routers. Log into both ZyXEL IPSec routers and check the settings in each field methodically and slowly. Make sure both the ZyWALL and remote IPSec router have the same security settings for the VPN tunnel. It may help to display the settings for both routers side-by-side.

Here are some general suggestions. See also Chapter 21 on page 363.

- The system log can often help to identify a configuration problem.
- If the sites are/were previously connected using a leased line or ISDN router, physically disconnect these devices from the network before testing your new VPN connection. The old route may have been learnt by RIP and would take priority over the new VPN connection.
- To test whether or not a tunnel is working, ping from a computer at one site to a computer at the other.
  Before doing so, ensure that both computers have Internet access (via the IPSec routers).
- It is also helpful to have a way to look at the packets that are being sent and received by the ZyWALL and remote IPSec router (for example, by using a packet sniffer).

Check the configuration for the following ZyWALL features.

- The ZyWALL does not put IPSec SAs in the routing table. You must create a policy route for each VPN tunnel. See Chapter 12 on page 271.
- Make sure the To-ZyWALL firewall rules allow IPSec VPN traffic to the ZyWALL. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.

- The ZyWALL supports UDP port 500 and UDP port 4500 for NAT traversal. If you enable this, make sure the To-ZyWALL firewall rules allow UDP port 4500 too.
- Make sure regular firewall rules allow traffic between the VPN tunnel and the rest of the network. Regular firewall rules check packets the ZyWALL sends before the ZyWALL encrypts them and check packets the ZyWALL receives after the ZyWALL decrypts them. This depends on the zone to which you assign the VPN tunnel and the zone from which and to which traffic may be routed.
- If you set up a VPN tunnel across the Internet, make sure your ISP supports AH or ESP (whichever you are using).
- If you have the ZyWALL and remote IPSec router use certificates to authenticate each other, make sure they trust each other's certificates. If the ZyWALL's certificate is self-signed, import it into the remote IPsec router. If it is signed by a CA, make sure the remote IPsec router trusts that CA. The ZyWALL uses one of its **Trusted Certificates** to authenticate the remote IPSec router's certificate. The trusted certificate can be the remote IPSec router's self-signed certificate or that of a trusted CA that signed the remote IPSec router's certificate.

## I cannot set up an L2TP VPN tunnel.

1. Make sure you have configured L2TP correctly on the remote user computers. See Section 28.6 on page 451 for examples.
2. Make sure you configured an appropriate policy route on the ZyWALL.
3. Make sure there is not a firewall or NAT router between the ZyWALL and the remote users.
4. Make sure the remote users are using public IP addresses.

## The VPN connection is up but VPN traffic cannot be transmitted through the VPN tunnel.

Routing policies define how the ZyWALL forwards packets to their destinations. You must create a policy route for the ZyWALL to route VPN traffic through a VPN tunnel to the remote network.

The VPN wizard automatically creates a corresponding policy route. If you use the **VPN > IPSec VPN** or **VPN > L2TP VPN** screens to set up a VPN tunnel, you need to manually configure a policy route for the VPN tunnel.

### I cannot download the ZyWALL's firmware package.

The ZyWALL's firmware package cannot go through the ZyWALL when you enable the anti-virus **Destroy compressed files that could not be decompressed** option. The ZyWALL classifies the firmware package as not being able to be decompressed and deletes it.

You can upload the firmware package to the ZyWALL with the option enabled, so you only need to clear the **Destroy compressed files that could not be decompressed** option while you download the firmware package. See Section 30.2.1 on page 511 for more on the anti-virus **Destroy compressed files that could not be decompressed** option.

### I changed the LAN IP address and can no longer access the Internet.

The ZyWALL automatically updates address objects based on an interface's IP address, subnet, or gateway if the interface's IP address settings change. However, you need to manually edit any address objects for your LAN that are not based on the interface.

## 51.1 Resetting the ZyWALL

If you cannot access the ZyWALL by any method, try restarting it by turning the power off and then on again. If you still cannot access the ZyWALL by any method or you forget the administrator password(s), you can reset the ZyWALL to its factory-default settings. Any configuration files or shell scripts that you saved on the ZyWALL should still be available afterwards.

Use the following procedure to reset the ZyWALL to its factory-default settings. This overwrites the settings in the startup-config.conf file with the settings in the system-default.conf file.

Note: This procedure removes the current configuration.

If you want to reboot the device without changing the current configuration, see Chapter 50 on page 827.

1 Make sure the **SYS** LED is on and not blinking.

2 Press the **RESET** button and hold it until the **SYS** LED begins to blink. (This usually takes about five seconds.)

3 Release the **RESET** button, and wait for the ZyWALL to restart.

You should be able to access the ZyWALL using the default settings.

## 51.2 Getting More Troubleshooting Help

Search for support information for your model at www.zyxel.com for more troubleshooting suggestions.

# 52

# Product Specifications

The following specifications are subject to change without notice. See Chapter 2 on page 35 for a general overview of key features.

This table provides basic device specifications.

**Table 274** Default Login Information

| ATTRIBUTE | SPECIFICATION |
|---|---|
| Default IP Address (P4) | 192.168.1.1 |
| Default Subnet Mask (P4) | 255.255.255.0 (24 bits) |
| Default Password | 1234 |

This table provides hardware specifications.

**Table 275** Hardware Specifications

| FEATURE | SPECIFICATION |
|---|---|
| Ethernet Interfaces | Number of Ethernet interfaces: 7<br>All Ethernet interfaces are Gigabit Ethernet, full duplex RJ-45 connectors, auto-negotiation, auto-MDI/MDIX (auto-crossover) |
| Management interface | RS-232, DB9F connector |
| AUX port | RS-232, DB9M connector |
| USB Slots | 2, 2.0 plug and play |
| Compatible USB Cards | Huawei E220 and E270(3G) |
| Extension Card Slot | Slot for optional hardware accessories<br>PCMCIA slot for a wireless LAN or cellular (3G) card. |
| Compatible PCMCIA Cards | ZyXEL's G-170S IEEE 802.11g wireless card.<br>Sierra Wireless AC850, AC860, AC880 or AC881 3G card |
| Power Requirements | 12V DC |
| Operating Environment | Temperature: 0 C to 50 C<br>Humidity: 5% to 95% (non-condensing) |
| Storage Environment | Temperature: -30 C to 60 C<br>Humidity: 5% to 95% (non-condensing) |

**Table 275** Hardware Specifications (continued)

| FEATURE | SPECIFICATION |
|---|---|
| MTBF | Mean Time Between Failures: 323,823 hours |
| Dimensions | 242 (W) x 175 (D) x 35.5 (H) mm |
| Weight | 1.2 kg |
| Rack-mounting | Rack-mountable (rack-mount kit included) |
| Wall-mounting | The ZyWALL has wall-mounting holes on the bottom panel. The centers of the holes are located 156 mm apart. |

**It is recommended that you do NOT wall-mount the ZyWALL. A wall-mounting kit is not included.**

This table gives details about the ZyWALL's features.

**Table 276** Feature Specifications

| MODEL<br>FEATURE | USG 200 | USG 100 |
|---|---|---|
| # of MAC | 6 | 5 |
| Flash Size | 256 | 256 |
| DRAM Size | 256 | 256 |
| | | |
| **INTERFACE** | | |
| VLAN | 32 | 32 |
| Virtual (alias) | 4 per interface | 4 per interface |
| PPP | 3 | 2 |
| Bridge | 8 | 8 |
| **ROUTING** | | |
| Static Routes | 128 | 128 |
| Policy Routes | 500 | 200 |
| Sessions | 40,000 | 20,000 |
| **NAT** | | |
| Virtual Servers | up to 512 | up to 256 |
| Trigger Port Rules | up to 8 per PR rule | up to 8 per PR rule |
| HTTP Redirect | up to interface limit | up to interface limit |
| New Session Rate (sessions per second) | 1400 | 1000 |
| **FIREWALL** | | |
| Firewall ACL Rules | 1000 | 500 |
| **APPLICATION PATROL** | | |
| Maximum Rules for Other Protocols | 24 | 16 |

**Table 276** Feature Specifications (continued)

| MODEL / FEATURE | USG 200 | USG 100 |
|---|---|---|
| Maximum Rules for Each Protocol | 24 | 16 |
| Default Ports | 8 | 8 |
| **USER PROFILES** | | |
| Maximum Local Users | 192 | 128 |
| Maximum Admin Users | 5 | 5 |
| Maximum User Groups | 64 | 32 |
| Maximum Users in One User Group | 192 | 128 |
| **OBJECTS** | | |
| Address Objects | 500 | 200 |
| Address Groups | 100 | 50 |
| Maximum address object in one group | 128 | 128 |
| Service Objects | 500 | 200 |
| Service Groups | 100 | 50 |
| Maximum service object in one group | 128 | 128 |
| Schedule Objects | 64 | 32 |
| Maximum Number of LDAP Groups | 4 | 2 |
| Maximum Number of LDAP Servers for Each LDAP Group | 2 | 2 |
| Maximum Number of RADIUS Groups | 4 | 2 |
| Maximum Number of RADIUS Servers for Each RADIUS Group | 2 | 2 |
| Maximum AD server for each AD group | 2 | 2 |
| Maximum AD group number | 4 | 4 |
| Maximum Number of Authentication Methods | 4 | 2 |
| Maximum Number of Zones | 7 | 6 |
| Maximum Number of Trunks | 5 | 5 |
| **IPSEC VPN** | | |
| Maximum Number of IPSec VPN Tunnels | 100 | 50 |
| Maximum Number of IPSec VPN Concentrators | 4 | 2 |
| **CERTIFICATES** | | |
| Certificate Buffer Size | 128 K | 64 K |
| **BUILT-IN SERVICES** | | |
| A record | 64 | 64 |
| NS record | 8 | 8 |
| MX record | 8 | 8 |

**Table 276** Feature Specifications (continued)

| MODEL / FEATURE | USG 200 | USG 100 |
|---|---|---|
| Maximum Number of Service Control Entries | 16 per service | 16 per service |
| Maximum DHCP Host Pool | 256 | 128 |
| Maximum Number of DDNS Profiles | 5 | 5 |
| DHCP Relay | 2 per interface | 2 per interface |
| **CENTRALIZED LOG** | | |
| Log Entries | 512 | 512 |
| Debug Log Entries | 1024 | 1024 |
| Admin E-mail Addresses | 2 | 2 |
| Syslog Servers | 4 | 4 |
| **IDP** | | |
| Maximum Number of IDP Profiles | 8 | 8 |
| Custom Signatures | 64 | 32 |
| Maximum Number of IDP Rules | 32 | 32 |
| **ADP** | | |
| Maximum Number of ADP Profiles | 8 | 8 |
| Maximum Number of ADP Rules | 32 | 32 |
| Maximum Block Host Number | 1000 | 1000 |
| Maximum Block Period | 3600 | 3600 |
| **CONTENT FILTER** | | |
| Maximum Number of Content Filter Policies | 16 | 16 |
| Maximum Number of Content Filter Profiles | 16 | 16 |
| Maximum Number of Forbidden Domain Entries | 128 per profile | 128 per profile |
| Maximum Number of Trusted Domain Entries | 128 per profile | 128 per profile |
| Maximum Number of Keywords that Can Be Blocked | 128 per profile | 128 per profile |
| Local Cache Size | 2048 | 1024 |
| Maximum Number of Concurrent Connection Requests | 192 | 128 |
| **ANTI-SPAM** | | |
| Maximum Number of Concurrent Mail Sessions | 150 | 100 |
| Maximum Number of Anti-Spam Rules | 32 | 32 |
| Maximum Number of White List Entries | 128 | 128 |

**Table 276** Feature Specifications (continued)

| MODEL / FEATURE | USG 200 | USG 100 |
|---|---|---|
| Maximum Number of Black List Entries | 128 | 128 |
| Maximum Number of DNSBLs | 5 | 5 |
| Maximum Number of Anti-Spam Statistics | 500 | 500 |
| Maximum Anti-Spam Statistics Ranking | 10 | 10 |
| **ANTI-VIRUS** | | |
| Maximum Number of Concurrent ZIP File Decompression Sessions | 50 ZIP files<br>8 RAR-LZSS or 1 RAR-PPM | 30 ZIP files<br>4 RAR-LZSS or 1 RAR-PPM |
| Maximum Number of Anti-Virus Rules | 32 | 32 |
| Maximum Number of White List Entries | 256 | 256 |
| Maximum Number of Black List Entries | 256 | 256 |
| Maximum Number of Anti-Virus Statistics | 500 | 500 |
| Maximum Anti-Virus Statistics Ranking | 10 | 10 |
| **SSL VPN** | | |
| Maximum SSL VPN Connections | 2 without a license<br>10 with license | 2 without a license<br>5 with license |
| **OTHERS** | | |
| Maximum Number of Device HA VRRP Groups | 16 | 16 |
| Maximum Number of OSPF Areas | 32 | 32 |

The following table, which is not exhaustive, lists standards referenced by ZyWALL features.

**Table 277** Standards Referenced by Features

| FEATURE | STANDARDS REFERENCED |
|---|---|
| Interface-Bridge | A subset of the ANSI/IEEE 802.1d standard |
| Interface | RFCs 2131, 2132, 1541 |
| Interface-PPP | RFCs 1144, 1321, 1332, 1334, 1661, 1662, 2472 |
| Interface-PPTP | RFCs 2637, 3078 |
| Interface-PPPOE | RFC 2516 |
| Interface-VLAN | IEEE 802.1Q |
| Dynamic Route, Show IP route | RFCs 1058, 2082, 2453, 2328, 3101, 3137 |
| Telnet server | RFCs 1408, 1572 |
| SSH server | RFCs 4250, 4251, 4252, 4253, 4254 |

**Table 277** Standards Referenced by Features (continued)

| FEATURE | STANDARDS REFERENCED |
|---|---|
| Built-in service, DNS server | RFCs 1034, 1035, 1123, 1183, 1535, 1536, 1706, 1712, 1750, 1876, 1982, 1995, 1996, 2136, 2163, 2181, 2230, 2308, 2535, 2536, 2537, 2538, 2539, 2671, 2672, 2673, 2782, 3007, 3090 |
| Built-in service, DHCP server | RFCs 1542, 2131, 2132, 2485, 2489 |
| Built-in service, HTTP server | RFCs 1945, 2616, 2965, 2732, 2295 |
| Built-in service, SNMP agent | RFCs 1067, 1213, 2576, 2578, 2579, 2580, 2741, 2667, 2981, 3371 |
| Login, LDAP support. | RFCs 2251, 2252, 2253, 2254, 2255, 2256, 2589, 2829, 2830 |
| Used by Apache | RFCs 2437, 2246, 2560, 2712, 3268, 3280, 3820, 4132 |
| Built-in service, FTP server | RFCs 959, 2228, 2389, 2865, 2138, 2640 |
| Used by Centralized log | RFC 3164 |
| Login, new PAM module | OSF-RFC 86.0, 1321 |
| Built-in service, NTP client | RFCs 958, 1059, 1119, 1305 |
| Used by SSH service | RFCs 4250, 4251, 4252, 4253, 4254 |
| Used by Time service | RFCs 3339 |
| Used by Telnet service | RFCs 318, 854, 1413 |
| Used by SIP ALG | RFCs 3261, 3264 |
| DHCP relay | RFC 1541 |
| ZySH | W3C XML standard |
| ARP | RFC 826 |
| IP/IPv4 | RFC 791 |
| TCP | RFC 793 |

# 52.1 3G or WLAN PCMCIA Card Installation

Only insert a compatible 802.11b/g-compliant wireless LAN PCMCIA or CardBus card or 3G card. Slide the connector end of the card into the slot.

Note: Do not force, bend or twist the card.

**Figure 565** WLAN Card Installation


# 52.2 Power Adaptor Specifications

**Table 278** North American Plug Standards

| | |
|---|---|
| AC POWER ADAPTOR MODEL | PSA18R-120P (ZA)-R |
| INPUT POWER | 100-240VAC, 50/60HZ, 0.5A |
| OUTPUT POWER | 12VDC, 3.5A |
| POWER CONSUMPTION | 20 W MAX. |
| SAFETY STANDARDS | UL, CUL (UL 60950-1 FIRST EDITIONCSA C22.2 NO. 60950-1-03 1ST.) |

**Table 279** European Plug Standards

| | |
|---|---|
| AC POWER ADAPTOR MODEL | PSA18R-120P (ZE)-R |
| INPUT POWER | 100-240VAC, 50/60HZ, 0.5A |
| OUTPUT POWER | 12VDC, 3.5A |
| POWER CONSUMPTION | 20 W MAX. |
| SAFETY STANDARDS | TUV, CE (EN 60950-1) |

**Table 280** United Kingdom Plug Standards

| | |
|---|---|
| AC POWER ADAPTOR MODEL | PSA18R-120P (ZK)-R |
| INPUT POWER | 100-240VAC, 50/60HZ, 0.5A |

**Table 280** United Kingdom Plug Standards

| | |
|---|---|
| OUTPUT POWER | 12VDC, 3.5A |
| POWER CONSUMPTION | 20 W MAX. |
| SAFETY STANDARDS | TUV (BS EN 60950-1) |

**Table 281** Australia And New Zealand Plug Standards

| | |
|---|---|
| AC POWER ADAPTOR MODEL | PSA18R-120P (ZS)-R |
| INPUT POWER | 100-240VAC, 50/60HZ, 0.5A |
| OUTPUT POWER | 12VDC, 3.5A |
| POWER CONSUMPTION | 20 W MAX. |
| SAFETY STANDARDS | AS/NZ60950 |

**Table 282** Japan Plug Standards

| | |
|---|---|
| AC POWER ADAPTOR MODEL | PSA18R-120P (ZA)-R |
| INPUT POWER | 100-240VAC, 50/60HZ, 0.5A |
| OUTPUT POWER | 12VDC, 3.5A |
| POWER CONSUMPTION | 20 W MAX. |
| SAFETY STANDARDS | JET |

**Table 283** China Plug Standards

| | |
|---|---|
| AC POWER ADAPTOR MODEL | PSA18R-120P (ZA)-R |
| INPUT POWER | 100-240VAC, 50/60HZ, 0.5A |
| OUTPUT POWER | 12VDC, 3.5A |
| POWER CONSUMPTION | 20 W MAX. |
| SAFETY STANDARDS | CCC |

# PART XI
# Appendices and Index

# A

# Log Descriptions

This appendix provides descriptions of example log messages.

**Table 284** Content Filter Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Content filter has been enabled | An administrator turned the content filter on. |
| Content filter has been disabled | An administrator turned the content filter off. |
| Content filter report has been disabled | The content filter report was turned off. |
| Content filter has been enabled | The content filter was report turned on. |
| Content filter has been changed zsb port to 80 | The content filtering checking for unsafe web sites has been changed to use port 80 due to a configuration change. |
| Content filter has been changed zsb port to 23 | The content filtering checking for unsafe web sites has been changed to use port 23 due to a configuration change. |

**Table 285** Forward Web Site Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| %s: Trusted Web site | The device allowed access to a web site in a trusted domain.<br><br>%s: website host |
| %s | The device allowed access to a web site. The content filtering service is registered and activated or the service is not activated in a profile, this is a web site that is not blocked according to a profile and the default policy is not set to block.<br><br>%s: website host |
| %s: Service is not registered | The device allowed access to a web site. The content filtering service is unregistered and the default policy is not set to block.<br><br>%s: website host |

**Table 286** Blocked Web Site Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| %s :%s | The rating server responded that the web site is in a specified category and access was blocked according to a content filter profile.<br>1st %s: website host<br>2nd %s: website category |
| %s: Unrated | The rating server responded that the web site cannot be categorized and access was blocked according to a content filter profile.<br>%s: website host |
| %s: Service is unavailable | Content filter rating service is temporarily unavailable and access to the web site was blocked due to:<br>1. Can't resolve rating server IP (No DNS)<br>2. Invalid service license<br>4. Rating service is restarting<br>5. Can't connect to rating server<br>6. Query failed<br>7. Query timeout<br>8. Too many queries<br>9. Unknown reason<br>%s: website host |
| %s: %s(cache hit) | The web site's category exists in the device's local cache and access was blocked according to a content filter profile.<br>1st %s: website host<br>2nd %s: website category |
| %s: Not in trusted web list | The web site is not a trusted host/domain, and the device blocks all traffic except for trusted web sites.<br>%s: website host |
| %s: Contains ActiveX | The web site contains ActiveX and access was blocked according to a profile.<br>%s: website host |
| %s: Contains Java applet | The web site contains Java applet and access was blocked according to a profile.<br>%s: website host |
| %s: Contains cookie | The web site contains a cookie and access was blocked according to a profile.<br>%s: website host |

**Table 286** Blocked Web Site Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| %s: Proxy mode is detected | The system detected a proxy connection and blocked access according to a profile.<br>%s: website host |
| %s: Forbidden Web site | The web site is in forbidden web site list.<br>%s: website host |
| %s: Keyword blocking | The web content matched a user defined keyword.<br>%s: website host |
| %s: Blocking by default policy | No content filter policy is applied and access was blocked since the default action is block.<br>%s: website host |

**Table 287** Anti-Spam Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Anti-Spam has been activated. | The anti-spam feature has been turned on. |
| Anti-Spam has been deactivated. | The anti-spam feature has been turned off. |
| Anti-Spam policy %d has been modified. | The anti-spam policy with the specified index number (%d) has been changed. |
| Anti-Spam policy %d has been inserted. | The anti-spam policy with the specified index number (%d) has been added into the list. |
| Anti-Spam policy %d has been appended. | The anti-spam policy with the specified index number (%d) has been added to the end of the list. |
| Anti-Spam policy %d has been deleted. | The anti-spam policy with the specified index number (%d) has been removed. |
| Anti-Spam policy %d has been moved to %d. | The anti-spam policy with the specified index number (first %d) was moved to the specified index number (second %d). |
| White List checking has been activated. | The anti-spam white list has been turned on. |
| White List checking has been deactivated. | The anti-spam white list has been turned off. |
| White List rule %d has been added. | The anti-spam white list rule with the specified index number (%d) has been added. |
| White List rule %d has been modified. | The anti-spam white list rule with the specified index number (%d) has been changed. |
| White List rule %d has been deleted. | The anti-spam white list rule with the specified index number (%d) has been removed. |
| White List rule %d has been activated. | The anti-spam white list rule with the specified index number (%d) has been turned on. |
| White List rule %d has been deactivated. | The anti-spam white list rule with the specified index number (%d) has been turned off. |

**Table 287** Anti-Spam Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Black List checking has been activated. | The anti-spam black list has been turned on. |
| Black List checking has been deactivated. | The anti-spam black list has been turned off. |
| Black List rule %d has been added. | The anti-spam black list rule with the specified index number (%d) has been added. |
| Black List rule %d has been modified. | The anti-spam black list rule with the specified index number (%d) has been changed. |
| Black List rule %d has been deleted. | The anti-spam black list rule with the specified index number (%d) has been removed. |
| Black List rule %d has been activated. | The anti-spam black list rule with the specified index number (%d) has been turned on. |
| Black List rule %d has been deactivated. | The anti-spam black list rule with the specified index number (%d) has been turned off. |
| DNSBL checking has been activated. | anti-spam DNSBL (DNS Black List) server checking has been turned on. |
| DNSBL checking has been deactivated. | The anti-spam DNSBL checking has been turned off. |
| DNSBL domain %s has been added. | The specified DNSBL domain name (%s) has been added. |
| DNSBL domain %s has been modified to %s. | The specified DNSBL domain name (first %s) has been changed to the second %s. |
| DNSBL domain %s has been deleted. | The specified DNSBL domain name (%s) has been removed. |
| DNSBL domain %s has been activated. | The specified DNSBL domain name (%s) has been turned on. |
| DNSBL domain %s has been deactivated. | The specified DNSBL domain name (%s) has been turned off. |
| Match White List: %d. From:%s Subject:%s | An e-mail matched the specified white list rule (%d). The e-mail's From (first %s) and Subject (second %s) header values are listed. |
| Match Black List: %d. From:%s Subject:%s | An e-mail matched the specified black list rule (%d). The e-mail's From (first %s) and Subject (second %s) header values are listed. |
| IP %s in DNSBL %s. From:%s Subject:%s | The listed IP address (the first %s) was listed in the specified DNSBL (second %s). The e-mail's From (third %s) and Subject (fourth %s) header values are listed. |
| DNSBL timeout. Mail From:%s Subject:%s | Queries to the DSNBL timed out. The e-mail's From (first %s) and Subject (second %s) header values are listed. |
| Mail sessions have reached the maximum threshold of %d. | The number of concurrent e-mail sessions has exceeded the maximum number of concurrent e-mail sessions that the anti-spam feature can handle (%d). |

**Table 288** SSL VPN Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| %s %s from %s has logged in SSLVPN | A user has logged into SSL VPN.<br>The first %s is the type of user account.<br>The second %s is the user's user name.<br>The third %s is the name of the service the user is using (HTTP or HTTPS). |
| %s %s from %s has logged out SSLVPN | A user has logged out of SSL VPN.<br>The first %s is the type of user account.<br>The second %s is the user's user name.<br>The third %s is the name of the service the user is using (HTTP or HTTPS).<br>The **Note** field's %s is the user name. |
| %s accesses web application %s | The specified user (first %s) has logged into the specified SSL VPN web application (second %s). |
| SSL tunnel is established | An SSL tunnel has been built. The source is the login IP address. The destination is the IP address given to the SSL user. |
| SSL tunnel is disconnected | An SSL tunnel has been disconnected. The source is the login IP address. The destination is the IP address given to the SSL user. |
| The %s address-object is invalid IP in SSL Policy %s. | The listed address object (first %s) is not an allowed IP for the listed SSL policy (second %s). |
| The %s address-object does not has assignable IP in SSL Policy %s. | There are no more assignable IP addresses in the listed address object (first %s). The address object is used by the listed SSL policy (second %s). |
| The %s address-object is wrong type for '1st-dns' in SSL Policy %s. | The listed address object (first %s) is not the right kind for the first DNS server specified in the listed SSL VPN policy (second %s). |
| The %s address-object is wrong type for '2nd-dns' in SSL Policy %s. | The listed address object (first %s) is not the right kind for the second DNS server specified in the listed SSL VPN policy (second %s). |
| The %s address-object is wrong type for '1st-wins' in SSL Policy %s. | The listed address object (first %s) is not the right kind for the first WINS server specified in the listed SSL VPN policy (second %s). |
| The %s address-object is wrong type for '2nd-wins' in SSL Policy %s. | The listed address object (first %s) is not the right kind for the second WINS server specified in the listed SSL VPN policy (second %s). |

**Table 288** SSL VPN Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| The %s address-object is wrong type for 'network' in SSL Policy %s. | The listed address object (first %s) is not the right kind to be specified as a network in the listed SSL VPN policy (second %s). |
| The SSL VPN policy %s has been changed 'ip-pool' value. | The IP pool setting has been modified in the specified SSL VPN policy (%s). |
| The SSL VPN policy %s has been changed '1st-dns' value. | The first DNS server setting has been modified in the specified SSL VPN policy (%s). |
| The SSL VPN policy %s has been changed '2nd-dns' value. | The second DNS server setting has been modified in the specified SSL VPN policy (%s). |
| The SSL VPN policy %s has been changed '1st-wins' value. | The first WINS server setting has been modified in the specified SSL VPN policy (%s). |
| The SSL VPN policy %s has been changed 'network' value. | The list of networks has been modified in the specified SSL VPN policy (%s). |
| The SSL VPN policy %s has been changed '2nd-wins' value. | The second WINS server setting has been modified in the specified SSL VPN policy (%s). |
| The IP pool is same subnet with %s in SSL VPN policy %s. So %s will not be injected to client side. | The IP pool is in the same subnet as the specified address object (first %s) in the listed SSL VPN policy (second %s), so the listed address (third %s) will not be given to an SSL VPN client. |
| The %s is same subnet with IP pool in SSL VPN policy %s. So %s will not be injected to client side. | The specified address object (first %s) is in the same subnet as the IP pool in the listed SSL VPN policy (second %s), so the listed address (third %s) will not be given to an SSL VPN client. |
| The SSL VPN policy %s does not configure users or user groups. | There are no users or user groups configured for the listed SSL VPN policy (%s). |
| SSL VPN policy rule %s has been inserted. | The listed SSL VPN policy (%s) has been inserted in the list of SSL VPN policy rules. |
| SSL VPN policy rule %s has been appended. | The listed SSL VPN policy (%s) has been added to the end of the list. |
| SSL VPN policy rule %s has been modified. | The configuration of the listed SSL VPN policy (%s) has been changed. |
| SSL VPN policy rule %s has been moved to %d. | The listed SSL VPN policy (%s) has been moved to the listed position (%d) in the list of SSL VPN policies. |
| SSL VPN policy rule %s has been deleted. | The listed SSL VPN policy has been removed. |

**Table 288** SSL VPN Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| %s %s is accessed. sent=<bytes> rcvd=<bytes> | The listed SSL VPN access was used to send and receive the listed numbers of bytes.<br>The first %s is the type of SSL VPN access (web application, file sharing, or network extension).<br>The second %s is the name of the application. This is N/A for a network extension. |
| %s %s from %s has been logged out SSLVPN (re-auth timeout) | The specified user was signed out by the device due to a re-authentication timeout.<br>The first %s is the type of user account.<br>The second %s is the user's user name.<br>The third %s is the name of the service the user is using (HTTP or HTTPS). |
| %s %s from %s has been logged out SSLVPN (lease timeout) | The specified user was signed out by the device due to a lease timeout.<br>The first %s is the type of user account.<br>The second %s is the user's user name.<br>The third %s is the name of the service the user is using (HTTP or HTTPS). |
| %s %s from %s has been logged out SSLVPN (idle timeout) | The specified user was signed out by the device due to an idle timeout.<br>The first %s is the type of user account.<br>The second %s is the user's user name.<br>The third %s is the name of the service the user is using (HTTP or HTTPS). |
| Failed login attempt to SSLVPN from %s (login on a lockout address) | An SSL VPN login attempt from the listed user (%s) was blocked due to too many failed login attempts. |
| Failed login attempt to SSLVPN from %s (reach the max. number of user) | The listed user (%s) failed to log into SSL VPN because the maximum number of users were already logged in. |
| Failed login attempt to SSLVPN from %s (reach the max. number of simultaneous logon) | The listed user (%s) failed to log into SSL VPN because the maximum number of simultaneous logons was already reached. |
| Failed login attempt to SSLVPN from %s (incorrect password or inexistent username) | The listed user (%s) failed to log into SSL VPN because of entering an incorrect password or a user name that does not exist. |

**Table 289** L2TP Over IPSec Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| The configuration of L2TP over IPSec has been changed. | The L2TP over IPSec configuration has been modified. |
| L2TP over IPSec may not work since Crypto Map %s using Manual Key. | L2TP over IPSec does not support manual key management. L2TP over IPSec may not work because the IPSec VPN connection it uses (Crypto Map %s) has been set to use manual key management. |
| L2TP over IPSec may not work since Crypto Map %s using Tunnel Mode. | L2TP over IPSec does not support tunnel mode encapsulation. L2TP over IPSec may not work because the IPSec VPN connection it uses (Crypto Map %s) has been set to use tunnel mode encapsulation. |
| L2TP over IPSec may not work since Crypto Map %s is deactivated. | L2TP over IPSec may not work because the IPSec VPN connection it uses (Crypto Map %s) has been turned off. |
| User %s has been denied from L2TP service. (Inexistent User) | A user with the specified user name (%s) was denied access to the L2TP over IPSec service because the user name does not exist. |
| User %s has been denied from L2TP service. (Disallowed User) | A user with the specified user name (%s) was denied access to the L2TP over IPSec service because the user name is not specified in the L2TP over IPSec configuration. |
| User %s has been denied from L2TP service. (Incorrect Password) | A user with the specified user name (%s) was denied access to the L2TP over IPSec service because the correct password was not provided. |
| User %s has been denied from L2TP service.(Incorrect Username or Password) | A user with the specified user name (%s) was denied access to the L2TP over IPSec service because an incorrect user name or password was provided. |
| User has been denied from L2TP service. (address pool exhausted) | An attempted login to the L2TP over IPSec service failed because the L2TP over IPSec IP address pool does not have any more IP addresses to give out. |
| User %s has been granted an L2TP over IPSec session. | A user with the specified user name (%s) was given access to the L2TP over IPSec service. |
| L2TP over IPSec sessions have been all disconnected since configuration of Tunnel %s has been changed | L2TP over IPSec may not work because the configuration of the IPSec VPN connection it uses (Crypto Map %s) has been changed. |

The ZySH logs deal with internal system errors.

**Table 290** ZySH Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Invalid message queue. Maybe someone starts another zysh daemon. | |
| ZySH daemon is instructed to reset by %d | 1st:pid num |
| System integrity error! | |
| Group OPS | |
| cannot close property group | |
| cannot close group | |
| %s: cannot get size of group | 1st:zysh group name |
| %s: cannot specify properties for entry %s | 1st:zysh group name, 2st:zysh entry name |
| %s: cannot join group %s, loop detected | 1st:zysh group name, 2st:zysh group name |
| cannot create, too many groups (>%d) | 1st:max group num |
| %s: cannot find entry %s | 1st:zysh group name, 2st:zysh entry name |
| %s: cannot remove entry %s | 1st:zysh group name, 2st:zysh entry name |
| List OPS | |
| can't alloc entry: %s! | 1st:zysh entry name |
| can't retrieve entry: %s! | 1st:zysh entry name |
| can't get entry: %s! | 1st:zysh entry name |
| can't print entry: %s! | 1st:zysh entry name |
| %s: cannot retrieve entries from list! | 1st:zysh list name |
| can't get name for entry %d! | 1st:zysh entry index |
| can't get reference count: %s! | 1st:zysh list name |
| can't print entry name: %s! | 1st:zysh entry name |
| Can't append entry: %s! | 1st:zysh entry name |
| Can't set entry: %s! | 1st:zysh entry name |
| Can't define entry: %s! | 1st:zysh entry name |
| %s: list is full! | 1st:zysh list name |
| Can't undefine %s | 1st:zysh list name |

**Table 290** ZySH Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Can't remove %s | 1st:zysh list name |
| Table OPS | |
| %s: cannot retrieve entries from table! | 1st:zysh table name |
| %s: index is out of range! | 1st:zysh table name |
| %s: cannot set entry #%d | 1st:zysh table name,2st: zysh entry num |
| %s: table is full! | 1st:zysh table name |
| %s: invalid old/new index! | 1st:zysh table name |
| Unable to move entry #%d! | 1st:zysh entry num |
| %s: invalid index! | 1st:zysh table name |
| Unable to delete entry #%d! | 1st:zysh entry num |
| Unable to change entry #%d! | 1st:zysh entry num |
| %s: cannot retrieve entries from table! | 1st:zysh table name |
| %s: invalid old/new index! | 1st:zysh table name |
| Unable to move entry #%d! | 1st:zysh entry num |
| %s: apply failed at initial stage! | 1st:zysh table name |
| %s: apply failed at main stage! | 1st:zysh table name |
| %s: apply failed at closing stage! | 1st:zysh table name |

**Table 291** ADP Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| from <zone> to <zone> [type=<type>] <message> , Action: <action>, Severity: <severity> | The ZyWALL detected an anomaly in traffic traveling between the specified zones.<br>The <type> = {scan-detection(<attack>) \| flood-detection(<attack>) \| http-inspection(<attack>) \| tcp-decoder(<attack>)}.<br>The <message> gives details about the attack, although the message is dropped if the log is more than 128 characters.<br>The <action> is what the ZyWALL did with the packet.<br>The <severity> is the threat level (very low, low, medium, high, or severe). |
| Enable ADP succeeded. | ADP was turned on. |
| Disable ADP succeeded. | ADP was turned off. |
| ADP rule <num> has been deleted. | The specified ADP rule has been deleted. |
| ADP rule <num> has been moved to <num>. | The ADP rule with the specified index number (first num) was moved to the specified index number (second num). |
| New ADP rule has been appended. | An ADP rule has been added to the end of the list. |
| ADP rule <num> has been inserted. | An ADP rule has been inserted. <num> is the number of the new rule. |
| ADP rule <num> has been modified. | The ADP rule of the specified number has been changed. |
| ADP profile <name> has been deleted. | The ADP rule with the specified name has been removed. |
| ADP profile <name> has been changed to <name>. | An ADP rule's name has been changed from first <name> to the second <name>. |
| ADP profile <name> has been created. | An ADP profile with the specified name has been added. |
| ADP profile <name> has been modified. | The ADP rule with the specified name has been changed. |
| Packet payload length is over the maximum system handle length | The ZyWALL's ADP feature detected a packet with a length over 16000 bytes. |
| LAND attack packet. Source IP is the same as Destination IP. | The ZyWALL's ADP feature detected traffic with the same IP address set as both the source and the destination. |

**Table 292** Anti-Virus Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Initializing Anti-Virus signature reference table has failed. | The ZyWALL failed to initialize the anti-virus signatures due to an internal error. |
| Reloading Anti-Virus signature database has failed. | The ZyWALL failed to reload the anti-virus signatures due to an internal error. |
| Reloading Anti-Virus signature reference table has failed. | The ZyWALL failed to reload the anti-virus signatures due to an internal error. |
| %s Virus infected - ID:%d,%s,%s. | The ZyWALL's anti-virus feature detected a virus-infected file.<br>1st %s: The protocol of the infected packet.<br>2nd %d: virus ID<br>3rd %s: name of the virus<br>4th %s: name of the infected file |
| %s, due to over maximum compressed file, %s could not be decompressed. | The ZyWALL could not decompress a compressed file because there were too many compressed files at the same time.<br>1st %s: The protocol of the packet.<br>2nd %s: The filename of the related file. |
| %s, due to more than one layer compressed file, %s could not be decompressed. | The ZyWALL could not decompress a compressed file because it contained other compressed files.<br>1st %s: The protocol of the packet.<br>2nd %s: The filename of the related file. |
| %s, due to password protected compressed file, %s could not be decompressed. | The ZyWALL could not decompress a compressed file because it had password protection.<br>1st %s: The protocol of the packet.<br>2nd %s: The filename of the related file. |
| %s, %s matched White-List %s | A file matched a file pattern in the anti-virus white list.<br>1st %s: The protocol of the packet.<br>2nd %s: The filename of the related file.<br>3rd %s: The file pattern that the file matched. |
| %s, %s matched the Black-List %s | A file matched a file pattern in the anti-virus black list.<br>1st %s: The protocol of the packet.<br>2nd %s: The filename of the related file.<br>3rd %s: The file pattern that the file matched. |

**Table 292** Anti-Virus Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| AV signature update has failed. Can not update last update time. | The anti-virus signatures update did not succeed. |
| AV signature update has failed. (Replacement failure) | Anti-virus signatures update failed because the ZyWALL was not able to replace the old set of anti-virus signatures with the new one. |
| AV signature update has failed. (Unknown signature package). | Anti-virus signatures update failed because the ZyWALL was not able to identify whether the downloaded signature package was an incremental or full update. |
| AV signature update from version %s to version %s has succeeded | The ZyWALL updated the anti-virus signatures from the listed version to the second listed version. |
| AV signature update has failed. (File damaged) | An anti-virus signatures update failed because the signature file has been corrupted. |
| AV signature update has failed. (Memory not enough) | An anti-virus signatures update failed because the ZyWALL did not have enough system resources free to finish the signature update. |
| AV signature size is over system limitation | An anti-virus signatures update failed because the anti-virus signature file was too large. |
| AV signature update has failed. | An anti-virus signatures update failed for unknown reasons. |
| Anti-Virus signatures missing, refer to your user documentation to recover the default database file. | When the ZyWALL started it could not find the anti-virus signature file. See the CLI reference guide for how to restore the default system database. |
| Update signature version has failed. | An attempt to update the anti-virus signature version failed.<br>cannot update signature version |
| AV signature update from %s version %s to %s version %s has succeeded. | The anti-virus signatures have been updated.<br>1st %s: The anti-virus engine type before the update.<br>2nd %s: The signature version before the update.<br>3rd %s: The anti-virus engine type after the update.<br>4th %s: The signature version after the update. |
| AV signature size is over system limitation | The anti-virus signature file size is too large. |
| AV has been activated | Anti-virus has been turned on. |
| AV has been deactivated | Anti-virus has been turned off. |
| Anti-Virus rule %d has been moved to %d | The anti-virus rule with the specified index number (1st %d) was moved to the specified index number (2nd %d). |
| Anti-Virus rules have been flushed. | All of the anti-virus rules have been deleted. |
| Anti-Virus rule %d has been deleted. | The anti-virus rule of the specified number has been deleted. |

**Table 292** Anti-Virus Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Anti-Virus rule %d has been modified. | The anti-virus rule of the specified number has been changed. |
| Anti-Virus rule %d has been inserted. | An anti-virus rule has been inserted. %d is the number of the new rule. |
| Anti-Virus rule %d has been appended. | The anti-virus rule with the listed number (%d) has been added to the end of the list. |
| File pattern %s has been modified to %s in %s | A anti-virus file pattern was changed in the white list or the black list.<br>1st%s: The original file pattern.<br>2ed %s: The new file pattern.<br>3rd %s The white list or black list. |
| File pattern %s has been deleted from %s | An anti-virus file pattern was deleted from the white or black list.<br>1st %s: The file pattern.<br>2nd %s: The white list or black list. |
| File pattern %s has been added in %s | An anti-virus file pattern was added to the white or black list.<br>1st %s: The file pattern.<br>2nd %s: The white list or black list. |
| %s has been %s | An anti-virus file pattern white list or black list was turned on or off.<br>1st %s: The white list or black list.<br>2nd %s: Activated/deactivated. |
| %s, due to decompress malfunction, %s could not be decompressed. Action on file: %s | File decompression failed due to an internal error.<br>1st %s: The protocol of the packet.<br>2nd %s: The filename of the related file.<br>3rd %s: Whether the file was deleted (DESTROY) or forwarded (PASS). |
| Update signature info has failed. | Updating of the signature file information failed due to an internal error. |

**Table 293** User Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| %s %s from %s has logged in ZyWALL | A user logged into the ZyWALL.<br>1st %s: The type of user account.<br>2nd %s: The user's user name.<br>3rd %s: The name of the service the user is using (HTTP, HTTPS, FTP, Telnet, SSH, or console). |
| %s %s from %s has logged out ZyWALL | A user logged out of the ZyWALL.<br>1st %s: The type of user account.<br>2nd %s: The user's user name.<br>3rd %s: The name of the service the user is using (HTTP, HTTPS, FTP, Telnet, SSH, or console). |
| %s %s from %s has been logged out ZyWALL (re-auth timeout) | The ZyWALL is signing the specified user out due to a re-authentication timeout.<br>1st %s: The type of user account.<br>2nd %s: The user's user name.<br>3rd %s: The name of the service the user is using (HTTP, HTTPS, FTP, Telnet, SSH, or console). |
| %s %s from %s has been logged out ZyWALL (lease timeout) | The ZyWALL is signing the specified user out due to a lease timeout.<br>1st %s: The type of user account.<br>2nd %s: The user's user name.<br>3rd %s: The name of the service the user is using (HTTP, HTTPS, FTP, Telnet, SSH, or console). |
| %s %s from %s has been logged out ZyWALL (idle timeout) | The ZyWALL is signing the specified user out due to an idle timeout.<br>1st %s: The type of user account.<br>2nd %s: The user's user name.<br>3rd %s: The name of the service the user is using (HTTP, HTTPS, FTP, Telnet, SSH, or console). |
| Console has been put into lockout state | Too many failed login attempts were made on the console port so the ZyWALL is blocking login attempts on the console port. |
| Address %u.%u.%u.%u has been put into lockout state | Too many failed login attempts were made from an IP address so the ZyWALL is blocking login attempts from that IP address.<br>%u.%u.%u.%u: the source address of the user's login attempt |

**Table 293** User Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Failed login attempt to ZyWALL from %s (login on a lockout address) | A login attempt came from an IP address that the ZyWALL has locked out.<br>%u.%u.%u.%u: the source address of the user's login attempt |
| Failed login attempt to ZyWALL from %s (reach the max. number of user) | The ZyWALL blocked a login because the maximum login capacity for the particular service has already been reached.<br>%s: service name |
| Failed login attempt to ZyWALL from %s (reach the max. number of simultaneous logon) | The ZyWALL blocked a login because the maximum simultaneous login capacity for the administrator or access account has already been reached.<br>%s: service name |
| User %s has been denied access from %s | The ZyWALL blocked a login according to the access control configuration.<br>%s: service name |
| User %s has been denied access from %s | The ZyWALL blocked a login attempt by the specified user name because of an invalid user name or password.<br>2nd %s: service name |

**Table 294** myZyXEL.com Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Send registration message to MyZyXEL.com server has failed. | The device was not able to send a registration message to MyZyXEL.com. |
| Get server response has failed. | The device sent packets to the MyZyXEL.com server, but did not receive a response. The root cause may be that the connection is abnormal. |
| Timeout for get server response. | zysh need to catch MyZyXEL.com agent's return code, this log will be shown when timeout. |
| User has existed. | The user name already exists in MyZyXEL.com's database. So the user can't use it for device registration and needs to specify another one. |
| User does not exist. | The user name does not yet exist in MyZyXEL.com's database. So the user can use it for device registration. |
| Internal server error. | MyZyXEL.com's database had an error when checking the user name. |
| Device registration has failed:%s. | Device registration failed, an error message returned by the MyZyXEL.com server will be appended to this log.<br>%s: error message returned by the myZyXEL.com server |
| Device registration has succeeded. | The device registered successfully with the myZyXEL.com server. |

**Table 294** myZyXEL.com Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Registration has failed. Because of lack must fields. | The device received an incomplete response from the myZyXEL.com server and it caused a parsing error for the device. |
| %s:Trial service activation has failed:%s. | Trail service activation failed for the specified service, an error message returned by the MyZyXEL.com server will be appended to this log.<br>1st %s: service name<br>2nd %s: error message returned by the myZyXEL.com server |
| %s:Trial service activation has succeeded. | Trail service was activated successfully for the specified service.<br>%s: service name |
| Trial service activation has failed. Because of lack must fields. | The device received an incomplete response from the myZyXEL.com server and it caused a parsing error for the device. |
| Standard service activation has failed:%s. | Standard service activation failed, this log will append an error message returned by the MyZyXEL.com server.<br>%s: error message returned by the myZyXEL.com server |
| Standard service activation has succeeded. | Standard service activation has succeeded. |
| Standard service activation has failed. Because of lack must fields. | The device received an incomplete response from the myZyXEL.com server and it caused a parsing error for the device. |
| Service expiration check has failed:%s. | The service expiration day check failed, this log will append an error message returned by the MyZyXEL.com server.<br>%s: error message returned by myZyXEL.com server |
| Service expiration check has succeeded. | The service expiration day check was successful. |
| Service expiration check has failed. Because of lack must fields. | The device received an incomplete response from the myZyXEL.com server and it caused a parsing error for the device. |
| Server setting error. | The device could not retrieve the myZyXEL.com server's IP address or FQDN from local. |
| Resolve server IP has failed. | The device could not resolve the myZyXEL.com server's FQDN to an IP address through gethostbyname(). |
| Verify server's certificate has failed. | The device could not process an HTTPS connection because it could not verify the myZyXEL.com server's certificate. |
| Connect to MyZyXEL.com server has failed. | The device could not connect to the MyZyXEL.com server. |
| Do account check. | The device started to check whether or not the user name in MyZyXEL.com's database. |

**Table 294** myZyXEL.com Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Do device register. | The device started device registration. |
| Do trial service activation. | The device started trail service activation. |
| Do standard service activation. | The device started standard service activation. |
| Do expiration check. | The device started the service expiration day check. |
| Build query message has failed. | Some information was missing in the packets that the device sent to the MyZyXEL.com server. |
| Parse receive message has failed. | The device cannot parse the response returned by the MyZyXEL.com server. Maybe some required fields are missing. |
| Change Anti-Virus engine. | The device started to change the type of anti-virus engine. |
| Change Anti-Virus engine has failed:%s. | The device failed to change the type of anti-virus engine. %s is the server response error message. |
| Change Anti-Virus engine has succeeded. | The device successfully changed the type of anti-virus engine. |
| Change Anti-Virus engine type has failed. Because of lack must fields. | The device failed to change the type of anti-virus engine because the response from the server is missing required fields. |
| Resolve server IP has failed. Update stop. | The update has stopped because the device couldn't resolve the myZyXEL.com server's FQDN to an IP address through gethostbyname(). |
| Verify server's certificate has failed. Update stop. | The device could not process an HTTPS connection because it could not verify the myZyXEL.com server's certificate. The update has stopped. |
| Send download request to update server has failed. | The device's attempt to send a download message to the update server failed. |
| Get server response has failed. | The device sent packets to the MyZyXEL.com server, but did not receive a response. The root cause may be that the connection is abnormal. |
| Timeout for get server response. | zysh need to catch MyZyXEL.com agent's return code, this log will be shown when timeout. |
| Send update request to update server has failed. | The device could not send an update message to the update server. |
| Update has failed. Because of lack must fields. | The device received an incomplete response from the update server and it caused a parsing error for the device. |
| Update server is busy now. File download after %d seconds. | The update server was busy so the device will wait for the specified number of seconds and send the download request to the update server again. |
| Device has latest file. No need to update. | The device already has the latest version of the file so no update is needed. |

**Table 294** myZyXEL.com Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Device has latest signature file; no need to update | The device already has the latest version of the signature file so no update is needed. |
| Connect to update server has failed. | The device cannot connect to the update server. |
| Wrong format for packets received. | The device cannot parse the response returned by the server. Maybe some required fields are missing. |
| Server setting error. Update stop. | The device could not resolve the update server's FQDN to an IP address through gethostbyname(). The update process stopped. |
| Build query message failed. | Some information was missing in the packets that the device sent to the server. |
| Starting signature update. | The device started an IDP signature update. |
| IDP signature download has succeeded. | The device successfully downloaded an IDP signature file. |
| IDP signature update has succeeded. | The device successfully downloaded and applied an IDP signature file. |
| IDP signature download has failed. | The device still cannot download the IDP signature after 3 retries. |
| Anti-Virus signature download has succeeded. | The device successfully downloaded an anti-virus signature file. |
| Anti-Virus signature update has succeeded. | The device successfully downloaded and applied an anti-virus signature file. |
| Anti-Virus signature download has failed. | The device still cannot download the anti-virus signature after 3 retries. |
| System protect signature download has succeeded. | The device successfully downloaded the system protect signature file. |
| System protect signature update has succeeded. | The device successfully downloaded and applied a system protect signature file. |
| System protect signature download has failed. | The device still cannot download the system protect signature file after 3 retries. |
| Resolve server IP has failed. | The device could not resolve the myZyXEL.com server's FQDN to an IP address through gethostbyname(). |
| Connect to MyZyXEL.com server has failed. | The device could not connect to the MyZyXEL.com server. |
| Build query message has failed. | Some information was missing in the packets that the device sent to the server. |
| Verify server's certificate has failed. | The device could not process an HTTPS connection because it could not verify the server's certificate. |

**Table 294** myZyXEL.com Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Get server response has failed. | The device sent packets to the server, but did not receive a response. The root cause may be that the connection is abnormal. |
| Expiration daily-check has failed:%s. | The daily check for service expiration failed, an error message returned by the MyZyXEL.com server will be appended to this log.<br>%s: error message returned by myZyXEL.com server |
| Do expiration daily-check has failed. Because of lack must fields. | The device received an incomplete response to the daily service expiration check and the packets caused a parsing error for the device. |
| Server setting error. | The device could not retrieve the server's IP address or FQDN from local. |
| Do expiration daily-check has failed. | The daily check for service expiration failed. |
| Do expiration daily-check has succeeded. | The daily check for service expiration was successful. |
| Expiration daily-check will trigger PPP interface. Do self-check. | Before the device sends an expiration day check packet, it needs to check whether or not it will trigger a PPP connection. |
| System bootup. Do expiration daily-check. | The device processes a service expiration day check immediately after it starts up. |
| After register. Do expiration daily-check immediately. | The device processes a service expiration day check immediately after device registration. |
| Time is up. Do expiration daily-check. | The processes a service expiration day check every 24 hrs. |
| Read MyZyXEL.com storage has failed. | Read data from EEPROM has failed. |
| Open /proc/MRD has failed. | This error message is shown when getting MAC address. |
| IDP service has expired. | The IDP service period has expired. The device can find this through either a service expiration day check via MyZyXEL.com server or by the device's own count. |
| Content-Filter service has expired. | The content filtering service period has expired. The device can find this through either a service expiration day check via MyZyXEL.com server or by the device's own count. |
| Unknown TLS/SSL version: %d. | The device only supports SSLv3 protocol. %d: SSL version assigned by client. |
| Load trusted root certificates has failed. | The device needs to load the trusted root certificate before the device can verify a server's certificate. This log displays if the device failed to load it. |
| Certificate has expired. | Verification of a server's certificate failed because it has expired. |

**Table 294** myZyXEL.com Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Self signed certificate. | Verification of a server's certificate failed because it is self-signed. |
| Self signed certificate in certificate chain. | Verification of a server's certificate failed because there is a self-signed certificate in the server's certificate chain. |
| Verify peer certificates has succeeded. | The device verified a server's certificate while processing an HTTPS connection. |
| Certification verification failed: Depth: %d, Error Number(%d):%s. | Verification of a server's certificate failed while processing an HTTPS connection. This log identifies the reason for the failure.<br>1st %d: certificate chain level<br>2nd %d: error number<br>%s: error message |
| Certificate issuer name:%s. | Verification of the specified certificate failed because the device could not get the certificate's issuer name. %s is the certificate name. |
| The wrong format for HTTP header. | The header format of a packet returned by a server is wrong. |
| Timeout for get server response. | After the device sent packets to a server, the device did not receive any response from the server. The root cause may be a network delay issue. |
| Download file size is wrong. | The file size downloaded for AS is not identical with content-length |
| Parse HTTP header has failed. | Device can't parse the HTTP header in a response returned by a server. Maybe some HTTP headers are missing. |

**Table 295** IDP Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| System internal error. Detect IDP engine status failed. | There was an internal system error. The device failed in checking whether or not IDP is activated. |
| System internal error. Enable IDP failed. | There was an internal system error. The device failed in turning on IDP. |
| System internal error. Disable IDP failed. | There was an internal system error. The device failed in turning off IDP. |
| Enable IDP succeeded. | The device turned on the use of the IDP signature file. |
| Disable IDP succeeded. | The device turned off the use of the IDP signature file. |
| Enable IDP engine failed. | The device failed to turn on the IDP engine. |
| Disable IDP engine failed. | The device failed to turn off the IDP engine. |

**Table 295** IDP Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Enable IDP engine succeeded. | The device turned on the IDP engine. |
| Disable IDP engine succeeded. | The device turned off the IDP engine. |
| IDP service is not registered. IDP will not be activated. | The IDP service could has not been turned on and the IDP signatures will not be updated because the IDP service is not registered. |
| IDP service standard license is expired. Update signature failed. | The IDP standard service license expired so the device cannot update the IDP signatures. |
| IDP service standard license is not registered. Update signature failed. | A IDP standard service license has not been registered. The device cannot update the IDP signatures. |
| IDP service trial license is expired. Update signature failed. | The IDP service trial license has expired. The device cannot update the IDP signatures. |
| IDP service trial license is not registered. Update signature failed. | The IDP service trial license has not been registered yet. The device cannot update the IDP signatures. |
| Custom signature add error: sid <sid>, <error_message>. | An attempt to add a custom IDP signature failed. The error sid and message are displayed. |
| Custom signature import error: line <line>, sid <sid>, <error_message>. | An attempt to import a custom IDP signature failed. The errored line number in the file, the error sid and error message are displayed. |
| Custom signature replace error: line <line>, sid <sid>, <error_message>. | Custom IDP signature replacing failed. Error line number of file, sid and message will be shown |
| Custom signature edit error: sid <sid>, <error_message>. | An attempt to edit a custom IDP signature failed. The error sid and message are displayed. |
| Custom signature more than <num>. Replacement custom signature number is <num>. | An attempt to replace a custom IDP signature failed. The maximum number of custom signatures (first num) and the number of the replacement signature (second num) display. |
| Custom signature more than <num>. Remaining custom signature number is <num. Adding custom signature number is <num>. | An attempt to add a custom IDP signature failed. The maximum number of custom signatures (first num), the number of remaining capacity for custom signatures (second num), and the number of the custom signature (third num) that was not added display. |
| Get custom signature number error. | The device failed to get the custom IDP signature number. |

**Table 295** IDP Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Add custom signature error: signature <sid> is over length. | An attempt to add a custom IDP signature failed because the signature's contents were too long. |
| Edit custom signature error: signature <sid> is over length. | An attempt to edit a custom IDP signature failed because the signature's contents were too long. |
| IDP off-line update failed. File damaged. | An update attempt for the IDP signatures failed. The signature file may be corrupt. |
| IDP signature update failed. File crashed. | An attempt to update the IDP signature file failed because the device could not decrypt the signature file. |
| IDP signature update failed. File damaged. | An attempt to update the IDP signature file failed because the device could not decompress the signature file. |
| IDP signature update failed. File update failed. | An attempt to update the IDP signatures failed. Updating the signature file failed. |
| IDP signature update failed. Can not update last update time. | An attempt to update the IDP signatures failed. Updating the time for the last signature file update failed. |
| IDP signature update failed. Can not update synchronized file. | An attempt to update the IDP signatures failed. Rebuilding of the IDP device HA synchronized file failed. |
| IDP signature update from version <version> to version <version> has succeeded. | An IDP signature update succeeded. The previous and updated IDP signature versions are listed. |
| IDP system-protect signature update from version <version> to version <version> has succeeded. | An update of the IDP system-protect signatures succeeded. The previous and updated signature versions are listed. |
| System-protect error. Create IDP debug directory failed | The IDP system-protect function had an error. Creation of the IDP debug directory failed. |
| System internal error. Create IDP statistics entry failed. | There was an internal system error. Creation of an IDP statistics entry failed. |
| System-protect error. Out of memory. IDP activation unchanged. | The IDP system-protect function had an error. The device did not have enough available memory. The setting for IDP activation has not changed. |
| System-protect error. Create IDP proc failed. IDP activation failed. | Activation of the IDP system-protect function failed due to an internal system error. |

**Table 295** IDP Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| from <zone> to <zone> [type=<type>] <message> , Action: <action>, Severity: <severity> | The ZyWALL detected an intrusion in traffic traveling between the specified zones.<br>The <type> = {scan-detection(<attack>) \| flood-detection(<attack>) \| http-inspection(<attack>) \| tcp-decoder(<attack>)}.<br>The <message> gives details about the attack, although the message is dropped if the log is more than 128 characters.<br>The <action is what the ZyWALL did with the packets.<br>The <severity> is the threat level (very low, low, medium, high, or severe). |
| Program DFA failed. | There was an internal system error. The IDP search engine failed. |
| IDP signature update failed. Fail to extract temporary file. | An attempt to update the IDP signatures failed because the device could not extract the signature package's temporary file. |
| IDP signature update failed. | An attempt to update the IDP signatures failed due to an internal system error. |
| IDP signature update failed. Invalid signature content. | An attempt to update the IDP signatures failed due to an internal system error. |
| System internal error. Create IDP traffic anomaly entry failed. | There was an internal system error. |
| Query signature version failed. | The device could not get the signature version from the new signature package it downloaded from the update server. |
| Can not get signature version. | The device could not get the signature version from the new signature package it downloaded from the update server. |
| IDP system-protect signature update failed. Invalid IDP config file. | An IDP system-protect signature update failed. |
| IDP system-protect signature update failed. Invalid signature content. | An IDP system-protect signature update failed. |
| Enable IDP system-protect succeeded. | The IDP system-protect feature was successfully turned on. |
| Disable IDP system-protect succeeded. | The IDP system-protect feature was successfully turned off. |
| Check duplicate sid failed. Allocate memory error. | Checking for duplicated signature IDs failed. There was an error while allocating memory. |
| Check duplicate sid failed. Open file error. | Checking for duplicated signature IDs failed. Opening a temporary file failed. |

**Table 295** IDP Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Duplicate sid <sid> in import file at line <linenum>. | The listed signature ID is duplicated at the listed line number in the signature file. |
| IDP rule <num> has been deleted. | The listed IDP rule has been removed. |
| IDP rule <num> has been moved to <num>. | The IDP rule with the specified index number (first num) was moved to the specified index number (second num). |
| New IDP rule has been appended. | An IDP rule has been added to the end of the list. |
| IDP rule <num> has been inserted. | An IDP rule has been inserted. <num> is the number of the new rule. |
| IDP rule <num> has been modified. | The IDP rule of the specified number has been changed. |
| IDP profile <name> has been deleted. | The IDP profile with the specified name has been removed. |
| IDP profile <name> has been changed to <name>. | An IDP profile's name has been changed from first <name> to the second <name>. |
| IDP profile <name> has been created. | The IDP profile with the specified name has been added. |
| IDP profile <name> has been modified. | IDP profile has been modified. <name> is profile name. |
| IDP signatures missing, please refer to your user documentation to recover the default database file | When the ZyWALL started it could not find the IDP signature file. See the CLI reference guide for how to restore the default system database. |
| IDP signature size is over system limitation. | The IDP signature set is too large (exceeds the ZyWALL's system limitation). |

**Table 296** Application Patrol

| MESSAGE | EXPLANATION |
|---|---|
| Service=%s Mode=%s Rule=%s Access=%s | Common packet logging. 1st %s: Protocol Name, 2nd %s: "port-less" or "port-base", 3rd %s: Rule Index, 4th %s: "forward", "drop" or "reject". |
| Service=%s Rule=%s Action=%s Access=drop | Special packet logging for IM action. 1st %s: Protocol Name, 2nd %s: "port-less" or "port-base", 3rd %s: "login", "message", "audio", "video" or "file-transfer". |
| Initialize App. Patrol has succeeded. | Application patrol was successfully initiated. |
| Rule %s:%s has been modified | An application patrol rule has been modified. 1st %s: Protocol Name, 2nd: Rule Index. |
| App. Patrol has been activated. | Application patrol was turned on. |
| App. Patrol has been deactivated. | Application patrol was turned off. |

**Table 296** Application Patrol (continued)

| MESSAGE | EXPLANATION |
|---|---|
| Protocol %s has been enabled. | The listed protocol has been turned on in the application patrol. |
| Protocol %s has been disabled. | The listed protocol has been turned off in the application patrol. |
| Classification mode of protocol %s has been modified to portless. | The device will now use the portless classification mode to identify the listed protocol's traffic. |
| Classification mode of protocol %s has been modified to portbase. | The device will now use the port-based classification mode to identify the listed protocol's traffic. |
| Bandwidth graph of protocol %s has been enabled. | The bandwidth graph has been turned on for the listed protocol's traffic. |
| Bandwidth graph of protocol %s has been disabled. | The bandwidth graph has been turned off for the listed protocol's traffic. |
| Default port %s of protocol %s has been added. | The listed default port (first %s) has been added for the listed protocol (second %s). |
| Default port %s of protocol %s has been removed. | The listed default port (first %s) has been deleted for the listed protocol (second %s). |
| Rule %s:%s has been moved to index %s. | An application patrol rule has been moved.<br>1st %s: Protocol name<br>2nd %s: From rule index number<br>3rd %s: To rule index number |
| Rule %s:%s has been removed. | An application patrol rule has been deleted.<br>1st %s: Protocol name<br>2nd %s: From rule index number<br>3rd %s: To rule index number |
| System fatal error: 60011001. | The device failed to initiate the application patrol daemon. |
| System fatal error: 60011002. | The device failed to get the application patrol protocol list. |
| System fatal error: 60011003. | The device failed to initiate XML. |
| System fatal error: 60011004. | The device failed to turn application patrol off while the system was initiating. |

**Table 297** IKE Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Peer has not announced DPD capability | The remote IPSec router has not announced its dead peer detection (DPD) capability to this device. |
| [COOKIE] Invalid cookie, no sa found | Cannot find SA according to the cookie. |
| [DPD] No response from peer. Using existing Phase-1 SA in %u seconds. Trying with Phase-1 rekey. | The device's DPD feature has not detected a response from the remote IPSec router. %u is the retry time. |
| [HASH] : Tunnel [%s] Phase 1 hash mismatch | %s is the tunnel name. When negotiating Phase-1, the exchange hash did not match. |
| [HASH] : Tunnel [%s] Phase 2 hash mismatch" | %s is the tunnel name. When negotiating Phase-2, the calculated quick mode authentication hash did not match. |
| [ID] : Invalid ID information | ID payload is not valid (in Phase-1 is local/peer ID, in Phase-2 is local/remote policy). |
| [ID] : Tunnel [%s] Local IP mismatch | %s is the tunnel name. When negotiating Phase-1, the local tunnel IP did not match the My IP in VPN gateway. |
| [ID] : Tunnel [%s] My IP mismatch | %s is the tunnel name. When negotiating Phase-1 and selecting matched proposal, My IP Address could not be resolved. |
| [ID] : Tunnel [%s] Phase 1 ID mismatch | %s is the tunnel name. When negotiating Phase-1, the peer ID did not match. |
| [ID] : Tunnel [%s] Phase 2 Local ID mismatch | %s is the tunnel name. When negotiating Phase-2 and checking IPsec SAs or the ID is IPv6 ID. |
| [ID] : Tunnel [%s] Phase 2 Remote ID mismatch | %s is the tunnel name. When negotiating Phase-2 and checking IPsec SAs or the ID is IPv6 ID. |
| [ID] : Tunnel [%s] Remote IP mismatch | %s is the tunnel name. When negotiating Phase-1, the peer tunnel IP did not match the secure gateway address in VPN gateway. |
| [SA] : Malformed IPSec SA proposal | When selecting a matched proposal, some protocol was given more than once. |
| [SA] : No proposal chosen | When selecting a matched proposal in phase-1 or phase-2, so proposal was selected. |
| [SA] : Tunnel [%s] Phase 1 authentication algorithm mismatch | %s is the tunnel name. When negotiating Phase-1, the authentication algorithm did not match. |
| [SA] : Tunnel [%s] Phase 1 authentication method mismatch | %s is the tunnel name. When negotiating Phase-1, the authentication method did not match. |
| [SA] : Tunnel [%s] Phase 1 encryption algorithm mismatch | %s is the tunnel name. When negotiating Phase-1, the encryption algorithm did not match. |

**Table 297** IKE Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| [SA] : Tunnel [%s] Phase 1 invalid protocol | %s is the tunnel name. When negotiating Phase-1, the packet was not a ISKAMP packet in the protocol field. |
| [SA] : Tunnel [%s] Phase 1 invalid transform | %s is the tunnel name. When negotiating Phase-1, the transform ID was invalid. |
| [SA] : Tunnel [%s] Phase 1 key group mismatch | %s is the tunnel name. When negotiating Phase-1, the DH group of the attribute list `attrs' did not match the security policy. |
| [SA] : Tunnel [%s] Phase 1 negotiation mode mismatch | %s is the tunnel name. When negotiating Phase-1, the negotiation mode did not match. |
| [SA] : Tunnel [%s] Phase 2 authentication algorithm mismatch | %s is the tunnel name. When negotiating Phase-2, the authentication algorithm did not match. |
| [SA] : Tunnel [%s] Phase 2 encapsulation mismatch | %s is the tunnel name. When negotiating Phase-2, the encapsulation did not match. |
| [SA] : Tunnel [%s] Phase 2 encryption algorithm mismatch | %s is the tunnel name. When negotiating Phase-2, the encryption algorithm did not match. |
| [SA] : Tunnel [%s] Phase 2 pfs mismatch | %s is the tunnel name. When negotiating Phase-2, the PFS specified did not match. |
| [SA] : Tunnel [%s] Phase 2 pfs unsupported: %d | %s is the tunnel name. When negotiating Phase-2, this device does not support the PFS specified. |
| [SA] : Tunnel [%s] Phase 2 SA encapsulation mismatch | %s is the tunnel name. When negotiating Phase-2, the SA encapsulation did not match. |
| [SA] : Tunnel [%s] Phase 2 SA protocol mismatch | %s is the tunnel name. When negotiating Phase-2, the SA protocol did not match. |
| [SA] : Tunnel [%s] SA sequence size mismatch | %s is the tunnel name. When negotiating Phase-2, the SA sequence size did not match. |
| [XCHG] exchange type is not IP, AGGR, or INFO | This device is the responder and this is the initiator's first packet, but exchange type is not IP, AGGR, or INFO and the packet is ignored. |
| Cannot resolve My IP Addr %s for Tunnel [%s] | 1st %s is my ip address. 2nd %s is the tunnel name. When selecting a matched proposal in phase-1, the engine could not get My-IP address. |
| Cannot resolve Secure Gateway Addr %s for Tunnel [%s] | 1st %s is my ip address. 2nd %s is the tunnel name; When selecting a matched proposal in phase-1, the engine could not get the correct secure gateway address. |
| Could not dial dynamic tunnel "%s" | %s is the tunnel name. The tunnel is a dynamic tunnel and the device cannot dial it. |
| Could not dial incomplete tunnel "%s" | %s is the tunnel name. The tunnel setting is not complete. |

**Table 297** IKE Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Could not dial manual key tunnel "%s" | %s is the tunnel name. The manual key tunnel cannot be dialed. |
| DPD response with invalid ID | When receiving a DPD response with invalid ID ignored. |
| DPD response with no active request | When receiving a DPD response with no active query. |
| IKE Packet Retransmit | When retransmitting the IKE packets. |
| Phase 1 IKE SA process done | When Phase 1 negotiation is complete. |
| Recv Main Mode request from [%s] | %s is the remote name; When receiving a request to enter Main mode. |
| Recv Aggressive Mode request from [%s] | %s is the remote name; When receiving a request to enter Aggressive mode. |
| Recv:[SA][KE][ID][CERT][CR][HASH][SIG][NONCE][DEL][VID][ATTR][NOTFY:%s] | This is a combined message for incoming IKE packets |
| Send Main Mode request to [%s] | %s is the remote name. The device sent a request to enter Main Mode. |
| Send Aggressive Mode request to [%s] | %s is the remote name. The device sent a request to enter Aggressive Mode. |
| Send:[SA][KE][ID][CERT][CR][HASH][SIG][NONCE][DEL][VID][ATTR][NOTFY:%s] | This is a combined message for outgoing IKE packets. |
| Start Phase 2: Quick Mode | Indicates the beginning of phase 2 using quick mode. |
| The cookie pair is : 0x%08x%08x / 0x%08x%08x | Indicates the initiator/responder cookie pair. |
| The IPSec tunnel "%s" is already established | %s is the tunnel name. When dialing a tunnel, the tunnel is already dialed. |
| Tunnel [%s] built successfully | %s is the tunnel name. The phase-2 tunnel negotiation is complete. |
| Tunnel [%s] Phase 1 pre-shared key mismatch | %s is the tunnel name. When negotiating phase-1, the pre-shared key did not match. |
| Tunnel [%s] Recving IKE request | %s is the tunnel name. The device received an IKE request. |
| Tunnel [%s] Sending IKE request | %s is the tunnel name. The device sent an IKE request. |
| Tunnel [%s] IKE Negotiation is in process | %s is the tunnel name. When IKE request is already sent but still attempting to dial a tunnel. |
| VPN gateway %s was disabled | %s is the gateway name. An administrator disabled the VPN gateway. |

**Table 297** IKE Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| VPN gateway %s was enabled | %s is the gateway name. An administrator enabled the VPN gateway. |
| XAUTH fail! My name: %s | %s is the my xauth name. This indicates that my name is invalid. |
| XAUTH fail! Remote user: %s | %s is the remote xauth name. This indicates that a remote user's name is invalid. |
| XAUTH succeed! My name: %s | %s is the my xauth name. This indicates that my name is valid. |
| XAUTH succeed! Remote user: %s | %s is the remote xauth name. This indicate that a remote user's name is valid |
| Dynamic Tunnel [%s:%s:0x%x:%s] built successfully | The variables represent the phase 1 name, tunnel name, SPI and the xauth name (optional). The phase-2 tunnel negotiation is complete. |
| Dynamic Tunnel [%s:%s:0x%x:0x%x:%s] rekeyed successfully | The variables represent the phase 1 name, tunnel name, old SPI, new SPI and the xauth name (optional). The tunnel was rekeyed successfully. |
| Tunnel [%s:%s:0x%x:%s] built successfully | The variables represent the phase 1 name, tunnel name, SPI and the xauth name (optional). The phase-2 tunnel negotiation is complete. |
| Tunnel [%s:%s:0x%x:0x%x:%s] rekeyed successfully | The variables represent the phase 1 name, tunnel name, old SPI, new SPI and the xauth name (optional). The tunnel was rekeyed successfully. |
| Tunnel [%s:%s] Phase 1 pre-shared key mismatch | The variables represent the phase 1 name and tunnel name. When negotiating phase-1, the pre-shared keys did not match. |
| Tunnel [%s:%s] Recving IKE request | The variables represent the phase 1 name and tunnel name. The device received an IKE request. |
| Tunnel [%s:%s] Sending IKE request | The variables represent the phase 1 name and tunnel name. The device sent an IKE request. |
| Tunnel [%s:0x%x] is disconnected | The variables represent the tunnel name and the SPI of a tunnel that was disconnected. |
| Tunnel [%s] rekeyed successfully | %s is the tunnel name. The tunnel was rekeyed successfully. |

**Table 298** IPSec Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Corrupt packet, Inbound transform operation fail | The device received corrupt IPsec packets and could not process them. |
| Encapsulated packet too big with length | An outgoing packet needed to be transformed but was longer than 65535. |
| Get inbound transform fail | When performing inbound processing for incoming IPSEC packets and ICMPs related to them, the engine cannot obtain the transform context. |

**Table 298** IPSec Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Get outbound transform fail | When outgoing packet need to be transformed, the engine cannot obtain the transform context. |
| Inbound transform operation fail | After encryption or hardware accelerated processing, the hardware accelerator dropped a packet (resource shortage, corrupt packet, invalid MAC, and so on). |
| Outbound transform operation fail | After encryption or hardware accelerated processing, the hardware accelerator dropped a packet (e.g., resource overflow, corrupt packet, and so on). |
| Packet too big with Fragment Off | An outgoing packet needed to be transformed, but the fragment flag was off and the packet was too big. |
| SPI:0x%x SEQ:0x%x Execute transform step fail, ret=%d | The variables represent the SPI, sequence number and the error number. When trying to perform transforming, the engine returned an error. |
| SPI:0x%x SEQ:0x%x No rule found, Dropping packet | The variables represent the SPI and the sequence number. The packet did not match the tunnel policy and was dropped. |
| SPI:0x%x SEQ:0x%x Packet Anti-Replay detected | The variables represent the SPI and the sequence number. The device received a packet again (that it had already received). |
| VPN connection %s was disabled. | %s is the VPN connection name. An administrator disabled the VPN connection. |
| VPN connection %s was enabled. | %s is the VPN connection name. An administrator enabled the VPN connection. |
| Due to active connection allowed exceeded, %s was deleted. | %s is the VPN connection name. The number of active connections exceeded the maximum allowed. |

**Table 299** Firewall Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| priority:%lu, from %s to %s, service %s, %s | 1st variable is the global index of rule, 2nd is the from zone,<br>3rd is the to zone, 4th is the service name, 5th is ACCEPT/ DROP/REJECT. |
| %s:%d: in %s(): | Firewall is dead, trace to %s is which file, %d is which line, %s is which function |
| Firewall has been %s. | %s is enabled/disabled |
| Firewall rule %d has been moved to %d. | 1st %d is the old global index of rule, 2nd %d is the new global index of rule |
| Firewall rule %d has been deleted. | %d is the global index of rule |
| Firewall rules have been flushed. | Firewall rules were flushed |
| Firewall rule %d was %s. | %d is the global index of rule, %s is appended/inserted/ modified |

**Table 299** Firewall Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Firewall %s %s rule %d was %s. | 1st %s is from zone, 2nd %s is to zone, %d is the index of the rule<br>3rd %s is appended/inserted/modified |
| Firewall %s %s rule %d has been moved to %d. | 1st %s is from zone, 2nd %s is to zone, 1st %d is the old index of the rule<br>2nd %d is the new index of the rule |
| Firewall %s %s rule %d has been deleted. | 1st %s is from zone, 2nd %s is to zone, %d is the index of the rule |
| Firewall %s %s rules have been flushed. | 1st %s is from zone, 2nd %s is to zone |
| abnormal TCP flag attack detected | Abnormal TCP flag attack detected |
| invalid state detected | Invalid state detected |
| The Asymmetrical Route has been enabled. | Asymmetrical route has been turned on. |
| The Asymmetrical Route has been disabled. | Asymmetrical Route has been turned off. |

**Table 300** Sessions Limit Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Maximum sessions per host (%d) was exceeded. | %d is maximum sessions per host. |

**Table 301** Policy Route Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Can't open bwm_entries | Policy routing can't activate BWM feature. |
| Can't open link_down | Policy routing can't detect link up/down status. |
| Cannot get handle from UAM, user-aware PR is disabled | User-aware policy routing is disabled due to some reason. |
| mblock: allocate memory failed! | Allocating policy routing rule fails: insufficient memory. |
| pt: allocate memory failed! | Allocating policy routing rule fails: insufficient memory. |
| To send message to policy route daemon failed! | Failed to send control message to policy routing manager. |
| The policy route %d allocates memory fail! | Allocating policy routing rule fails: insufficient memory.<br>%d: the policy route rule number |

**Table 301** Policy Route Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| The policy route %d uses empty user group! | Use an empty object group.<br>%d: the policy route rule number |
| The policy route %d uses empty source address group! | Use an empty object group.<br>%d: the policy route rule number |
| The policy route %d uses empty destination address group! | Use an empty object group.<br>%d: the policy route rule number |
| The policy route %d uses empty service group | Use an empty object group.<br>%d: the policy route rule number |
| Policy-route rule %d was inserted. | Rules is inserted into system.<br>%d: the policy route rule number |
| Policy-route rule %d was appended. | Rules is appended into system.<br>%d: the policy route rule number |
| Policy-route rule %d was modified. | Rule is modified.<br>%d: the policy route rule number |
| Policy-route rule %d was moved to %d. | Rule is moved.<br>1st %d: the original policy route rule number<br>2nd %d: the new policy route rule number |
| Policy-route rule %d was deleted. | Rule is deleted.<br>%d: the policy route rule number |
| Policy-route rules were flushed. | Policy routing rules are cleared. |
| BWM has been activated. | The global setting for bandwidth management on the ZyWALL has been turned on. |
| BWM has been deactivated. | The global setting for bandwidth management on the ZyWALL has been turned off. |

**Table 302** Built-in Services Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| User on %u.%u.%u.%u has been denied access from %s | HTTP/HTTPS/TELNET/SSH/FTP/SNMP access to the device was denied.<br>%u.%u.%u.%u is IP address<br>%s is HTTP/HTTPS/SSH/SNMP/FTP/TELNET |
| HTTPS certificate:%s does not exist. HTTPS service will not work. | An administrator assigned a nonexistent certificate to HTTPS.<br>%s is certificate name assigned by user |

**Table 302** Built-in Services Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| HTTPS port has been changed to port %s. | An administrator changed the port number for HTTPS.<br>%s is port number |
| HTTPS port has been changed to default port. | An administrator changed the port number for HTTPS back to the default (443). |
| HTTP port has changed to port %s. | An administrator changed the port number for HTTP.<br>%s is port number assigned by user |
| HTTP port has changed to default port. | An administrator changed the port number for HTTP back to the default (80). |
| SSH port has been changed to port %s. | An administrator changed the port number for SSH.<br>%s is port number assigned by user |
| SSH port has been changed to default port. | An administrator changed the port number for SSH back to the default (22). |
| SSH certificate:%s does not exist. SSH service will not work. | An administrator assigned a nonexistent certificate to SSH.<br>%s is certificate name assigned by user |
| SSH certificate:%s format is wrong. SSH service will not work. | After an administrator assigns a certificate for SSH, the device needs to convert it to a key used for SSH.<br>%s is certificate name assigned by user |
| TELNET port has been changed to port %s. | An administrator changed the port number for TELNET.<br>%s is port number assigned by user |
| TELNET port has been changed to default port. | An administrator changed the port number for TELNET back to the default (23). |
| FTP certificate:%s does not exist. | An administrator assigned a nonexistent certificate to FTP.<br>%s is certificate name assigned by user |
| FTP port has been changed to port %s. | An administrator changed the port number for FTP.<br>%s is port number assigned by user |
| FTP port has been changed to default port. | An administrator changed the port number for FTP back to the default (21). |
| SNMP port has been changed to port %s. | An administrator changed the port number for SNMP.<br>%s is port number assigned by user |
| SNMP port has been changed to default port. | An administrator changed the port number for SNMP back to the default (161). |
| Console baud has been changed to %s. | An administrator changed the console port baud rate.<br>%s is baud rate assigned by user |

**Table 302** Built-in Services Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Console baud has been reset to %d. | An administrator changed the console port baud rate back to the default (115200).<br>%d is default baud rate |
| DHCP Server on Interface %s will not work due to Device HA status is Stand-By | If interface is stand-by mode for device HA, DHCP server can't be run. Otherwise it has conflict with the interface in master mode.<br>%s is interface name |
| DHCP Server on Interface %s will be reapplied due to Device HA status is Active | When an interface has become the HA master, the DHCP server needs to start operating.<br>%s is interface name |
| DHCP's DNS option:%s has changed. | DHCP pool's DNS option support from WAN interface. If this interface is unlink/disconnect or link/connect, this log will be shown.<br>%s is interface name. The DNS option of DHCP pool has retrieved from it |
| Set timezone to %s. | An administrator changed the time zone.<br>%s is time zone value |
| Set timezone to default. | An administrator changed the time zone back to the default (0). |
| Enable daylight saving. | An administrator turned on daylight saving. |
| Disable daylight saving. | An administrator turned off daylight saving. |
| DNS access control rules have been reached the maximum number. | An administrator tried to add more than the maximum number of DNS access control rules (64). |
| DNS access control rule %u of DNS has been appended. | An administrator added a new rule.<br>%u is rule number |
| DNS access control rule %u has been inserted. | An administrator inserted a new rule.<br>%u is rule number |
| DNS access control rule %u has been appended | An administrator appended a new rule.<br>%u is rule number |
| DNS access control rule %u has been modified | An administrator modified the rule %u.<br>%u is rule number |
| DNS access control rule %u has been deleted. | An administrator removed the rule %u.<br>%u is rule number |

**Table 302** Built-in Services Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| DNS access control rule %u has been moved to %d. | An administrator moved the rule %u to index %d.<br>%u is previous index<br>%d variable is current index |
| The default record of Zone Forwarder have reached the maximum number of 128 DNS servers. | The default record DNS servers is more than 128. |
| Interface %s ping check is successful. Zone Forwarder adds DNS servers in records. | Ping check ok, add DNS servers in bind.<br>%s is interface name |
| Interface %s ping check is failed. Zone Forwarder removes DNS servers in records. | Ping check failed, remove DNS servers from bind.<br>%s is interface name |
| Interface %s ping check is disabled. Zone Forwarder adds DNS servers in records. | Ping check disabled, add DNS servers in bind.<br>%s is interface name |
| Wizard apply DNS server failed. | Wizard apply DNS server failed. |
| Wizard adds DNS server %s failed because DNS zone setting has conflictd. | Wizard apply DNS server failed because DNS zone conflicted.<br>%s is the IP address of the DNS server |
| Wizard adds DNS server %s failed because Zone Forwarder numbers have reached the maximum number of 32. | Wizard apply DNS server fail because the device already has the maximum number of DNS records configured.<br>%s is IP address of the DNS server. |
| Access control rules of %s have reached the maximum number of %u | The maximum number of allowable rules has been reached.<br>%s is HTTP/HTTPS/SSH/SNMP/FTP/TELNET.<br>%u is the maximum number of access control rules. |
| Access control rule %u of %s was appended. | A new built-in service access control rule was appended.<br>%u is the index of the access control rule.<br>%s is HTTP/HTTPS/SSH/SNMP/FTP/TELNET. |
| Access control rule %u of %s was inserted. | An access control rule was inserted successfully.<br>%u is the index of the access control rule.<br>%s is HTTP/HTTPS/SSH/SNMP/FTP/TELNET. |

**Table 302** Built-in Services Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Access control rule %u of %s was modified. | An access control rule was modified successfully.<br>%u is the index of the access control rule.<br>%s is HTTP/HTTPS/SSH/SNMP/FTP/TELNET. |
| Access control rule %u of %s was deleted. | An access control rule was removed successfully.<br>%u is the index of the access control rule.<br>%s is HTTP/HTTPS/SSH/SNMP/FTP/TELNET. |
| Access control rule %d of %s was moved to %d. | An access control rule was moved successfully.<br>1st %d is the previous index .<br>%s is HTTP/HTTPS/SSH/SNMP/FTP/TELNET.<br>2nd %d is current previous index. |
| SNMP trap can not be sent successfully | Cannot send a SNMP trap to a remote host due to network error |

**Table 303** System Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Port %d is up!! | When LINK is up, %d is the port number. |
| Port %d is down!! | When LINK is down, %d is the port number. |
| %s is dead at %s | A daemon (process) is gone (was killed by the operating system).<br>1st %s: Daemon Name, 2nd %s: date and time |
| %s process count is incorrect at %s | The count of the listed process is incorrect.<br>1st %s: Daemon Name, 2nd %s: date and time |
| %s becomes Zombie at %s | A process is present but not functioning.<br>1st %s: Daemon Name, 2nd %s: date and time<br>When memory usage exceed threshold-max, memory usage reaches %d%% :mem-threshold-max.<br>When local storage usage exceeds threshold-max, %s: Partition name file system usage reaches %d%%: disk-threshold-max.<br>When memory usage drops below threshold-min, System Memory usage drops below the threshold of %d%%: mem-threshold-min.<br>When local storage usage drops below threshold-min, %s: partition_name file system drops below the threshold of %d%%: disk-threshold-min. |
| DHCP Server executed with cautious mode enabled | DHCP Server executed with cautious mode enabled. |

**Table 303** System Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| DHCP Server executed with cautious mode disabled | DHCP Server executed with cautious mode disabled. |
| Received packet is not an ARP response packet | A packet was received but it is not an ARP response packet. |
| Receive an ARP response | The device received an ARP response. |
| Receive ARP response from %s (%s) | The device received an ARP response from the listed source. |
| The request IP is: %s, sent from %s | The device accepted a request. |
| Received ARP response NOT for the request IP address | The device received an ARP response that is NOT for the requested IP address. |
| Receive an ARP response from the client issuing the DHCP request | The device received an ARP response from the client issuing the DHCP request. |
| Receive an ARP response from an unknown client | The device received an ARP response from an unknown client. |
| In total, received %d arp response packets for the requested IP address | The device received the specified total number of ARP response packets for the requested IP address. |
| Clear arp cache successfully. | The ARP cache was cleared successfully. |
| Client MAC address is not an Ethernet address | A client MAC address is not an Ethernet address. |
| DHCP request received via interface %s (%s:%s), src_mac: %s with requested IP: %s | The device received a DHCP request through the specified interface. |
| IP confliction is detected. Send back DHCP-NAK. | IP conflict was detected. Send back DHCP-NAK. |
| Clear ARP cache done | Clear ARP cache done. |
| Set manual time has succeeded. Current time is %s | The device date and time was changed manually.<br>%s is the date and time. |
| NTP update successful, current time is %s | The device successfully synchronized with a NTP time server .<br>%s is the date and time. |
| NTP update failed | The device was not able to synchronize with the NTP time server successfully. |

**Table 303** System Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Device is rebooted by administrator! | An administrator restarted the device. |
| Insufficient memory. | Cannot allocate system memory. |
| Connect to dyndns server has failed. | Cannot connect to members.dyndns.org to update DDNS. |
| Update the profile %s has failed because of strange server response. | Update profile failed because the response was strange, %s is the profile name. |
| Update the profile %s has succeeded because the IP address of FQDN %s was not changed. | Update profile succeeded, because the IP address of profile is unchanged, %s is the profile name. |
| Update the profile %s has succeeded. | Update profile succeeded, %s is the profile name. |
| Update the profile %s has failed because the FQDN %s is invalid. | Update profile failed because FQDN for the profile is invalid for DynDNS, 1st %s is the profile name, 2nd %s is the FQDN of the profile. |
| Update the profile %s has failed because the FQDN %s is malformed. | The FQDN format is malformed for DynDNS server, 1st %s is the profile name, 2nd %s is the FQDN of the profile. |
| Update the profile %s has failed because the FQDN %s is not under your control. | The owner of this FQDN is not the user, 1st %s is the profile name, 2nd %s is the FQDN of the profile. |
| Update the profile %s has failed because the FQDN %s was blocked for abuse. | The FQDN is blocked by DynDNS, 1st %s is the profile name, 2nd %s is the FQDN of the profile. |
| Update the profile %s has failed because of authentication fail. | Try to update profile, but failed, because of authentication fail, %s is the profile name. |
| Update the profile %s has failed because of invalid system parameters. | Some system parameters are invalid to update FQDN, %s is the profile name. |
| Update the profile %s has failed because the FQDN %s was blocked. | The FQDN is blocked by DynDNS , 1st %s is the profile name, 2nd %s is the FQDN of the profile. |
| Update the profile %s has failed because too many or too few hosts found. | %s is the profile name. |
| Update the profile %s has failed because of dyndns internal error | Update profile failed because of a dynsdns internal error, %s is the profile name. |

**Table 303** System Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Update the profile %s has failed because the feature requested is only available to donators. | Update profile failed because the feature requested is only available to donators, %s is the profile name. |
| Update the profile %s has failed because of error response. | Update profile failed because the response is incorrect, %s is the profile name. |
| Update the profile %s has failed because %s. | Update profile failed, and show the response message, 1st %s is the profile name, 2nd %s is the reason. |
| Update the profile %s has failed because of unknown error. | Update profile failed because unknown error. Sometimes, the force authentication will result in this error, 1st %s is the profile name. |
| Update the profile %s has failed because Username was empty. | DDNS profile needs username, %s is the profile name. |
| Update the profile %s has failed because Password was empty. | DDNS profile needs password, %s is the profile name. |
| Update the profile %s has failed because Domain name was empty. | DDNS profile needs domain name, %s is the profile name. |
| Update the profile %s has failed because Custom IP was empty. | The DDNS profile's IP select type is custom, and a custom IP was not defined, %s is the profile name. |
| Update the profile %s has failed because WAN interface was empty. | If the DDNS profile's IP select type is iface, it needs a WAN iface, %s is the profile name. |
| The profile %s has been paused because the VRRP status of WAN interface was standby. | The profile is paused by device-HA, because the VRRP status of that iface is standby, %s is the profile name. |
| Update the profile %s has failed because WAN interface was link-down. | DDNS profile cannot be updated for WAN IP because WAN iface is link-down, %s is the profile name. |
| Update the profile %s has failed because WAN interface was not connected. | DDNS profile cannot be updated for WAN IP because WAN iface is PPP and not connected, %s is the profile name. |
| Update the profile %s has failed because IP address of WAN interface was empty. | DDNS profile cannot be updated because the IP of WAN iface is 0.0.0.0, 1st %s is the profile name. |
| Update the profile %s has failed because ping-check of WAN interface has failed. | DDNS profile cannot be updated because the ping-check for WAN iface failed , %s is the profile name. |

**Table 303** System Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| The profile %s has been paused because the HA interface of VRRP status was standby. | The profile is paused by Device-HA, because the VRRP status of that HA iface is standby, %s is the profile name. |
| Update the profile %s has failed because HA interface was link-down. | DDNS profile cannot be updated for HA IP address because HA iface is link-down, %s is the profile name. |
| Update the profile %s has failed because the HA interface was not connected. | DDNS profile cannot be updated for HA IP address because HA iface is PPP and not connected, %s is the profile name. |
| Update the profile %s has failed because IP address of HA interface was empty. | DDNS profile cannot be updated because the IP address of HA iface is 0.0.0.0, %s is the profile name. |
| Update the profile %s has failed because ping-check of HA interface has failed. | DDNS profile cannot be updated because the fail of ping-check for HA iface, %s is the profile name |
| DDNS has been disabled by Device-HA. | DDNS is disabled by Device-HA, because all VRRP groups are standby. |
| DDNS has been enabled by Device-HA. | DDNS is enabled by Device-HA, because one of VRRP groups is active. |
| Disable DDNS has succeeded. | Disable DDNS. |
| Enable DDNS has succeeded. | Enable DDNS. |
| DDNS profile %s has been renamed as %s. | Rename DDNS profile, 1st %s is the original profile name, 2nd %s is the new profile name. |
| DDNS profile %s has been deleted. | Delete DDNS profile, %s is the profile name, |
| DDNS Initialization has failed. | Initialize DDNS failed, |
| All DDNS profiles are deleted | All DDNS profiles have been removed. |
| Collect Diagnostic Information has failed - Server did not respond. | There was an error and the diagnostics were not completed. |
| Collect Diagnostic Infomation has succeeded. | The diagnostics scripts were executed successfully. |
| Port %d is up!! | The specified port has it's link up. |
| Port %d is down!! | The specified port has it's link down. |

**Table 304** Connectivity Check Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Can't open link_up2 | Cannot recover routing status which is link-down. |
| Can not open %s.pid | Cannot open connectivity check process ID file.<br>%s: interface name |
| Can not open %s.arg | Cannot open configuration file for connectivity check process.<br>%s: interface name |
| The connectivity-check is activate for %s interface | The link status of interface is still activate after check of connectivity check process.<br>%s: interface name |
| The connectivity-check is fail for %s interface | The link status of interface is fail after check of connectivity check process.<br>%s: interface name |
| Can't get gateway IP of %s interface | The connectivity check process can't get the gateway IP address for the specified interface.<br>%s: interface name |
| Can't alloc memory | The connectivity check process can't get memory from OS. |
| Can't load %s module | The connectivity check process can't load module for check link-status.<br>%s: the connectivity module, currently only ICMP available. |
| Can't handle 'isalive' function of %s module | The connectivity check process can't execute 'isalive' function from module for check link-status.<br>%s: the connectivity module, currently only ICMP available. |
| Create socket error | The connectivity check process can't get socket to send packet. |
| Can't get IP address of %s interface | The connectivity check process can't get IP address of interface.<br>%s: interface name. |
| Can't get flags of %s interface | The connectivity check process can't get interface configuration.<br>%s: interface name |
| Can't get remote address of %s interface | The connectivity check process can't get remote address of PPP interface<br>%s: interface name |
| Can't get NETMASK address of %s interface | The connectivity check process can't get netmask address of interface.<br>%s: interface name |
| Can't get BROADCAST address of %s interface | The connectivity check process can't get broadcast address of interface<br>%s: interface name |

**Table 304** Connectivity Check Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Can't use MULTICAST IP for destination | The connectivity check process can't use multicast address to check link-status. |
| The destination is invalid, because destination IP is broadcast IP | The connectivity check process can't use broadcast address to check link-status. |
| Can't get MAC address of %s interface! | The connectivity check process can't get MAC address of interface.<br>%s: interface name |
| To send ARP REQUEST error! | The connectivity check process can't send ARP request packet. |
| The %s routing status seted to DEAD by connectivity-check | The interface routing can't forward packet.<br>%s: interface name |
| The %s routing status seted ACTIVATE by connectivity-check | The interface routing can forward packet.<br>%s: interface name |
| The link status of %s interface is inactive | The specified interface failed a connectivity check. |

**Table 305** Device HA Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Device HA VRRP Group %s has been added. | An VRRP group has been created, %s: the name of VRRP group. |
| Device HA VRRP group %s has been modified. | An VRRP group has been modified, %s: the name of VRRP group. |
| Device HA VRRP group %s has been deleted. | An VRRP group has been deleted, %s: the name of VRRP group. |
| Device HA VRRP interface %s for VRRP Group %s has changed. | Configuration of an interface that belonged to a VRRP group has been changed, 1st %s: VRRP interface name, 2ed %s: %s: the name of VRRP group. |
| Device HA syncing from %s starts. | Device HA Syncing from Master starts when user click "Sync Now" using Auto Sync, %s: The IP of FQDN of Master. |
| %s has no file to sync, Skip syncing it for %s. | There is no file to be synchronized from the Master when syncing a object (AV/AS/IDP/Certificate/System Configuration), But in fact, there should be something in the Master for the device to synchronize with, 1st %s: The syncing object, 2ed %s: The feature name for the syncing object. |
| Master configuration is the same with Backup. Skip updating it. | The System Startup configuration file synchronized from the Master is the same with the one in the Backup, so the configuration does not have to be updated. |

**Table 305** Device HA Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| %s file not existed, Skip syncing it for %s | There is no file to be synchronized from the Master when syncing a object (AV/AS/IDP/Certificate/System Configuration), But in fact, there should be something in the Master for the device to synchronize with, 1st %s: The syncing object, 2ed %s: The feature name for the syncing object. |
| Master firmware version can not be recognized. Stop syncing from Master. | Synchronizing stopped because the firmware version file was not found in the Master. A Backup device only synchronizes from the Master if the firmware versions are the same between the Master and the Backup. |
| Device HA Sync has failed when syncing %s for %s due to bad \"Sync Password\". | The synchronization password was incorrect when attempting to synchronize a certain object (AV/AS/IDP/Certificate/ System Configuration).<br>1st %s: The object to be synchronized, 2ed %s: The feature name for the object to be synchronized. |
| Device HA Sync has failed when syncing %s for %s due to bad \"Sync From\" or \"Sync Port\". | The Sync From IP address or Sync Port may be incorrect when synchronizing a certain object (AV/AS/IDP/Certificate/ System Configuration). |
| Device HA Sync has failed when syncing %s for %s. | Synchronization failed when synchronizing a certain object (AV/AS/IDP/Certificate/System Configuration) due to an unknown reason, 1st %s: The object to be synchronized, 2ed %s: The feature name for the object to be synchronized. |
| Sync Failed: Cannot connect to Master when syncing %s for %s. | Synchronization failed because the Backup could not connect to the Master. The object to be synchronized, 2ed %s: The feature name for the object to be synchronized. |
| Backup firmware version can not be recognized. Stop syncing from Master. | The firmware version on the Backup cannot be resolved to check if it is the same as on the Master. A Backup device only synchronizes from the Master if the Master and the Backup have the same firmware versions. |
| Sync failed: Remote Firmware Version Unknown | The firmware version on the Master cannot be resolved to check if it is the same as on the Master. A Backup device only synchronizes from the Master if the Master and the Backup have the same firmware versions. |
| Master firmware version should be the same with Backup. | The Backup and Master have different firmware versions. A Backup device only synchronizes from the Master if the Master and the Backup have the same firmware versions. |
| Update %s for %s has failed. | Updating a certain object failed when updating (AS/AV/IDP/ Certificate/System Configuration). 1st %s: The object to be synchronized, 2ed %s: The feature name for the object to be synchronized. |
| Update %s for %s has failed: %s. | Updating a certain object failed when updating (AS/AV/IDP/ Certificate/System Configuration) due to some reason. 1st %s: The object to be synchronized, 2ed %s: The feature name for the object to be synchronized. |
| Device HA has skipped syncing %s since %s is %s. | A certain service has no license or the license is expired, so it was not synchronized from the Master. 1st %s: The object to be synchronized, 2ed %s: The feature name for the object to be synchronized, 3rd %s: unlicensed or license expired. |

**Table 305** Device HA Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Device HA authentication type for VRRP group %s maybe wrong. | A VRRP group's Authentication Type (Md5 or IPSec AH) configuration may not match between the Backup and the Master. %s: The name of the VRRP group. |
| Device HA authenticaton string of text for VRRP group %s maybe wrong. | A VRRP group's Simple String (Md5) configuration may not match between the Backup and the Master. %s: The name of the VRRP group. |
| Device HA authentication string of AH for VRRP group %s maybe wrong. | A VRRP group's AH String (IPSec AH) configuration may not match between the Backup and the Master. %s: The name of the VRRP group. |
| Retrying to update %s for %s. Retry: %d. | An update failed. Retrying to update the failed object again. 1st %s: The object to be synchronized, 2ed %s: The feature name for the object to be synchronized, %d: the retry count. |
| Recovring to Backup original state for %s has failed. | An update failed. The device will try to recover the failed update feature to the original state before Device HA synchronizes the specified object. |
| Recovering to Backup original state for %s has succeeded. | Recovery succeeded when an update for the specified object failed. |
| One of VRRP groups has became avtive. Device HA Sync has aborted from Master %s. | %s: IP or FQDN of Master |
| Master configuration file does not exist. Skip updating ZySH Startup Configuration. | |
| System internal error: %s. Skip updating %s. | 1st %s: error string, 2ed %s: the syncing object |
| Master configuration file is empty. Skip updating ZySH Startup Configuration. | |
| Device HA Sync has failed when syncing %s for %s due to transmission timeout. | 1st %s: the syncing object, 2ed %s: the feature name for the syncing object |
| VRRP interface %s has been shutdown. | %s: The name of the VRRP interface. |
| VRRP interface %s has been brought up. | %s: The name of the VRRP interface. |

**Table 306** Routing Protocol Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| RIP on interface %s has been stopped because Device-HA binds this interface. | Device-HA is currently running on the interface %s, so all the local service have to be stopped including RIP. %s: Interface Name |
| RIP on all interfaces have been stopped | Got the CLI command 'no router rip' to shut down RIP on all interfaces |
| Invalid RIP md5 authentication | RIP md5 authentication has been set without setting md5 authentication id and key first |
| Invalid RIP text authentication. | RIP text authentication has been set without setting authentication key first |
| RIP on interface %s has been activated. | RIP on interface %s has been activated. %s: Interface Name |
| RIP direction on interface %s has been changed to In-Only. | RIP direction on interface %s has been changed to In-Only. %s: Interface Name |
| RIP direction on interface %s has been changed to Out-Only. | RIP direction on interface %s has been changed to Out-Only. %s: Interface Name |
| RIP authentication mode has been changed to %s. | RIP authentication mode has been changed to text or md5. |
| RIP text authentication key has been changed. | RIP text authentication key has been changed. |
| RIP md5 authentication id and key have been changed. | RIP md5 authentication id and key have been changed. |
| RIP global version has been changed to %s. | RIP global version has been changed to version 1 or 2. |
| RIP redistribute OSPF routes has been enabled. | RIP redistribute OSPF routes has been enabled. |
| RIP redistribute static routes has been enabled. | RIP redistribute static routes has been enabled. |
| RIP on interface %s has been deactivated. | RIP on interface %s has been deactivated. %s: Interface Name |
| RIP direction on interface %s has been changed to BiDir. | RIP direction on interface %s has been changed to BiDir. %s: Interface Name |
| RIP authentication has benn disabled. | RIP text or md5 authentication has been disabled. |
| RIP text authentication key has been deleted. | RIP text authentication key has been deleted. |

**Table 306** Routing Protocol Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| RIP md5 authentication id and key have been deleted. | RIP md5 authentication id and key have been deleted. |
| RIP global version has been deleted. | RIP global version has been deleted. |
| RIP redistribute OSPF routes has been disabled. | RIP redistribute OSPF routes has been disabled. |
| RIP redistribute static routes has been disabled. | RIP redistribute static routes has been disabled. |
| RIP v2-broadcast on interface %s has been enabled. | RIP v2-broadcast on interface %s has been enabled. %s: Interface Name. |
| RIP send-version on interface %s has been changed to %s. | RIP send-version on interface %s has been changed to version 1 or 2 or both 1 2. %s: Interface Name. |
| RIP receive-version on interface %s has been changed to %s. | RIP receive-version on interface %s has been changed to version 1 or 2 or both 1 2. 2nd%s: Interface Name. |
| RIP send-version on interface %s has been reset to current global version %s. | RIP send-version on interface %s has been reset to current global version %s. 1st %s: Interface Name, 2nd %s: RIP Version |
| RIP receive-version on interface %s has been reset to current global version %s. | RIP receive-version on interface %s has been reset to current global version %s. 1st %s: Interface Name, 2nd %s: RIP |
| RIP v2-broadcast on interface %s has been disabled. | RIP v2-broadcast on interface %s has been disabled. %s: Interface Name |
| OSPF on interface %s has been stopped because Device-HA binds this interface. | Device-HA is currently running on the interface %s, so all the local service have to be stopped including OSPF. %s: Interface Name |
| Area %s cannot be removed. This area is in use. | One or more interfaces are still using this area, so area %s cannot be removed. %s: OSPF Area |
| Invalid OSPF %s authentication of area %s. | OSPF md5 or text authentication has been set without setting md5 authentication id and key, or text authentication key first. |
| Invalid OSPF virtual-link %d md5 authentication of area %s. | Virtual-link %s md5 authentication has been set without setting md5 authentication id and key first. %s: Virtual-Link ID |
| Invalid OSPF virtual-link %s text authentication of area %s. | Virtual-link %s text authentication has been set without setting text authentication key first. %s: Virtual-Link ID |

**Table 306** Routing Protocol Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Invalid OSPF virtual-link %s authentication of area %s. | Virtual-link %s authentication has been set to same-as-area but the area has invalid authentication configuration. %s: Virtual-Link ID |
| Invalid OSPF md5 authentication on interface %s. | Invalid OSPF md5 authentication is set on interface %s. %s: Interface Name |
| Invalid OSPF text authentication on interface %s. | Invalid OSPF text authentication is set on interface %s. %s: Interface Name |
| Interface %s does not belong to any OSPF area. | Interface %s has been set OSPF authentication same-as-area, however the interface does not belong to any OSPF area. %s: Interface Name |
| Invalid OSPF authentication of area %s on interface %s. | Interface %s has been set OSPF authentication same-as-area, however the area has invalid text authentication configuration. %s: Interface Name |

**Table 307** NAT Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| The NAT range is full | The NAT mapping table is full. |
| %s FTP ALG has succeeded. | The FTP Application Layer Gateway (ALG) has been turned on or off.<br><br>%s: Enable or Disable |
| Extra signal port of FTP ALG has been modified. | Extra FTP ALG port has been changed. |
| Signal port of FTP ALG has been modified. | Default FTP ALG port has been changed. |
| %s H.323 ALG has succeeded. | The H.323 ALG has been turned on or off. %s: Enable or Disable |
| Extra signal port of H.323 ALG has been modified. | Extra H.323 ALG port has been changed. |
| Signal port of H.323 ALG has been modified. | Default H.323 ALG port has been changed. |
| %s SIP ALG has succeeded. | The SIP ALG has been turned on or off. %s: Enable or Disable |
| Extra signal port of SIP ALG has been modified. | Extra SIP ALG port has been changed. |
| Signal port of SIP ALG has been modified. | Default SIP ALG port has been changed. |
| Register SIP ALG extra port=%d failed. | SIP ALG apply additional signal port failed.<br><br>%d: Port number |

**Table 307** NAT Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Register SIP ALG signal port=%d failed. | SIP ALG apply signal port failed.<br>%d: Port number |
| Register H.323 ALG extra port=%d failed. | H323 ALG apply additional signal port failed.<br>%d: Port number |
| Register H.323 ALG signal port=%d failed. | H323 ALG apply signal port failed.<br>%d: Port number |
| Register FTP ALG extra port=%d failed. | FTP ALG apply additional signal port failed.<br>%d: Port number |
| Register FTP ALG signal port=%d failed. | FTP ALG apply signal port failed.<br>%d: Port number |

**Table 308** PKI Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Generate X509certifiate "%s" successfully | The router created an X509 format certificate with the specified name. |
| Generate X509 certificate "%s" failed, errno %d | The router was not able to create an X509 format certificate with the specified name. See Table 296 on page 895 for details about the error number. |
| Generate certificate request "%s" successfully | The router created a certificate request with the specified name. |
| Generate certificate request "%s" failed, errno %d | The router was not able to create a certificate request with the specified name. See Table 296 on page 895 for details about the error number. |
| Generate PKCS#12 certificate "%s" successfully | The router created a PKCS#12 format certificate with the specified name. |
| Generate PKCS#12 certificate "%s" failed, errno %d | The router was not able to create anPKCS#12 format certificate with the specified name. See Table 296 on page 895 for details about the error number. |
| Prepare to import "%s" into "My Certificate" | %s is the name of a certificate request. |
| Prepare to import "%s" into Trusted Certificate" | %s is the name of a certificate request. |
| CMP enrollment "%s" successfully, CA "%s", URL "%s" | The device used CMP to enroll a certificate. 1st %s is a request name, 2nd %s is the CA name, 3rd %s is the URL . |
| CMP enrollment "%s" failed, CA "%s", URL "%s" | The device was unable to use CMP to enroll a certificate. 1st %s is a request name, 2nd %s is the CA name, 3rd %s is the URL |

**Table 308** PKI Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| SCEP enrollment "%s" successfully, CA "%s", URL "%s" | The device used SCEP to enroll a certificate. 1st %s is a request name, 2nd %s is the CA name, 3rd %s is the URL . |
| SCEP enrollment "%s" failed, CA "%s", URL "%s" | The device was unable to use SCEP to enroll a certificate. 1st %s is a request name, 2nd %s is the CA name, 3rd %s is the URL |
| Import X509 certificate "%s" into My Certificate successfully | The device imported a x509 format certificate into My Certificates. %s is the certificate request name. |
| Import X509 certificate "%s" into Trusted Certificate successfully | The device imported a x509 format certificate into Trusted Certificates. %s is the certificate request name. |
| Import PKCS#12 certificate "%s" into "My Certificate" successfully | The device imported a PKCS#12 format certificate into My Certificates. %s is the certificate request name. |
| Import PKCS#7 certificate "%s" into "My Certificate" successfully | The device imported a PKCS#7 format certificate into My Certificates. %s is the certificate request name. |
| Import PKCS#7 certificate "%s" into "Trusted Certificate" successfully | The device imported a PKCS#7 format certificate into Trusted Certificates. %s is the certificate request name. |
| Decode imported certificate "%s" failed | The device was not able to decode an imported certificate. %s is certificate the request name |
| Export PKCS#12 certificate "%s" from "My Certificate" successfully | The device exported a PKCS#12 format certificate from My Certificates. %s is the certificate request name. |
| Export PKCS#12 certificate "%s" from "My Certificate" failed | The device was not able to export a PKCS#12 format certificate from My Certificates. %s is the certificate request name. |
| Export X509 certificate "%s" from "My Certificate" failed | The device was not able to export a x509 format certificate from My Certificates. %s is the certificate request name. |
| Export X509 certificate "%s" from "Trusted Certificate" failed | The device was not able to export a x509 format certificate from Trusted Certificates. %s is the certificate request name. |
| Export X509 certificate "%s" from "My Certificate" successfully | The device exported a x509 format certificate from My Certificates. %s is the certificate request name. |

**Table 308** PKI Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Export X509 certificate "%s" from "Trusted Certificate" successfully | The device exported a x509 format certificate from Trusted Certificates. %s is the certificate request name. |
| Export X509 certificate "%s" from "My Certificate" failed | The device was not able to export a x509 format certificate from My Certificates. %s is the certificate request name. |
| Import PKCS#12 certificate "%s" with incorrect password | An administrator used the wrong password when trying to import a PKCS#12 format certificate. %s is the certificate name. |
| Cert trusted: %s | %s is the subject. |
| Due to %d, cert not trusted: %s | %d is an error number (see Table 296 on page 895), %s is the certificate subject. |

| CODE | DESCRIPTION |
|---|---|
| 1 | Algorithm mismatch between the certificate and the search constraints. |
| 2 | Key usage mismatch between the certificate and the search constraints. |
| 3 | Certificate was not valid in the time interval. |
| 4 | (Not used) |
| 5 | Certificate is not valid. |
| 6 | Certificate signature was not verified correctly. |
| 7 | Certificate was revoked by a CRL. |
| 8 | Certificate was not added to the cache. |
| 9 | Certificate decoding failed. |
| 10 | Certificate was not found (anywhere). |
| 11 | Certificate chain looped (did not find trusted root). |
| 12 | Certificate contains critical extension that was not handled. |
| 13 | Certificate issuer was not valid (CA specific information missing). |
| 14 | (Not used) |
| 15 | CRL is too old. |
| 16 | CRL is not valid. |
| 17 | CRL signature was not verified correctly. |
| 18 | CRL was not found (anywhere). |
| 19 | CRL was not added to the cache. |
| 20 | CRL decoding failed. |
| 21 | CRL is not currently valid, but in the future. |
| 22 | CRL contains duplicate serial numbers. |
| 23 | Time interval is not continuous. |
| 24 | Time information not available. |

| CODE | DESCRIPTION |
|---|---|
| 25 | Database method failed due to timeout. |
| 26 | Database method failed. |
| 27 | Path was not verified. |
| 28 | Maximum path length reached. |

**Table 309** Interface Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Interface %s has been deleted. | An administrator deleted an interface. %s is the interface name. |
| AUX Interface dialing failed. This AUX interface is not enabled. | A user tried to dial the AUX interface, but the AUX interface is not enabled. |
| AUX Interface disconnecting failed. This AUX interface is not enabled. | The AUX interface is not enabled and a user tried to use the disconnect aux command. |
| Please type phone number of interface AUX first then dial again. | A user tried to dial the AUX interface, but the AUX interface does not have a phone number set. |
| Please type phone number of Interface AUX first then disconnect again. | The AUX interface does not have a phone number set and a user tried to use the disconnect aux command. |
| Interface %s will reapply because Device HA become active status. | Device-ha became active and is using a PPP base interface, the PPP interface must reapply, %s is the interface name. |
| Interface %s will reapply because Device HA is not running. | Device-ha was deleted and free PPP base interface, PPP interface must reapply, %s is the interface name. |
| Interface %s will stop connect because Device HA become standby status. | When device-ha is stand-by and use PPP base interface, PPP interface connection will stop, %s: interface name. |
| Create interface %s has been failed. | When PPP can't running fail, %s: interface name. |
| Base interface %s is disabled. Interface %s is disabled now. | When user disable ethernet, vlan or bridge interface and this interface is base interface of PPP or virtual interface. PPP and virtual will disable too. 1st %s is interface name, 2nd %s is interface. |
| Interface %s has been changed. | An administrator changed an interface's configuration. %s: interface name. |
| Interface %s has been added. | An administrator added a new interface. %s: interface name. |

**Table 309** Interface Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Interface %s is enabled. | An administrator enabled an interface. %s: interface name. |
| Interface %s is disabled. | An administrator disabled an interface. %s: interface name. |
| %s MTU > (%s MTU - 8), %s may not work correctly. | An administrator configured a PPP interface, PPP interface MTU > (base interface MTU - 8), PPP interface may not run correctly because PPP packets will be fragmented by base interface and the peer will not receive correct PPP packets. 1st %s: PPP interface name, 2nd %s: ethernet interface name. |
| (%s MTU - 8) < %s MTU, %s may not work correctly. | An administrator configured ethernet, vlan or bridge and this interface is base interface of PPP interface. PPP interface MTU > (base interface MTU - 8), PPP interface may not run correctly because PPP packets will be fragmented by base interface and peer will not receive correct PPP packets.1st %s: Ethernet interface name, 2nd %s: PPP interface name. |
| Interface %s links down. Default route will not apply until interface %s links up. | An administrator set a static gateway in interface but this interface is link down. At this time the configuration will be saved but route will not take effect until the link becomes up.1st %s: interface name, 2nd %s: interface name. |
| name=%s,status=%s,TxPkts=%u, RxPkts=%u,Colli.=%u,TxB/s=%u, RxB/s=%u,UpTime=%s | Port statistics log. This log will be sent to the VRPT server.<br>1st %s: physical port name, 2nd %s: physical port status, 1st %u: physical port Tx packets, 2nd %u: physical port Rx packets, 3rd %u: physical port packets collisions, 4th %u: physical port Tx Bytes/s, 5th %u: physical port Rx Bytes/s, 3rd %s: physical port up time. |
| name=%s,status=%s,TxPkts=%u, RxPkts=%u,Colli.=%u,TxB/s=%u, RxB/s=%u | Interface statistics log. This log will be sent to the VRPT server.<br>1st %s: interface name, 2nd %s: interface status, 1st %u variable: interface Tx packets, 2nd %u variable: interface Rx packets, 3rd %u: interface packets collisions, 4th %u: interface Tx Bytes/s, 5th %u: interface Rx Bytes/s. |
| Interface %s start dailing. | A PPP or aux interface started dialing to a server. %s: interface name. |
| Interface %s connect failed: Connect to server failed. | A PPTP interface failed to connect to the PPTP server. %s: interface name. |
| Interface %s connection terminated. | A PPP or AUX connection will terminate. %s: interface name. |
| Interface %s connection terminated: idle timeout. | An idle PPP or AUX connection timed out.1%s: interface name. |
| Interface %s connect failed: MS-CHAPv2 mutual authentication failed. | MS-CHAPv2 authentication failed (the server must support mS-CHAPv2 and verify that the authentication failed, this does not include cases where the servers does not support MS-CHAPv2). %s: interface name. |

**Table 309** Interface Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Interface %s connect failed: MS-CHAP authentication failed. | MS-CHAP authentication failed (the server must support MS-CHAP and verify that the authentication failed, this does not include cases where the server does not support MS-CHAP). %s: interface name. |
| Interface %s connect failed: CHAP authentication failed. | CHAP authentication failed (the server must support CHAP and verify that the authentication failed, this does not include cases where the server does not support CHAP). CHAP: interface name. |
| Interface %s is connected. | A PPP or AUX interface connected successfully. %s: interface name. |
| Interface %s is disconnected. | A PPP or AUX interface disconnected successfully. %s: interface name. |
| Interface %s connect failed: Peer not responding. | The interface's connection will be terminated because the server did not send any LCP packets. %s: interface name. |
| Interface %s connect failed: PAP authentication failed. | PAP authentication failed (the server must support PAP and verify verify that the authentication failed, this does not include cases where the server does not support PAP). %s: PPP interface name. |
| Interface %s connect failed: Connect timeout. | A PPPOE connection timed out due to a lack of response from the PPPOE server. %s: PPP interface name. |
| Interface %s create failed because has no member. | A bridge interface has no member. %s: bridge interface name. |
| "Interface cellular Application Error Code %d\n. | The listed error code (%d) was generated due to an internal cellular interface error. |
| "An error [%d] occurred while negotiating with the device in %s. Please try to remove then insert the device. | The listed error code (%d) happened when the ZyWALL attempted to negotiate with the cellular device installed in (or connected to) the listed slot (%s). Remove and reinstall the device. |
| "Unable to negotiate with the device in %s. Please try to remove then insert the device. | The ZyWALL could not negotiate with the cellular device installed in (or connected to) the listed slot (%s). Remove and reinstall the device. |
| "Unable to configure the selected frequency band to the device in %s. Please try to remove then insert the device. | The ZyWALL failed to set the cellular device installed in (or connected to) the listed slot (%s) to use the frequency band you configured. The cellular device may not support the band or you may need to try removing and reinstalling the device. |
| "PIN code is required for inteface cellular%d. Please check the PIN code setting. | The PIN code configured for the listed cellular interface (%d) is incorrect or missing. |

**Table 309** Interface Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| "SIM card has been successfully unlocked by PUK code on interface cellular%d. | You entered the correct PUK code and unlocked the SIM card for the cellular device associated with the listed cellular interface (%d). |
| "Incorrect PUK code of interface cellular%d. Please check the PUK code setting. | You entered an incorrect PUK code so you were not able to unlock the SIM card for the cellular device associated with the listed cellular interface (%d). |
| "SIM card of interface cellular%d in %s is damaged or not inserted. Please remove the device, then check the SIM card. | The SIM card for the cellular device associated with the listed cellular interface (%d) cannot be detected. The SIM card may be missing, not inserted properly, or damaged. Remove the device and check its SIM card. If it does not appear to be damaged, try re-inserting the SIM card. |
| "SIM card of interface cellular%d in %s is locked. Please enter PUK code to unlock. | The SIM card for the cellular device associated with the listed cellular interface (%d) is locked. This may be because the PIN code was entered incorrectly more than three times. You need to enter the PUK code to unlock the SIM card. . |
| "Incorrect PIN code of interface cellular%d. Please check the PIN code setting. | The listed cellular interface (%d) does has the wrong PIN code configured. |
| "Unable to query the signal quality from the device in %s. Please try to remove then insert the device. | The ZyWALL could not check the signal strength for the listed cellular interface (%d). This could be due to an error or being out of range of the ISP's cellular station. |
| "Interface cellular%d cannot connect to the service provider. | The listed cellular interface (%d) cannot connect to the ISP. This could be due to an error or being out of range of the ISP's cellular station. |
| "Interface cellular%d is configured with incorrect APN. | The listed cellular interface (%d) does not have the correct APN (Access Point Name) configured. |
| "Interface cellular%d is configured with incorrect phone number. | The listed cellular interface (%d) does not have the correct phone number configured. |
| "Interface cellular%d is configured with incorrect username or password. | The listed cellular interface (%d) does not have the correct user name and password configured. |
| "Interface cellular%d is configured with device %s, but current inserted device is %s. | The listed cellular interface (%d) is configured for a particular cellular device (first %s), but a different cellular device (second %s) is inserted. |
| "Cellular device [%s %s] has been inserted into %s. | The cellular device (identified by its manufacturer and model) has been inserted in or connected to the specified slot. |

**Table 309** Interface Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| "Cellular device [%s %s] has been removed from %s. | The cellular device (identified by its manufacturer and model) has been removed from the specified slot. |
| Interface cellular%d required authentication password.Please set password in cellular%d edit page. | You need to manually enter the password for the listed cellular interface (%d). |

**Table 310** WLAN Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Wlan %s is enabled. | The WLAN (IEEE 802.11 b and or g) feature has been turned on. %s is the slot number where the WLAN card is or can be installed. |
| Wlan %s is disabled. | The WLAN (IEEE 802.11 b and or g) feature has been turned off. %s is the slot number where the WLAN card is or can be installed. |
| Wlan %s has been configured. | The WLAN (IEEE 802.11 b and or g) feature's configuration has been changed. %s is the slot number where the WLAN card is or can be installed. |
| Interface %s has been configured. | The configuration of the specified WLAN interface (%s) has been changed. |
| Interface %s has been deleted. | The specified WLAN interface (%s) has been removed. |
| Create interface %s has failed. Wlan device does not exist. | The wireless device failed to create the specified WLAN interface (%s). Remove the wireless device and reinstall it. |
| System internal error. No 802.1X or WPA enabled! | IEEE 802.1x or WPA is not enabled. |
| System internal error. Error configuring WPA state! | The ZyWALL was not able to configure the wireless device to use WPA. Remove the wireless device and reinstall it. |
| System internal error. Error enabling WPA/ 802.1X! | The ZyWALL was not able to enable WPA/IEEE 802.1X. |
| Station has associated. Interface: %s, MAC: %s. | A wireless client with the specified MAC address (second %s) associated with the specified WLAN interface (first %s). |
| WPA or WPA2 enterprise EAP timeout. Interface: %s, MAC: %s. | There was an EAP timeout for a wireless client connected to the specified WLAN interface (first %s). The MAC address of the wireless client is listed (second %s). |

**Table 310** WLAN Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Station association has failed. Maximum associations have reached the maximum number. Interface: %s, MAC: %s. | A wireless client with the specified MAC address (second %s) failed to connect to the specified WLAN interface (first %s) because the WLAN interface already has its maximum number of wireless clients. |
| WPA authentication has failed. Interface: %s, MAC: %s. | A wireless client used an incorrect WPA key and thus failed to connect to the specified WLAN interface (first %s). The MAC address of the wireless client is listed (second %s). |
| Incorrect password for WPA or WPA2 enterprise internal authentication. Interface: %s, MAC: %s. | A wireless client used an incorrect WPA or WPA2 user password and failed authentication by the ZyWALL's local user database while trying to connect to the specified WLAN interface (first %s). The MAC address of the wireless client is listed (second %s). |
| Incorrect username or password for WPA or WPA2 enterprise internal authentication. Interface: %s, MAC: %s. | A wireless client used an incorrect WPA or WPA2 user name or user password and failed authentication by the ZyWALL's local user database while trying to connect to the specified WLAN interface (first %s). The MAC address of the wireless client is listed (second %s). |
| System internal error. %s: STA %s could not extract EAP-Message from RADIUS message | There was an error when attempting to extract the EAP-Message from a RADIUS message. The first %s is the WLAN interface. The second %s is the MAC address of the wireless client. |

**Table 311** Account Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Account %s %s has been deleted. | A user deleted an ISP account profile.<br>1st %s: profile type, 2nd %se: profile name. |
| Account %s %s has been changed. | A user changed an ISP account profile's options.<br>1st %s: profile type, 2nd %s: profile name. |
| Account %s %s has been added. | A user added a new ISP account profile.<br>1st %s: profile type, 2nd %s: profile name. |

**Table 312** Port Grouping Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Interface %s links up because of changing Port Group. Enable DHCP client. | An administrator used port-grouping to assign a port to a representative Interface and this representative interface is set to DHCP client and only has one member. In this case the DHCP client will be enabled. %s: interface name. |
| Interface %s links down because of changing Port Group. Disable DHCP client. | An administrator used port-grouping to assign a port to a representative interface and this representative interface is set to DHCP client and has no members in its group. In this case the DHCP client will be disabled. %s: interface name. |
| Port Group on %s is changed. Renew DHCP client. | An administrator used port-grouping to assign a port to a representative interface and this representative interface is set to DHCP client and has more than one member in its group. In this case the DHCP client will renew. %s: interface name. |
| Port Grouping %s has been changed. | An administrator configured port-grouping, %s: interface name. |

**Table 313** Force Authentication Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Force User Authentication will be enabled due to http server is enabled. | Force user authentication will be turned on because HTTP server was turned on. |
| Force User Authentication will be disabled due to http server is disabled. | Force user authentication will be turned off because HTTP server was turned off. |
| Force User Authentication may not work properly! | |

**Table 314** File Manager Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| ERROR:#%s, %s | Apply configuration failed, this log will be what CLI command is and what error message is.<br>1st %s is CLI command.<br>2nd %s is error message when apply CLI command. |
| WARNING:#%s, %s | Apply configuration failed, this log will be what CLI command is and what warning message is.<br>1st %s is CLI command.<br>2nd %s is warning message when apply CLI command. |

**Table 314** File Manager Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| ERROR:#%s, %s | Run script failed, this log will be what wrong CLI command is and what error message is.<br>1st %s is CLI command.<br>2nd %s is error message when apply CLI command. |
| WARNING:#%s, %s | Run script failed, this log will be what wrong CLI command is and what warning message is.<br>1st %s is CLI command.<br>2nd %s is warning message when apply CLI command. |
| Resetting system... | Before apply configuration file. |
| System resetted. Now apply %s.. | After the system reset, it started to apply the configuration file.<br>%s is configuration file name. |
| Running %s... | An administrator ran the listed shell script.<br>%s is script file name. |

**Table 315** DHCP Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Can't find any lease for this client - %s, DHCP pool full! | All of the IP addresses in the DHCP pool are already assigned to DHCP clients, so there is no IP address to give to the listed DHCP client. |
| DHCP server offered %s to %s(%s) | The DHCP server feature gave the listed IP address to the computer with the listed hostname and MAC address. |
| Requested %s from %s(%s) | The ZyWALL received a DHCP request for the specified IP address from the computer with the listed hostname and MAC address. |
| No applicable lease found for DHCP request - %s ! | There is no matching DHCP lease for a DHCP client's request for the specified IP address. |
| DHCP released %s with %s(%s) | A DHCP client released the specified IP address. The DHCP client's hostname and MAC address are listed. |
| Sending ACK to %s | The DHCP server feature received a DHCP client's inform packet and is sending an ACK to the client. |
| DHCP server assigned %s to %s(%s) | The DHCP server feature assigned a client the IP address that it requested. The DHCP client's hostname and MAC address are listed. |

**Table 316** E-mail Daily Report Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Email Daily Report has been activated. | The daily e-mail report function has been turned on. The ZyWALL will e-mail a daily report about the selected items at the scheduled time if the required settings are configured correctly. |
| Email Daily Report has been deactivated. | The daily e-mail report function has been turned off. The ZyWALL will not e-mail daily reports. |
| Email daily report has been sent successfully. | The ZyWALL sent a daily e-mail report mail successfully. |
| Cannot resolve mail server address %s. | The (listed) SMTP address configured for the daily e-mail report function is incorrect. |
| Mail server authentication failed. | The user name or password configured for authenticating with the e-mail server is incorrect. |
| Failed to send report. Mail From address %s1 is inconsistent with SMTP account %s2. | The user name and password configured for authenticating with the e-mail server are correct, but the (listed) sender e-mail address does not match the (listed) SMTP e-mail account. |
| Failed to connect to mail server %s. | The ZyWALL could not connect to the SMTP e-mail server (%s). The address configured for the server may be incorrect or there may be a problem with the ZyWALL's or the server's network connection. |

**Table 317** IP-MAC Binding Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Drop packet %s-%u.%u.%u.%u-%02X:%02X:%02X:%02X:%02X:%02X | The IP-MAC binding feature dropped an Ethernet packet. The interface the packet came in through and the sender's IP address and MAC address are also shown. |
| Cannot bind ip-mac from dhcpd: %s#%u.%u.%u.%u#%02X:%02X:%02X:%02X:%02X:%02X. | The IP-MAC binding feature could not create an IP-MAC binding hash table entry. The interface the packet came in through, the sender's IP address and MAC address, are also shown along with the binding type ("s" for static or "d" for dynamic). |
| Cannot remove ip-mac binding from dhcpd: %s#%u.%u.%u.%u#%02X:%02X:%02X:%02X:%02X:%02X. | The IP-MAC binding feature could not delete an IP-MAC binding hash table entry. The interface the packet came in through, the sender's IP address and MAC address, are also shown along with the binding type ("s" for static or "d" for dynamic). |

# B

# Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**. Please refer to RFC 1700 for further information about port numbers.
  - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

**Table 318** Commonly Used Services

| NAME | PROTOCOL | PORT(S) | DESCRIPTION |
|---|---|---|---|
| AH (IPSEC_TUNNEL) | User-Defined | 51 | The IPSEC AH (Authentication Header) tunneling protocol uses this service. |
| AIM/New-ICQ | TCP | 5190 | AOL's Internet Messenger service. It is also used as a listening port by ICQ. |
| AUTH | TCP | 113 | Authentication protocol used by some servers. |
| BGP | TCP | 179 | Border Gateway Protocol. |
| BOOTP_CLIENT | UDP | 68 | DHCP Client. |
| BOOTP_SERVER | UDP | 67 | DHCP Server. |
| CU-SEEME | TCP<br>UDP | 7648<br>24032 | A popular videoconferencing solution from White Pines Software. |
| DNS | TCP/UDP | 53 | Domain Name Server, a service that matches web names (for example www.zyxel.com) to IP numbers. |

**Table 318** Commonly Used Services (continued)

| NAME | PROTOCOL | PORT(S) | DESCRIPTION |
|---|---|---|---|
| ESP (IPSEC_TUNNEL) | User-Defined | 50 | The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service. |
| FINGER | TCP | 79 | Finger is a UNIX or Internet related command that can be used to find out if a user is logged on. |
| FTP | TCP<br>TCP | 20<br>21 | File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail. |
| H.323 | TCP | 1720 | NetMeeting uses this protocol. |
| HTTP | TCP | 80 | Hyper Text Transfer Protocol - a client/server protocol for the world wide web. |
| HTTPS | TCP | 443 | HTTPS is a secured http session often used in e-commerce. |
| ICMP | User-Defined | 1 | Internet Control Message Protocol is often used for diagnostic or routing purposes. |
| ICQ | UDP | 4000 | This is a popular Internet chat program. |
| IGMP (MULTICAST) | User-Defined | 2 | Internet Group Management Protocol is used when sending packets to a specific group of hosts. |
| IKE | UDP | 500 | The Internet Key Exchange algorithm is used for key distribution and management. |
| IRC | TCP/UDP | 6667 | This is another popular Internet chat program. |
| MSN Messenger | TCP | 1863 | Microsoft Networks' messenger service uses this protocol. |
| NEW-ICQ | TCP | 5190 | An Internet chat program. |
| NEWS | TCP | 144 | A protocol for news groups. |
| NFS | UDP | 2049 | Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments. |
| NNTP | TCP | 119 | Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service. |
| PING | User-Defined | 1 | Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable. |
| POP3 | TCP | 110 | Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other). |

**Table 318** Commonly Used Services (continued)

| NAME | PROTOCOL | PORT(S) | DESCRIPTION |
|---|---|---|---|
| PPTP | TCP | 1723 | Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel. |
| PPTP_TUNNEL (GRE) | User-Defined | 47 | PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel. |
| RCMD | TCP | 512 | Remote Command Service. |
| REAL_AUDIO | TCP | 7070 | A streaming audio service that enables real time sound over the web. |
| REXEC | TCP | 514 | Remote Execution Daemon. |
| RLOGIN | TCP | 513 | Remote Login. |
| RTELNET | TCP | 107 | Remote Telnet. |
| RTSP | TCP/UDP | 554 | The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet. |
| SFTP | TCP | 115 | Simple File Transfer Protocol. |
| SMTP | TCP | 25 | Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another. |
| SNMP | TCP/UDP | 161 | Simple Network Management Program. |
| SNMP-TRAPS | TCP/UDP | 162 | Traps for use with the SNMP (RFC:1215). |
| SQL-NET | TCP | 1521 | Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers. |
| SSH | TCP/UDP | 22 | Secure Shell Remote Login Program. |
| STRM WORKS | UDP | 1558 | Stream Works Protocol. |
| SYSLOG | UDP | 514 | Syslog allows you to send system logs to a UNIX server. |
| TACACS | UDP | 49 | Login Host Protocol used for (Terminal Access Controller Access Control System). |
| TELNET | TCP | 23 | Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems. |

**Table 318** Commonly Used Services (continued)

| NAME | PROTOCOL | PORT(S) | DESCRIPTION |
|---|---|---|---|
| TFTP | UDP | 69 | Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol). |
| VDOLIVE | TCP | 7000 | Another videoconferencing solution. |

C

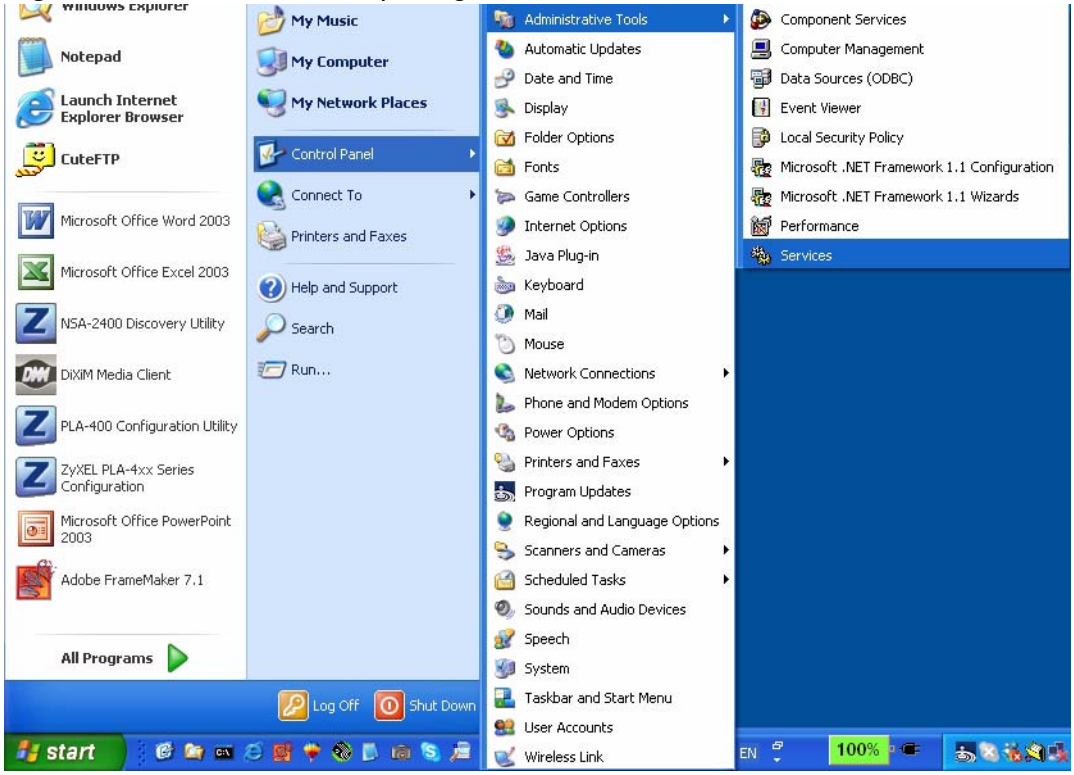
# Displaying Anti-Virus Alert Messages in Windows

With the anti-virus packet scan, when a virus is detected, you can have the ZyWALL display an alert message on Miscrosoft Windows-based computers. If the log shows that virus files are being detected but your Miscrosoft Windows-based computer is not displaying an alert message, use one of the following procedures to make sure your computer is set to display the messages.

## Windows XP

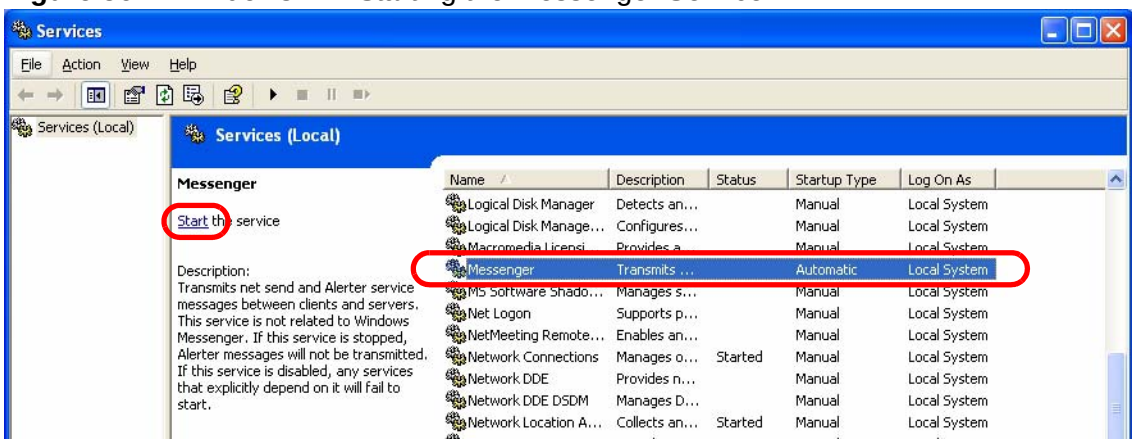
1 Click **Start > Control Panel > Administrative Tools > Services**.

**Figure 566** Windows XP: Opening the Services Window



2 Select the **Messenger** service and click **Start**.

**Figure 567** Windows XP: Starting the Messenger Service

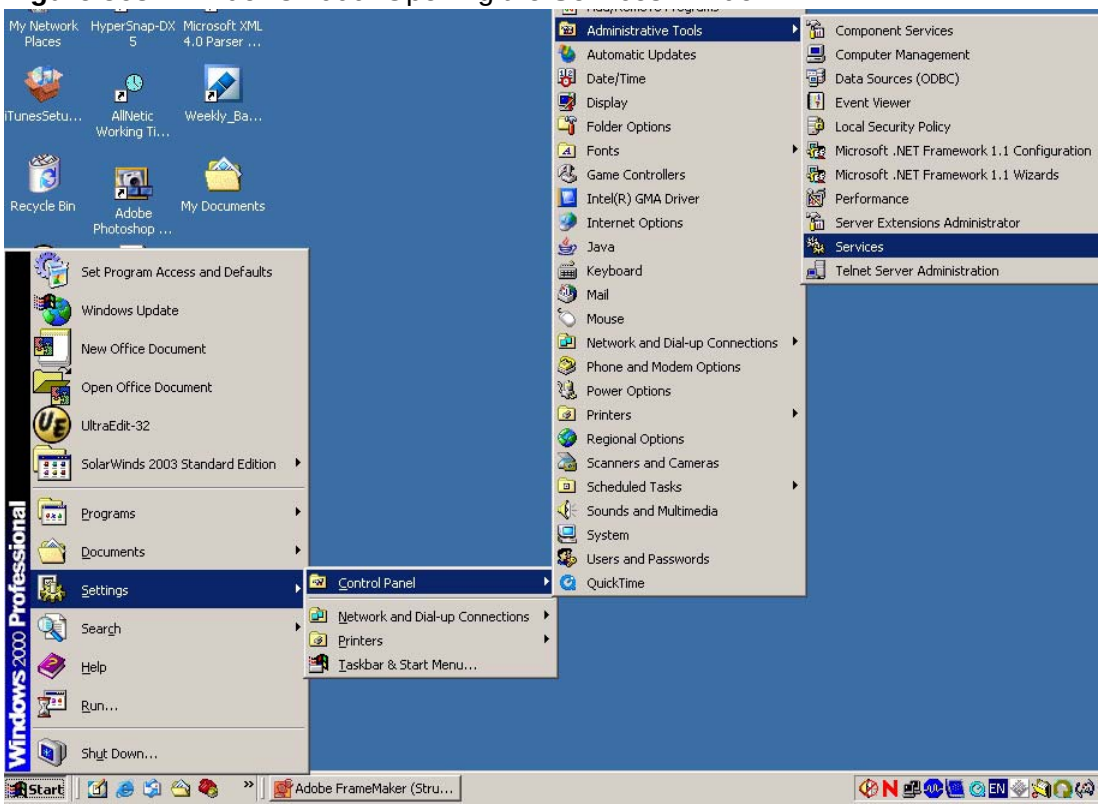



3 Close the window when you are done.

## Windows 2000

1 Click **Start > Settings > Control Panel > Administrative Tools > Services**.

**Figure 568** Windows 2000: Opening the Services Window



2 Select the **Messenger** service and click **Start Service**.

**Figure 569** Windows 2000: Starting the Messenger Service


3 Close the window when you are done.

## Windows 98 SE/Me

For Windows 98 SE/Me, you must open the **WinPopup** window in order to view real-time alert messages.

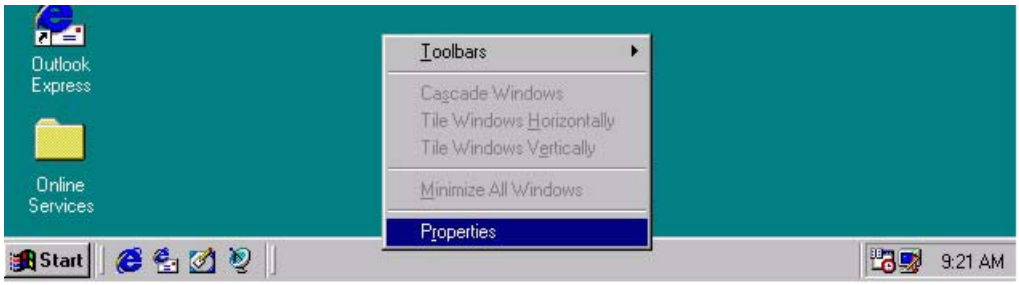
Click **Start** > **Run** and enter “winpopup” in the field provided and click **OK**. The **WinPopup** window displays as shown.

**Figure 570** Windows 98 SE: WinPopup


If you want to display the WinPopup window at startup, follow the steps below for Windows 98 SE (steps are similar for Windows Me).

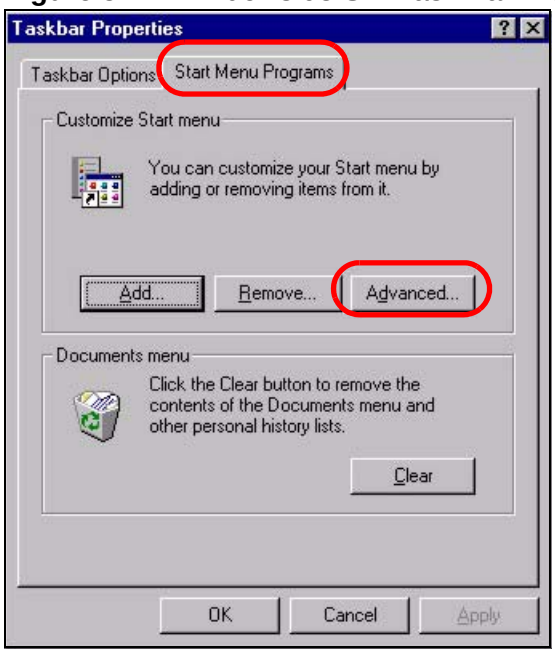
1 Right-click on the program task bar and click **Properties**.

**Figure 571** WIndows 98 SE: Program Task Bar




2 Click the **Start Menu Programs** tab and click **Advanced ...**.

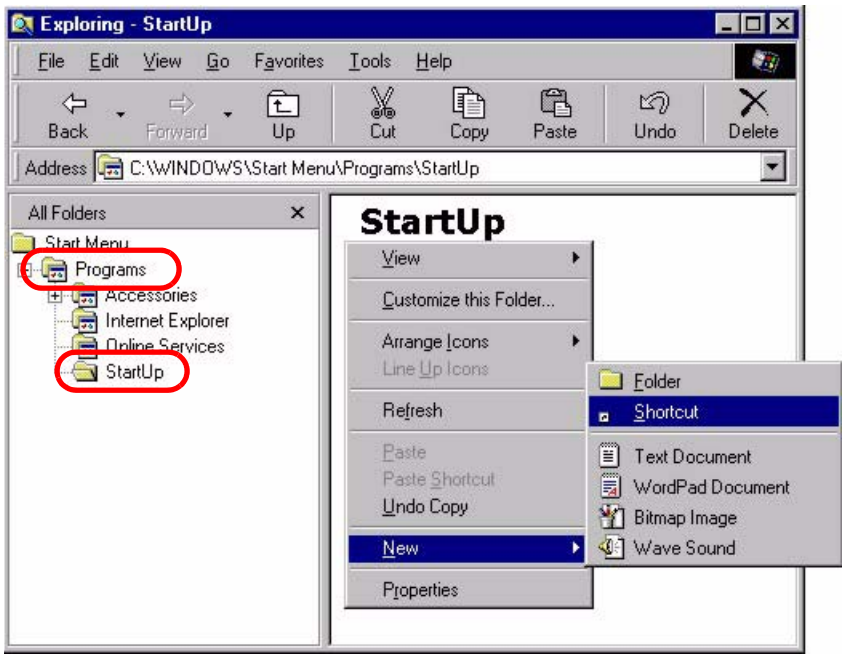
**Figure 572** Windows 98 SE: Task Bar Properties




3 Double-click **Programs** and click **StartUp**.

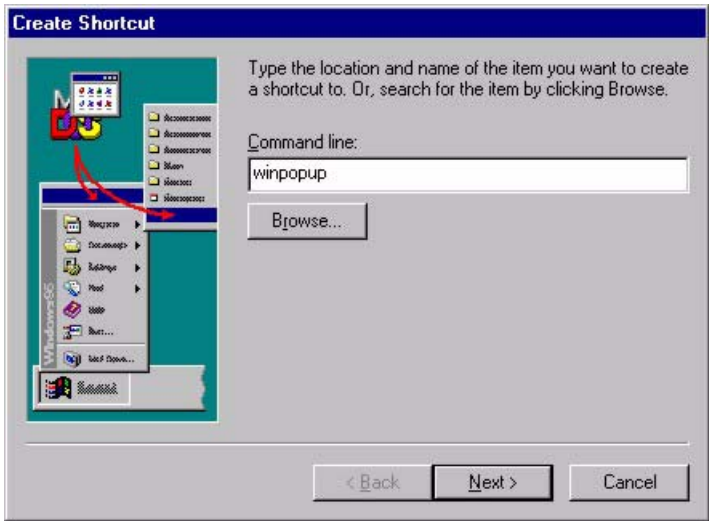
4 Right-click in the **StartUp** pane and click **New**, **Shortcut**.

**Figure 573** Windows 98 SE: StartUp



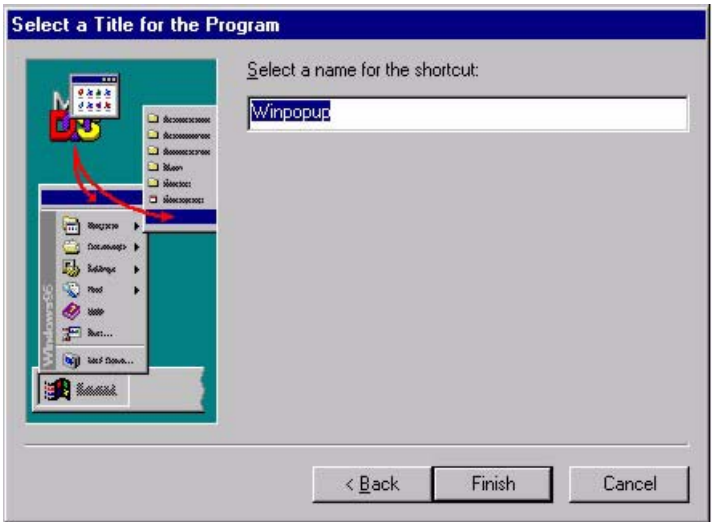

5 A **Create Shortcut** window displays. Enter “winpopup” in the **Command line** field and click **Next**.

**Figure 574** Windows 98 SE: Startup: Create Shortcut



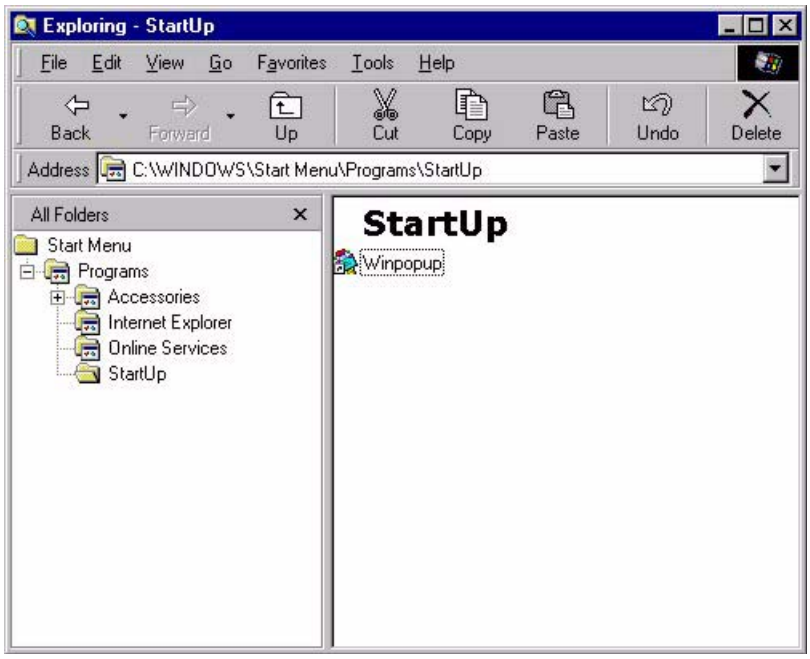
6 Specify a name for the shortcut or accept the default and click **Finish**.

**Figure 575** Windows 98 SE: Startup: Select a Title for the Program




7 A shortcut is created in the **StartUp** pane. Restart the computer when prompted.

**Figure 576** Windows 98 SE: Startup: Shortcut




Note: The WinPopup window displays after the computer finishes the startup process (see Figure 570 on page 911).

D

# Importing Certificates

This appendix shows you how to import public key certificates into your web browser.

Public key certificates are used by web browsers to ensure that a secure web site is legitimate. When a certificate authority such as VeriSign, Comodo, or Network Solutions, to name a few, receives a certificate request from a website operator, they confirm that the web domain and contact information in the request match those on public record with a domain name registrar. If they match, then the certificate is issued to the website operator, who then places it on the site to be issued to all visiting web browsers to let them know that the site is legitimate.

Many ZyXEL products, such as the NSA-2401, issue their own public key certificates. These can be used by web browsers on a LAN or WAN to verify that they are in fact connecting to the legitimate device and not one masquerading as it. However, because the certificates were not issued by one of the several organizations officially recognized by the most common web browsers, you will need to import the ZyXEL-created certificate into your web browser and flag that certificate as a trusted authority.

Note: You can see if you are browsing on a secure website if the URL in your web browser's address bar begins with `https://` or there is a sealed padlock icon (  ) somewhere in the main browser window (not all browsers show the padlock in the same location.)

In this appendix, you can import a public key certificate for:

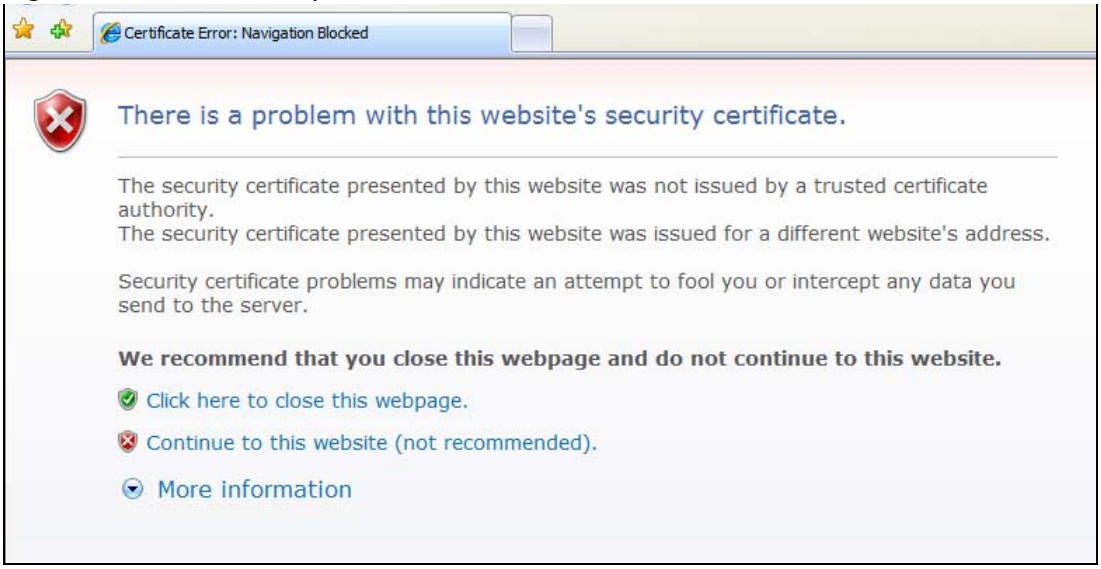


## Internet Explorer

The following example uses Microsoft Internet Explorer 7 on Windows XP Professional; however, they can also apply to Internet Explorer on Windows Vista.

1 If your device's Web Configurator is set to use SSL certification, then the first time you browse to it you are presented with a certification error.

**Figure 577** Internet Explorer 7: Certification Error

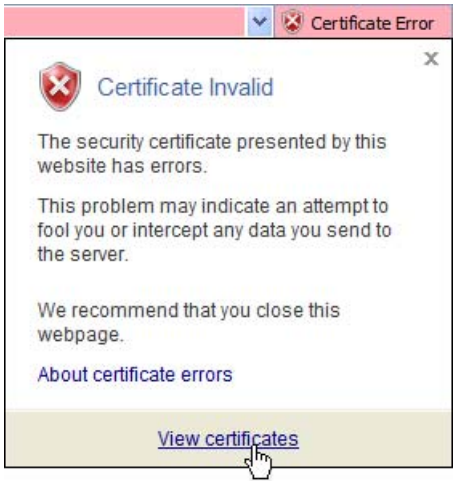



2 Click **Continue to this website (not recommended)**.

**Figure 578** Internet Explorer 7: Certification Error

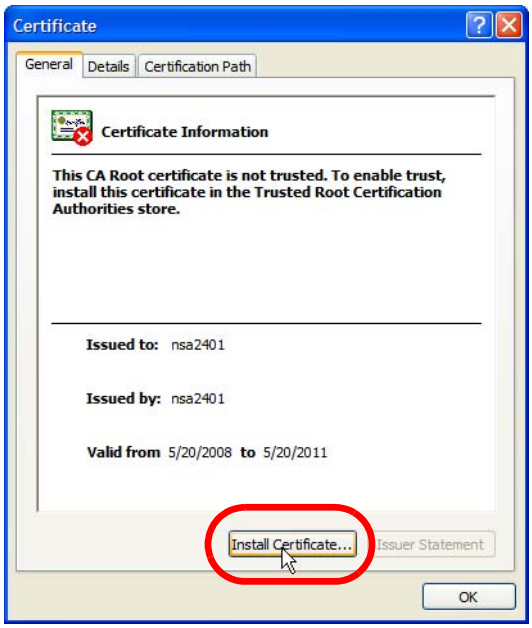

3 In the **Address Bar**, click **Certificate Error** > **View certificates**.

**Figure 579** Internet Explorer 7: Certificate Error



4 In the **Certificate** dialog box, click **Install Certificate**.

**Figure 580** Internet Explorer 7: Certificate

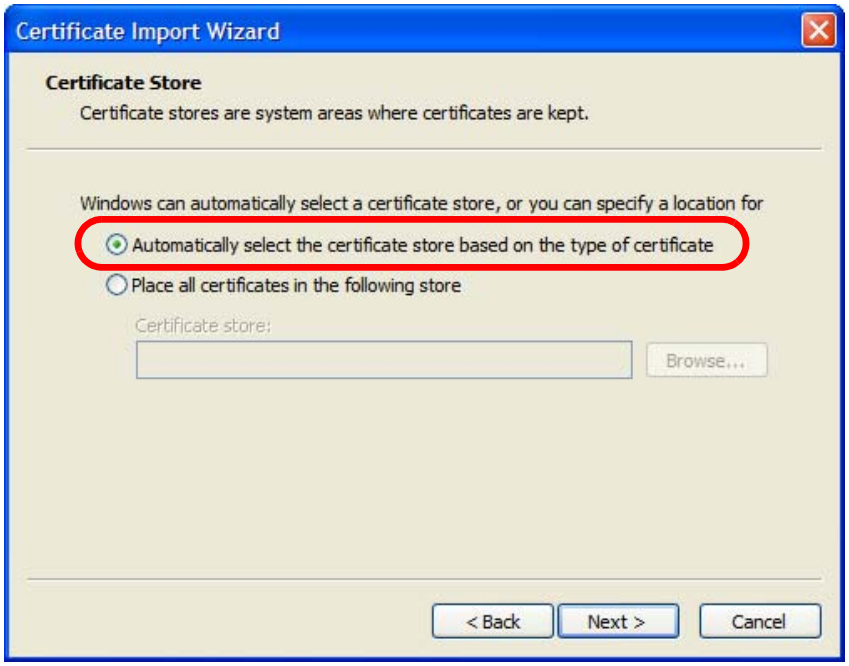



5 In the **Certificate Import Wizard**, click **Next**.

**Figure 581** Internet Explorer 7: Certificate Import Wizard

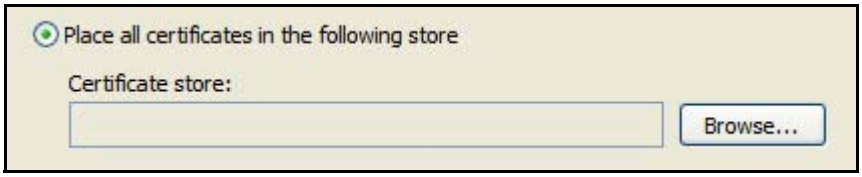
6 If you want Internet Explorer to **Automatically select certificate store based on the type of certificate**, click **Next** again and then go to step 9.

**Figure 582** Internet Explorer 7: Certificate Import Wizard




7 Otherwise, select **Place all certificates in the following store** and then click **Browse**.

**Figure 583** Internet Explorer 7: Certificate Import Wizard

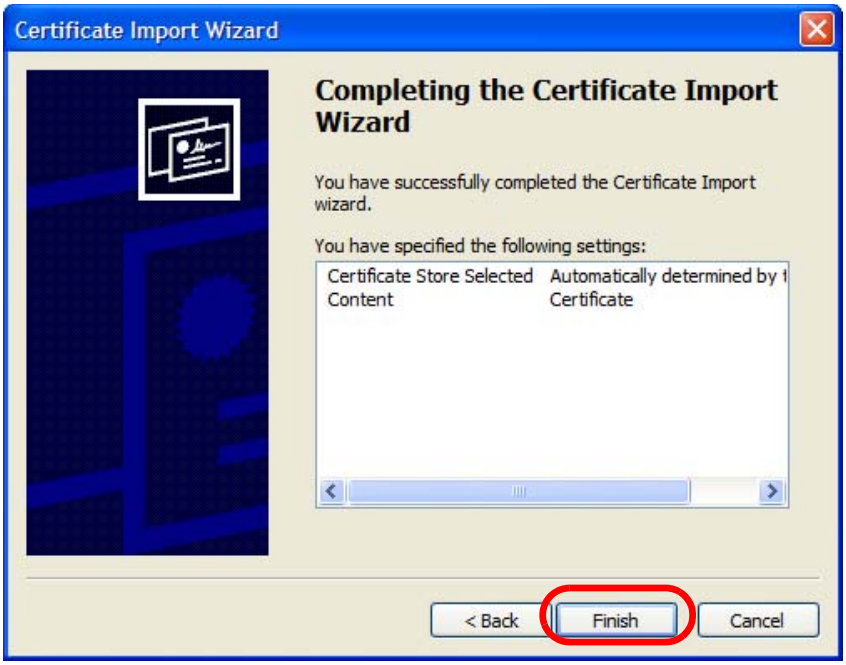


8 In the **Select Certificate Store** dialog box, choose a location in which to save the certificate and then click **OK**.

**Figure 584** Internet Explorer 7: Select Certificate Store


9 In the **Completing the Certificate Import Wizard** screen, click **Finish**.

**Figure 585** Internet Explorer 7: Certificate Import Wizard



10 If you are presented with another **Security Warning**, click **Yes**.

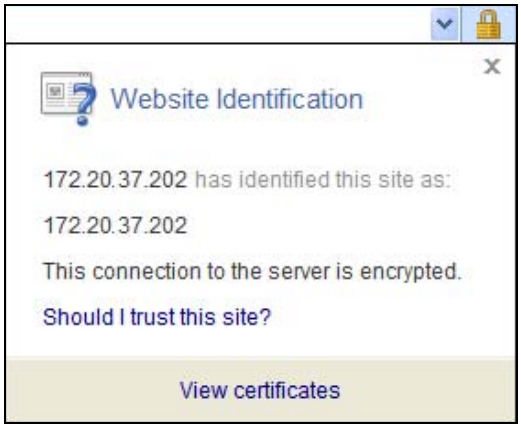
**Figure 586** Internet Explorer 7: Security Warning


11 Finally, click **OK** when presented with the successful certificate installation message.

**Figure 587** Internet Explorer 7: Certificate Import Wizard


12 The next time you start Internet Explorer and go to a ZyXEL Web Configurator page, a sealed padlock icon appears in the address bar. Click it to view the page's **Website Identification** information.

**Figure 588** Internet Explorer 7: Website Identification



## Installing a Stand-Alone Certificate File in Internet Explorer

Rather than browsing to a ZyXEL Web Configurator and installing a public key certificate when prompted, you can install a stand-alone certificate file if one has been issued to you.

1 Double-click the public key certificate file.

**Figure 589** Internet Explorer 7: Public Key Certificate File


2 In the security warning dialog box, click **Open**.

**Figure 590** Internet Explorer 7: Open File - Security Warning


3 Refer to steps 4-12 in the Internet Explorer procedure beginning on page 915 to complete the installation process.

## Removing a Certificate in Internet Explorer

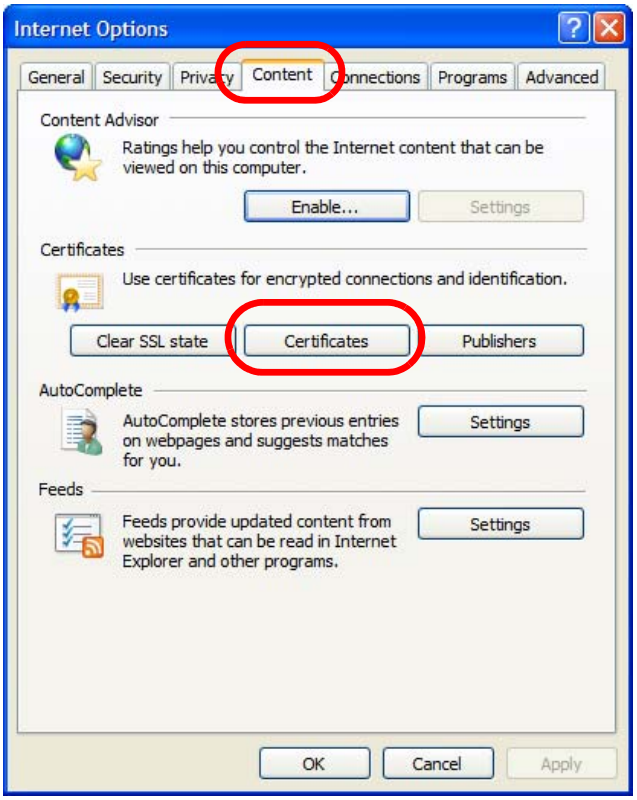
This section shows you how to remove a public key certificate in Internet Explorer 7.

1 Open **Internet Explorer** and click **Tools > Internet Options**.

**Figure 591** Internet Explorer 7: Tools Menu

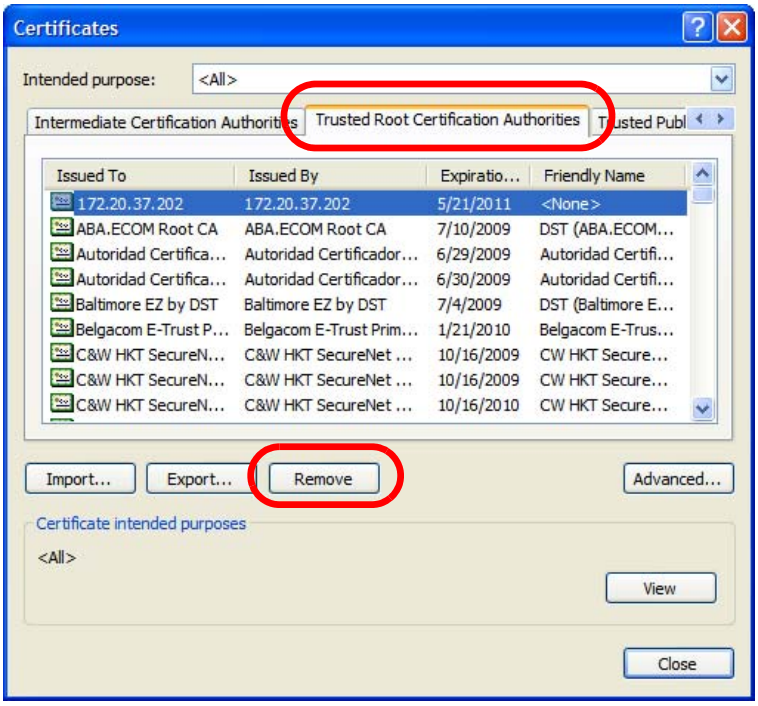

2 In the **Internet Options** dialog box, click **Content** > **Certificates**.

**Figure 592** Internet Explorer 7: Internet Options



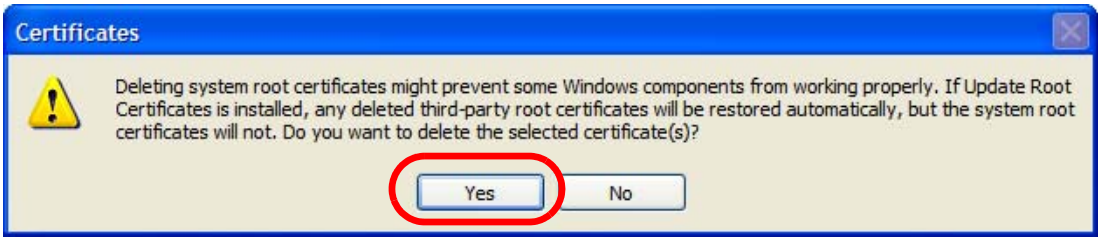
3 In the **Certificates** dialog box, click the **Trusted Root Certificates Authorities** tab, select the certificate that you want to delete, and then click **Remove**.

**Figure 593** Internet Explorer 7: Certificates



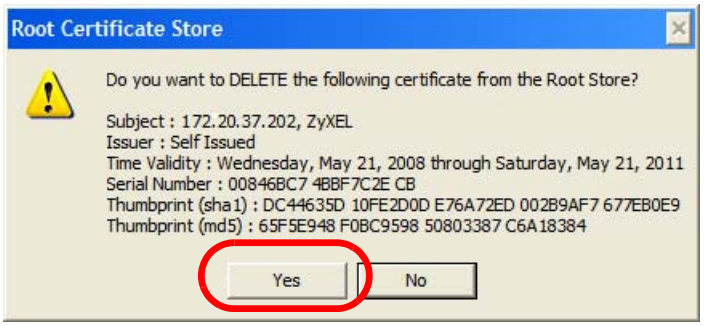

4 In the **Certificates** confirmation, click **Yes**.

**Figure 594** Internet Explorer 7: Certificates




5 In the **Root Certificate Store** dialog box, click **Yes**.

**Figure 595** Internet Explorer 7: Root Certificate Store



6 The next time you go to the web site that issued the public key certificate you just removed, a certification error appears.

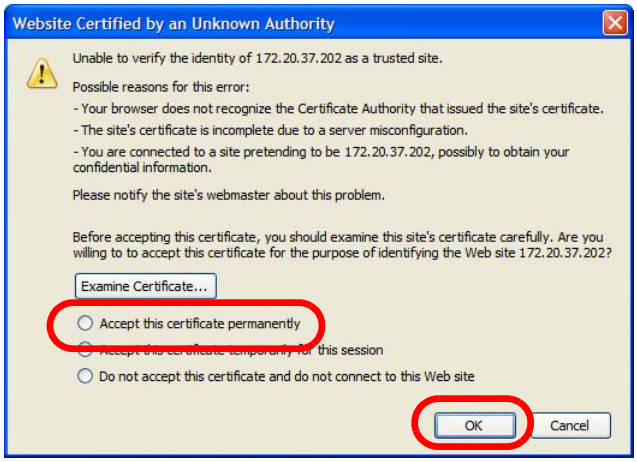
## Firefox

The following example uses Mozilla Firefox 2 on Windows XP Professional; however, the screens can also apply to Firefox 2 on all platforms.

1 If your device's Web Configurator is set to use SSL certification, then the first time you browse to it you are presented with a certification error.

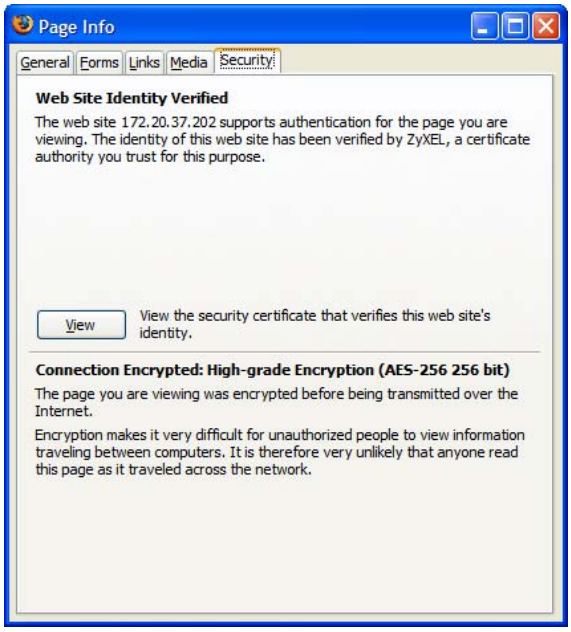
2 Select **Accept this certificate permanently** and click **OK.**

**Figure 596** Firefox 2: Website Certified by an Unknown Authority



3 The certificate is stored and you can now connect securely to the Web Configurator. A sealed padlock appears in the address bar, which you can click to open the **Page Info > Security** window to view the web page's security information.

**Figure 597** Firefox 2: Page Info

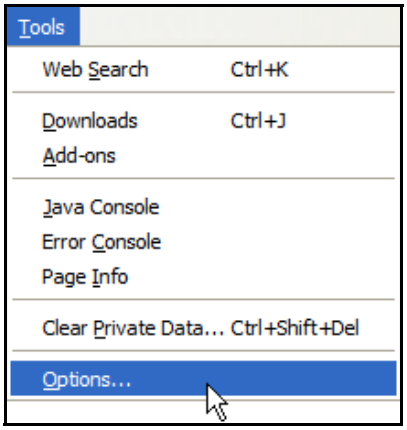



## Installing a Stand-Alone Certificate File in Firefox

Rather than browsing to a ZyXEL Web Configurator and installing a public key certificate when prompted, you can install a stand-alone certificate file if one has been issued to you.

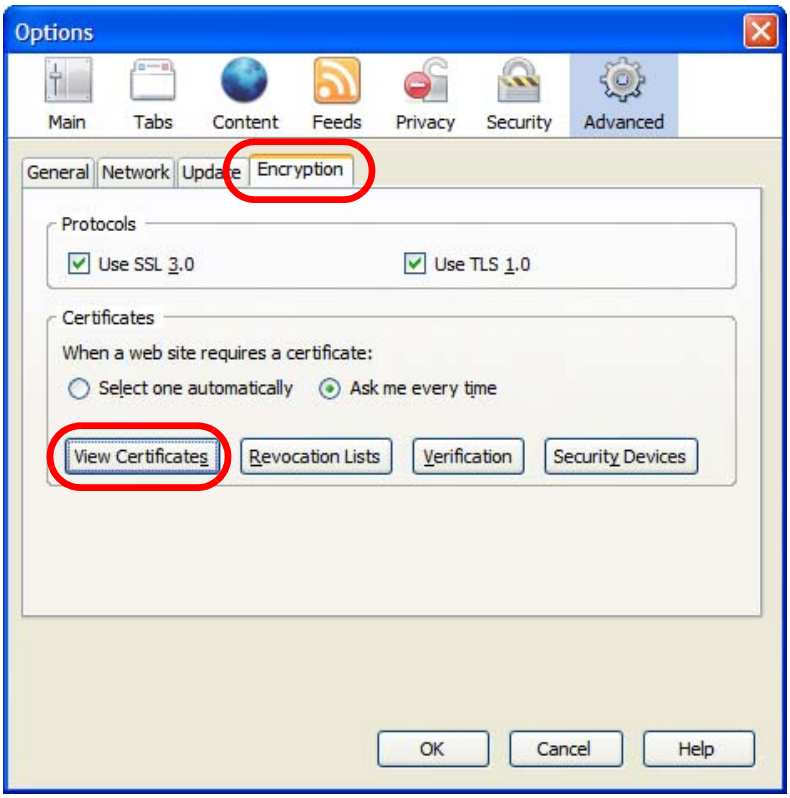
1 Open **Firefox** and click **Tools > Options**.

**Figure 598** Firefox 2: Tools Menu



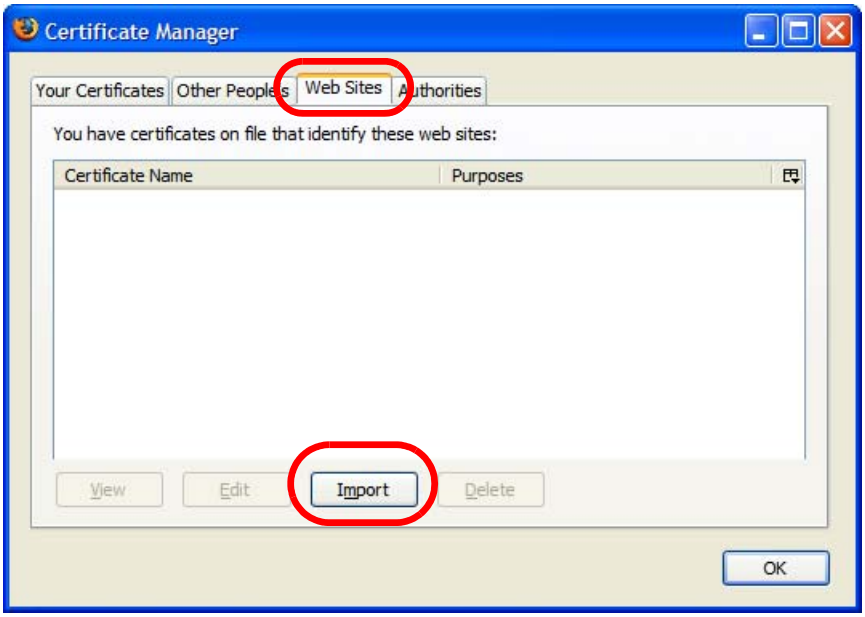

2 In the **Options** dialog box, click **Advanced** > **Encryption** > **View Certificates**.

**Figure 599** Firefox 2: Options



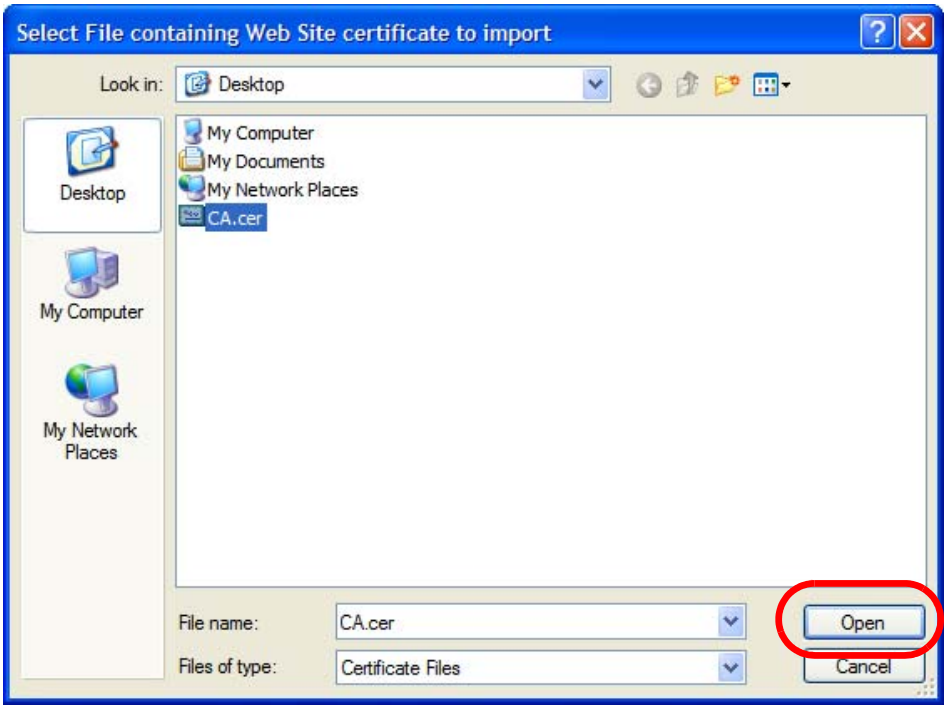
3 In the **Certificate Manager** dialog box, click **Web Sites** > **Import**.

**Figure 600** Firefox 2: Certificate Manager




4 Use the **Select File** dialog box to locate the certificate and then click **Open**.

**Figure 601** Firefox 2: Select File



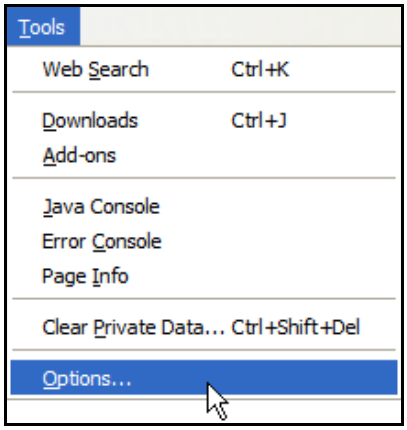

5 The next time you visit the web site, click the padlock in the address bar to open the **Page Info > Security** window to see the web page's security information.

## Removing a Certificate in Firefox

This section shows you how to remove a public key certificate in Firefox 2.

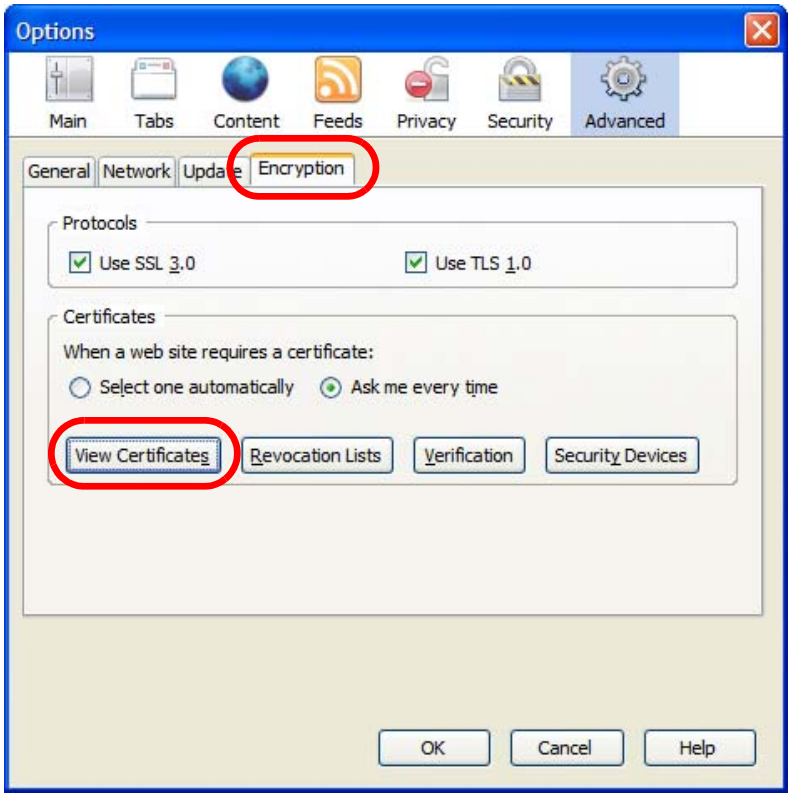
1 Open **Firefox** and click **Tools** > **Options**.

**Figure 602** Firefox 2: Tools Menu



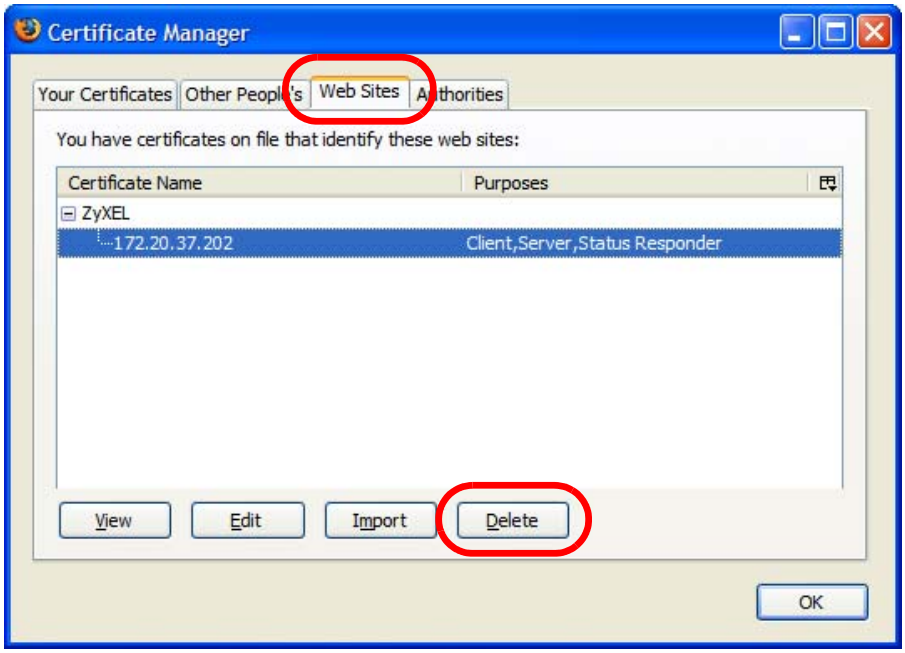

2 In the **Options** dialog box, click **Advanced** > **Encryption** > **View Certificates**.

**Figure 603** Firefox 2: Options



3 In the **Certificate Manager** dialog box, select the **Web Sites** tab, select the certificate that you want to remove, and then click **Delete**.

**Figure 604** Firefox 2: Certificate Manager




4 In the **Delete Web Site Certificates** dialog box, click **OK**.

**Figure 605** Firefox 2: Delete Web Site Certificates


5 The next time you go to the web site that issued the public key certificate you just removed, a certification error appears.

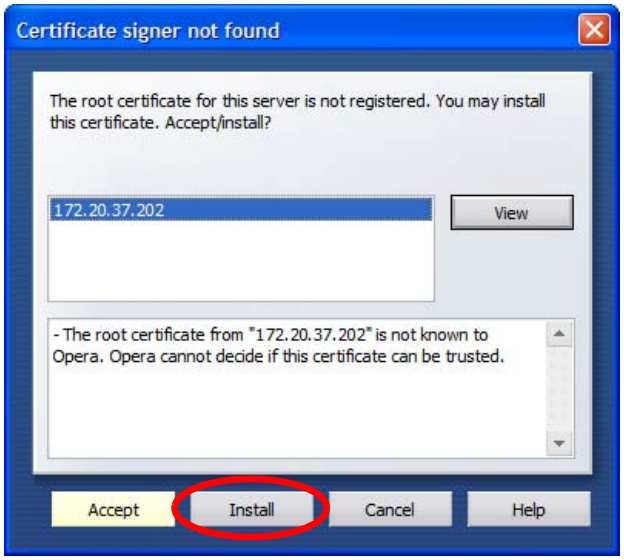
# Opera

The following example uses Opera 9 on Windows XP Professional; however, the screens can apply to Opera 9 on all platforms.

1 If your device's Web Configurator is set to use SSL certification, then the first time you browse to it you are presented with a certification error.

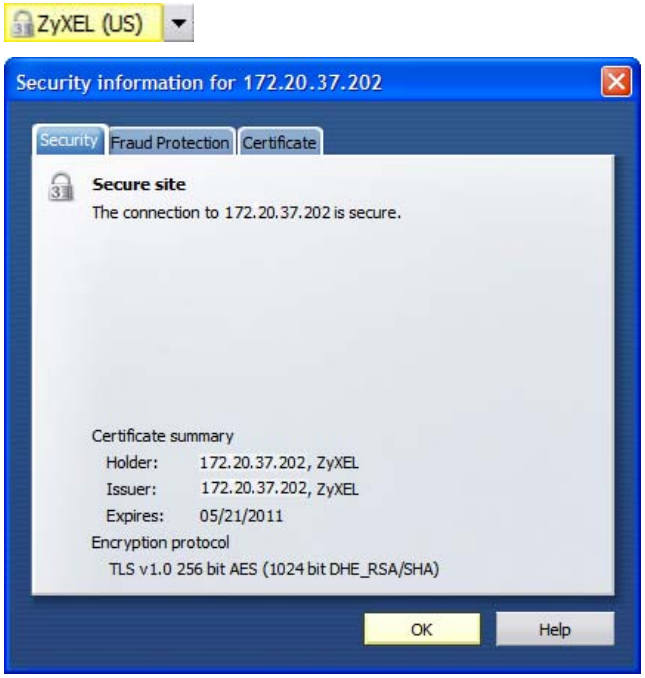
2 Click **Install** to accept the certificate.

**Figure 606** Opera 9: Certificate signer not found




3 The next time you visit the web site, click the padlock in the address bar to open the **Security information** window to view the web page's security details.

**Figure 607** Opera 9: Security information

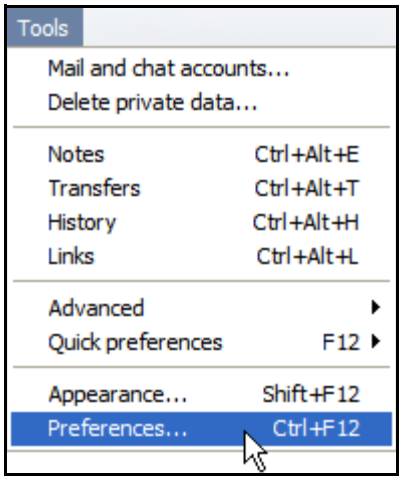


## Installing a Stand-Alone Certificate File in Opera

Rather than browsing to a ZyXEL Web Configurator and installing a public key certificate when prompted, you can install a stand-alone certificate file if one has been issued to you.

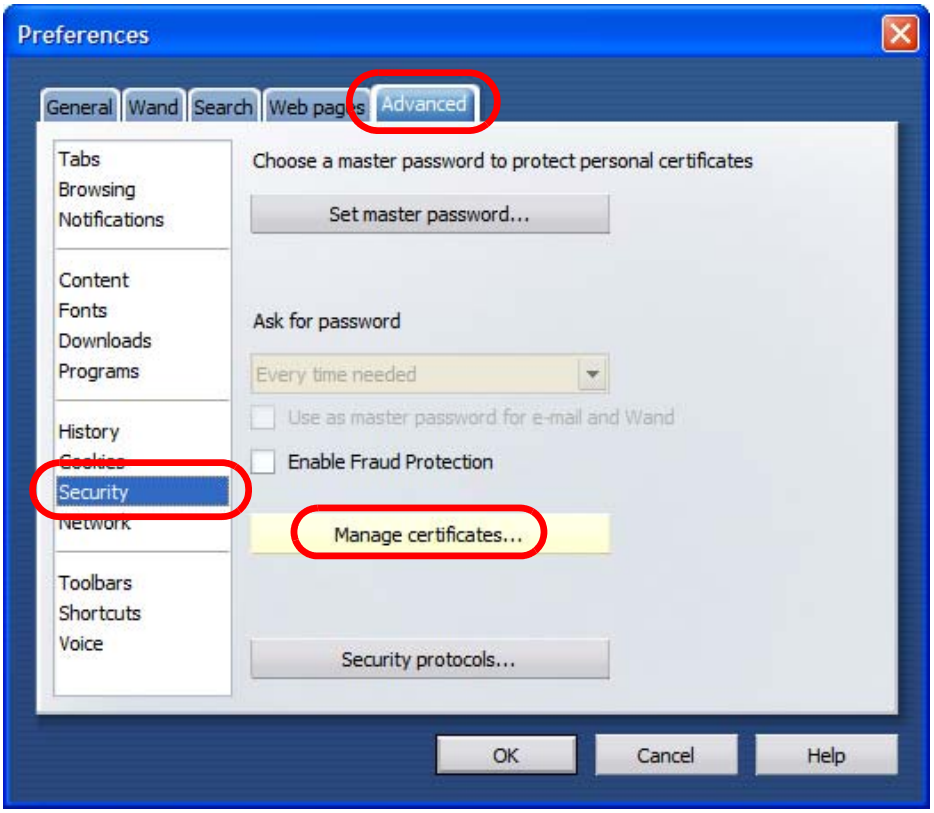
1 Open **Opera** and click **Tools** > **Preferences**.

**Figure 608** Opera 9: Tools Menu



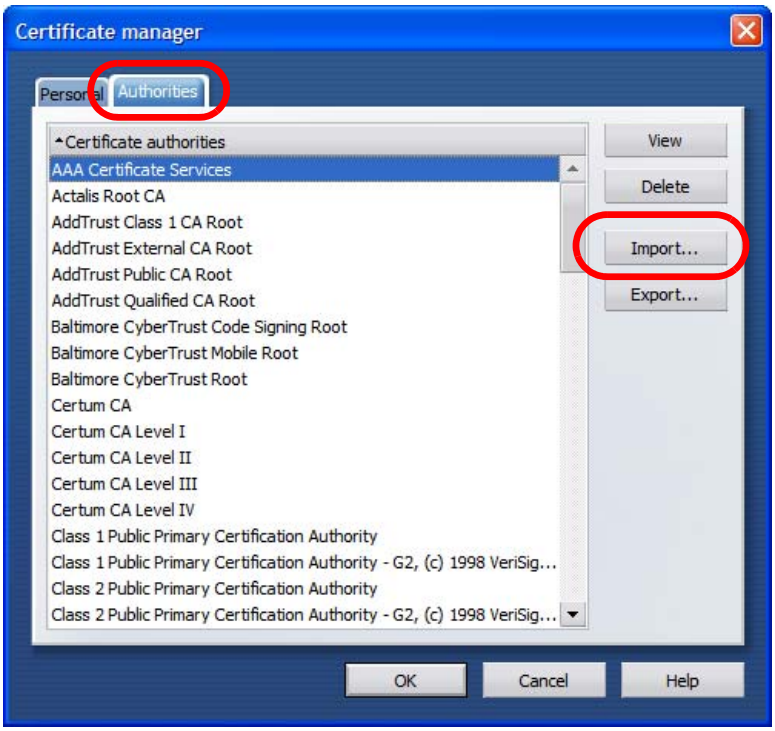
2 In **Preferences**, click **Advanced** > **Security** > **Manage certificates**.

**Figure 609** Opera 9: Preferences



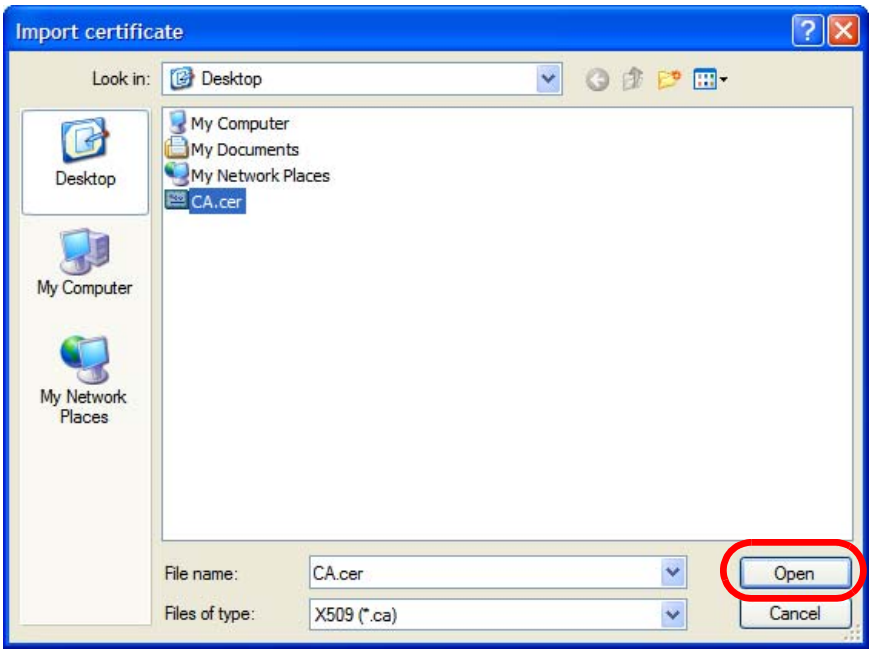
3 In the **Certificates Manager**, click **Authorities** > **Import**.

**Figure 610** Opera 9: Certificate manager



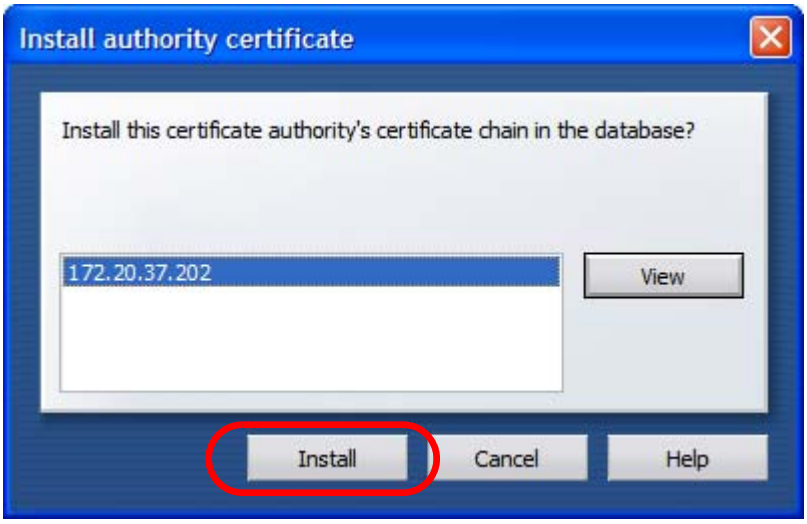

4 Use the **Import certificate** dialog box to locate the certificate and then click **Open.**

**Figure 611** Opera 9: Import certificate



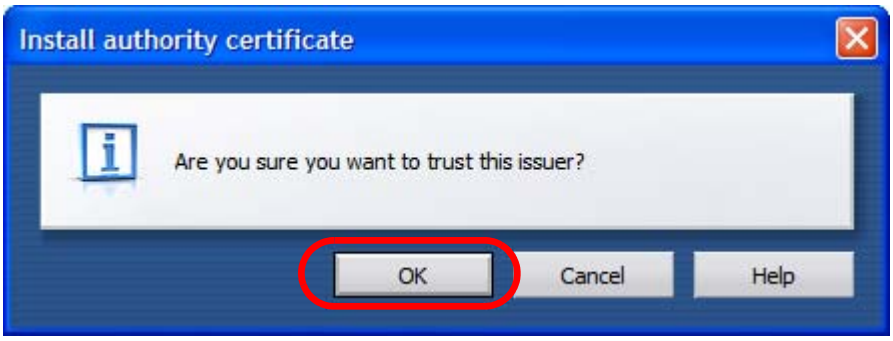
5 In the **Install authority certificate** dialog box, click **Install**.

**Figure 612** Opera 9: Install authority certificate




6 Next, click **OK**.

**Figure 613** Opera 9: Install authority certificate



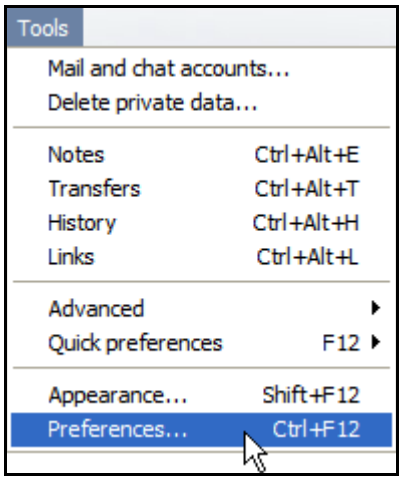

7 The next time you visit the web site, click the padlock in the address bar to open the **Security information** window to view the web page's security details.

## Removing a Certificate in Opera

This section shows you how to remove a public key certificate in Opera 9.

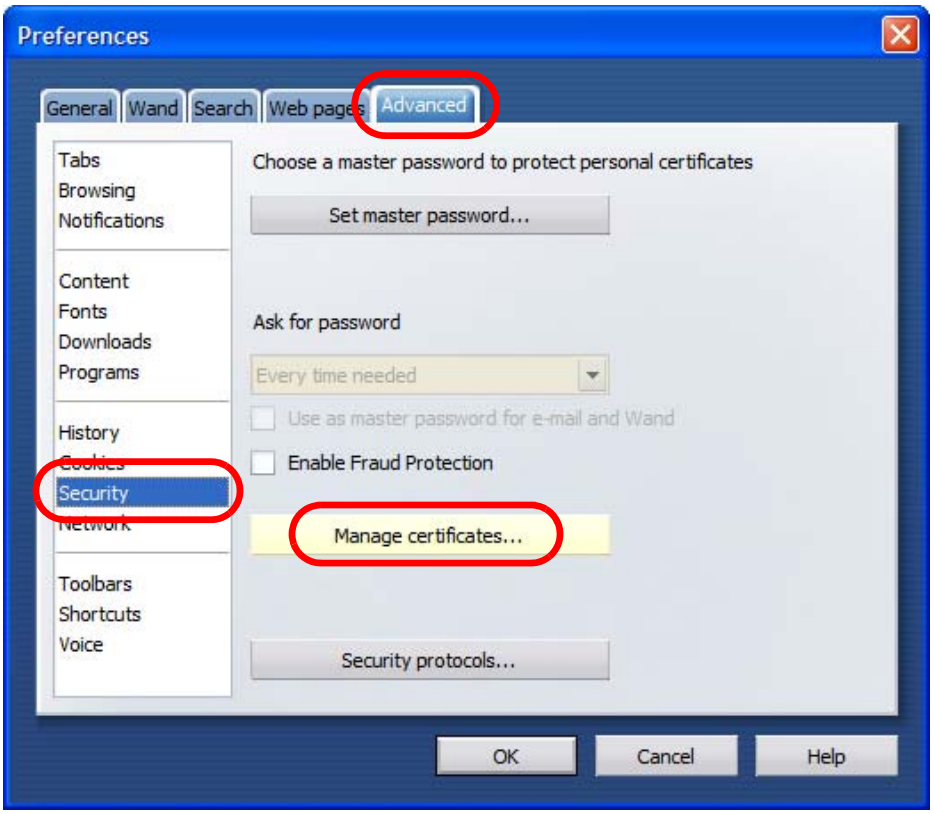
1 Open **Opera** and click **Tools** > **Preferences**.

**Figure 614** Opera 9: Tools Menu



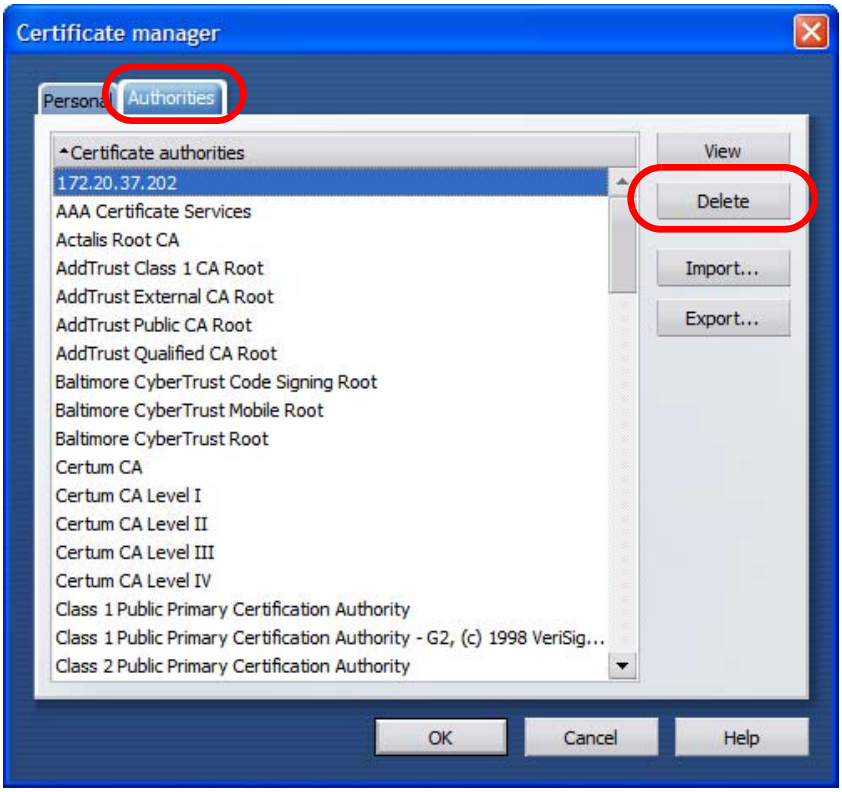

2 In **Preferences**, **Advanced** > **Security** > **Manage certificates**.

**Figure 615** Opera 9: Preferences



3 In the **Certificates manager**, select the **Authorities** tab, select the certificate that you want to remove, and then click **Delete**.

**Figure 616** Opera 9: Certificate manager




4 The next time you go to the web site that issued the public key certificate you just removed, a certification error appears.

Note: There is no confirmation when you delete a certificate authority, so be absolutely certain that you want to go through with it before clicking the button.

## Konqueror

The following example uses Konqueror 3.5 on openSUSE 10.3, however the screens apply to Konqueror 3.5 on all Linux KDE distributions.

1 If your device's Web Configurator is set to use SSL certification, then the first time you browse to it you are presented with a certification error.

2 Click **Continue**.

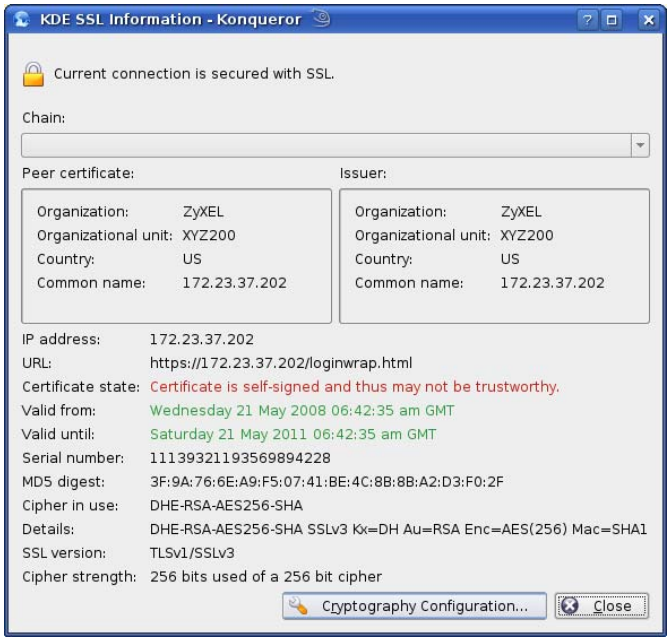
**Figure 617** Konqueror 3.5: Server Authentication


3 Click **Forever** when prompted to accept the certificate.

**Figure 618** Konqueror 3.5: Server Authentication


4 Click the padlock in the address bar to open the **KDE SSL Information** window and view the web page's security details.

**Figure 619** Konqueror 3.5: KDE SSL Information



## Installing a Stand-Alone Certificate File in Konqueror

Rather than browsing to a ZyXEL Web Configurator and installing a public key certificate when prompted, you can install a stand-alone certificate file if one has been issued to you.

1 Double-click the public key certificate file.

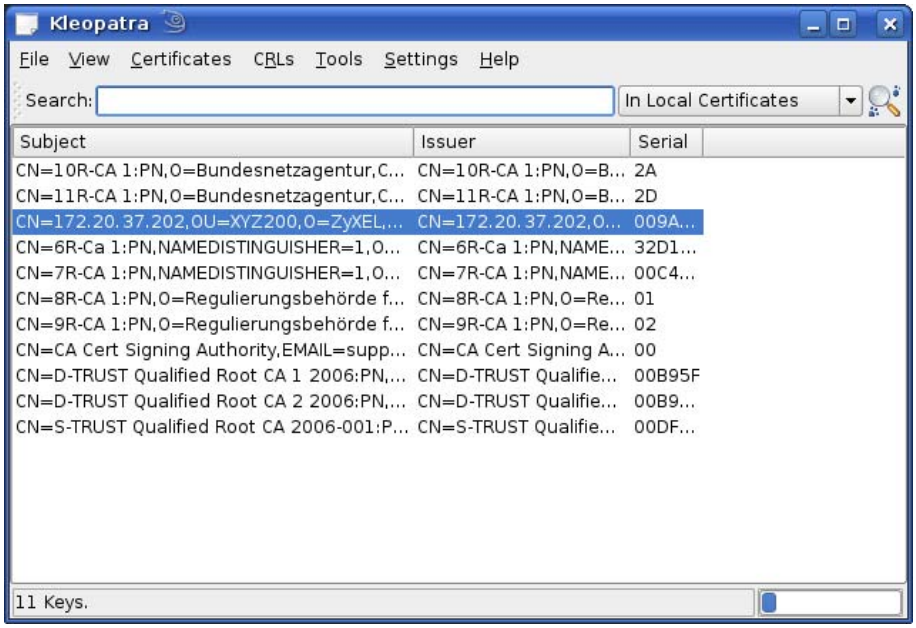
**Figure 620** Konqueror 3.5: Public Key Certificate File


2 In the **Certificate Import Result - Kleopatra** dialog box, click **OK**.

**Figure 621** Konqueror 3.5: Certificate Import Result


The public key certificate appears in the KDE certificate manager, **Kleopatra**.

**Figure 622** Konqueror 3.5: Kleopatra



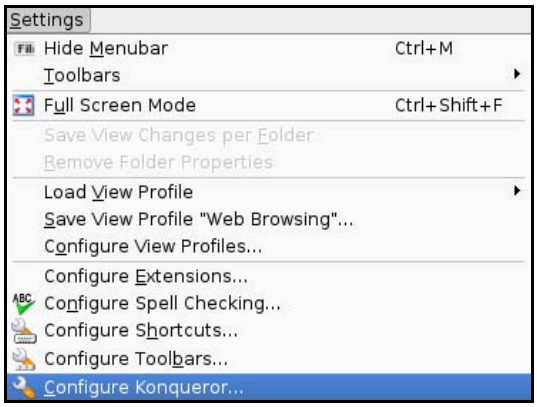
3 The next time you visit the web site, click the padlock in the address bar to open the **KDE SSL Information** window to view the web page's security details.

## Removing a Certificate in Konqueror

This section shows you how to remove a public key certificate in Konqueror 3.5.

1 Open **Konqueror** and click **Settings > Configure Konqueror**.

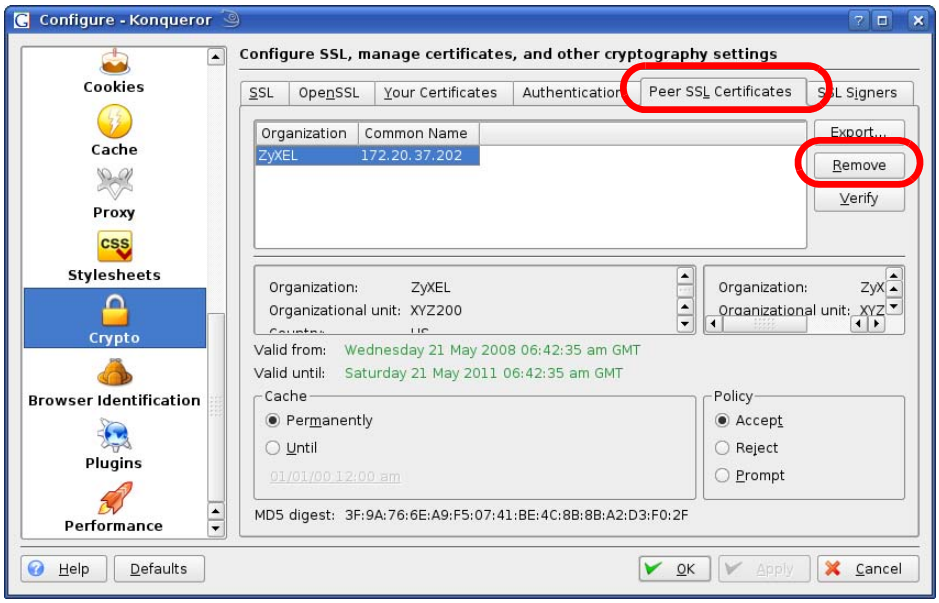
**Figure 623** Konqueror 3.5: Settings Menu




2 In the **Configure** dialog box, select **Crypto**.

3 On the **Peer SSL Certificates** tab, select the certificate you want to delete and then click **Remove**.

**Figure 624** Konqueror 3.5: Configure



4 The next time you go to the web site that issued the public key certificate you just removed, a certification error appears.

Note: There is no confirmation when you remove a certificate authority, so be absolutely certain you want to go through with it before clicking the button.

E

# Open Software Announcements

## Notice

Information herein is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, except the express written permission of ZyXEL Communications Corporation.

Note: This Product includes ppp-2.4.2 software under the PPP License

### PPP License

Copyright (c) 1993 The Australian National University.
All rights reserved.

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the Australian National University. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Copyright (c) 1989 Carnegie Mellon University.
All rights reserved.

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by Carnegie Mellon University. The name of the University may not be used to endorse or promote products derived from this software without specific prior

written permission. THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Note: This Product includes Netkit Telnet -0.17 software under the Netkit Telnet License

## Netkit Telnet License

Copyright (c) 1989 Regents of the University of California.
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1.Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2.Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3.Neither the name of the project nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Note: This Product includes ntp-4.1.2 software under the NTP License

## NTP License

Copyright (c) David L. Mills 1992-2004

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that

the above copyright notice appears in all copies and that both the copyright notice and this permission notice appear in supporting documentation, and that the name University of Delaware not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. The University of Delaware makes no representations about the suitability this software for any purpose. It is provided "as is" without express or implied warranty.

Note: This Product includes expat-1.95.6 software under the Expat License

### Expat License

Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.

IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Note: This Product includes libtecla-1.6.1 software under the an X11-style License

### an X11-style license

This *is* a Free Software License

- This license is compatible with The GNU General Public License, Version 1
- This license is compatible with The GNU General Public License, Version 2

This is just like a Simple Permissive license, but it requires that a copyright notice be maintained.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

Note: This Product includes openssl-0.9.8d-ocf software under the OpenSSL License

## OpenSSL

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

## OpenSSL License

Copyright (c) 1998-2007 The OpenSSL Project. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may “OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

## Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved. This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL. This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic

software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

Note: This Product includes libevent-1.1a and xinetd-2.3.14 software under the a 3-clause BSD License

## a 3-clause BSD-style license

This is a Free Software License

- This license is compatible with The GNU General Public License, Version 1
- This license is compatible with The GNU General Public License, Version 2

This is the BSD license without the obnoxious advertising clause. It's also known as the "modified BSD license." Note that the University of California now prefers this license to the BSD license with advertising clause, and now allows BSD itself to be used under the three-clause license.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of [original copyright holder] nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Note: This Product includes bind-9.2.3 software under the Internet Software Consortium and Nominum License

Copyright (C) 1996-2002 Internet Software Consortium.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND INTERNET SOFTWARE CONSORTIUM DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL INTERNET SOFTWARE CONSORTIUM BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

$Id: COPYRIGHT,v 1.6.2.2 2002/02/12 06:05:48 marka Exp $

Portions Copyright (C) 1996-2001 Nominum, Inc.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND NOMINUM DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL NOMINUM BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Note: This Product includes dhcp-3.0.3 software under the ISC License

### ISC license

Copyright (c) 2004-2005 by Internet Systems Consortium, Inc. ("ISC")

Copyright (c) 1995-2003 by Internet Software Consortium

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Internet Systems Consortium, Inc.

950 Charter Street

Redwood City, CA 94063

<info@isc.org>

http://www.isc.org/

Note: This Product includes httpd-2.0.55 software developed by the Apache Software Foundation under Apache License.

### Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed

by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works hereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works;

within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or

rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

Version 1.1



Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

The end-user documentation included with the redistribution, if any, must include the following acknowledgment: “This product includes software developed by the Apache Software Foundation (http://www.apache.org/).” Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.

The names “Apache” and “Apache Software Foundation” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact apache@apache.org.

Products derived from this software may not be called “Apache”, nor may “Apache” appear in their name, without prior written permission of the Apache Software Foundation.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation. For more information on the Apache Software Foundation, please see <http://www.apache.org/>.

Portions of this software are based upon public domain software originally written at the National Center for Supercomputing Applications, University of Illinois, Urbana-Champaign.

Note: This Product includes libosip2, libgcgi-0.9.5 and gmp-4.1 software under LGPL license.

## GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. [This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get

it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions

translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License. In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License").

Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables. The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library. Activities other than copying, distribution and modification are not covered by this License; they

are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions: a) The modified work must itself be a software library. b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change. c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License. d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful. (For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.) These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote

it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library. In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices. Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy. This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange. If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not

compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables. When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law. If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.) Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications. You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things: a) Accompany the work with the complete corresponding

machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.) b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with. c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution. d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place. e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy. For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate

distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things: a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above. b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the

wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR

CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCHDAMAGES.

END OF TERMS AND CONDITIONS.

Note: This Product includes bridge-utils 0.9.5, dhcpcd-1.3.22-pl4, pptp-linux-1.4.0, rp-pppoe-3.5, vlan-1.8, keepalived-1.1.11-p1, dietlibc 0.27, quagga-0.99.2, ez-ipupdate-3.0.11b7, libol-0.3.14, proftpd-1.2.10, syslog-ng-1.6.5, pam-0.76, tzcode2006c, iproute2, iptables-1.2.11/netfilter(kernel), dhcp-helper, busybox, Linux kernel, hostapd-0.5.7, wireless_tools.28, arp-sk-0.0.16, pcmcia-cs-3.2.8, libeeprog, mgetty-1.1.35, and ipset software under GPL license.

## GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you

modify it. For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software. Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you". Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program. In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code,

to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.) The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the

scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this

License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE

LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

All other trademarks or trade names mentioned herein, if any, are the property of their respective owners.

Note: This Product includes pcmcia-cs-3.2.8 software under MPL license.

## Mozilla Public License Version 1.1

1. Definitions.

1.0.1. "Commercial Use"

means distribution or otherwise making the Covered Code available to a third party.

1.1. "Contributor"

means each entity that creates or contributes to the creation of Modifications.

1.2. "Contributor Version"

means the combination of the Original Code, prior Modifications used by a Contributor, and the Modifications made by that particular Contributor.

1.3. "Covered Code"

means the Original Code or Modifications or the combination of the Original Code and Modifications, in each case including portions thereof.

1.4. "Electronic Distribution Mechanism"

means a mechanism generally accepted in the software development community for the electronic transfer of data.

1.5. "Executable"

means Covered Code in any form other than Source Code.

1.6. "Initial Developer"

means the individual or entity identified as the Initial Developer in the Source Code notice required by Exhibit A.

1.7. "Larger Work"

means a work which combines Covered Code or portions thereof with code not governed by the terms of this License.

1.8. "License"

means this document.

1.8.1. "Licensable"

means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently acquired, any and all of the rights conveyed herein.

1.9. "Modifications"

means any addition to or deletion from the substance or structure of either the Original Code or any previous Modifications. When Covered Code is released as a series of files, a Modification is:

Any addition to or deletion from the contents of a file containing Original Code or previous Modifications.

Any new file that contains any part of the Original Code or previous Modifications.

1.10. "Original Code"

means Source Code of computer software code which is described in the Source Code notice required by Exhibit A as Original Code, and which, at the time of its release under this License is not already Covered Code governed by this License.

1.10.1. "Patent Claims"

means any patent claim(s), now owned or hereafter acquired, including without limitation, method, process, and apparatus claims, in any patent Licensable by grantor.

1.11. "Source Code"

means the preferred form of the Covered Code for making modifications to it, including all modules it contains, plus any associated interface definition files, scripts used to control compilation and installation of an Executable, or source code differential comparisons against either the Original Code or another well known, available Covered Code of the Contributor's choice. The Source Code can be in a compressed or archival form, provided the appropriate decompression or de-archiving software is widely available for no charge.

1.12. "You" (or "Your")

means an individual or a legal entity exercising rights under, and complying with all of the terms of, this License or a future version of this License issued under Section 6.1. For legal entities, "You" includes any entity which controls, is controlled by, or is under common control with You. For purposes of this definition, "control" means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

2. Source Code License.

2.1. The Initial Developer Grant.

The Initial Developer hereby grants You a world-wide, royalty-free, non-exclusive license, subject to third party intellectual property claims:

under intellectual property rights (other than patent or trademark) Licensable by Initial Developer to use, reproduce, modify, display, perform, sublicense and distribute the Original Code (or portions thereof) with or without Modifications, and/or as part of a Larger Work; and

under Patents Claims infringed by the making, using or selling of Original Code, to make, have made, use, practice, sell, and offer for sale, and/or otherwise dispose of the Original Code (or portions thereof).

the licenses granted in this Section 2.1 (a) and (b) are effective on the date Initial Developer first distributes Original Code under the terms of this License.

Notwithstanding Section 2.1 (b) above, no patent license is granted: 1) for code that You delete from the Original Code; 2) separate from the Original Code; or 3)

for infringements caused by: i) the modification of the Original Code or ii) the combination of the Original Code with other software or devices.

2.2. Contributor Grant.

Subject to third party intellectual property claims, each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license

under intellectual property rights (other than patent or trademark) Licensable by Contributor, to use, reproduce, modify, display, perform, sublicense and distribute the Modifications created by such Contributor (or portions thereof) either on an unmodified basis, with other Modifications, as Covered Code and/or as part of a Larger Work; and

under Patent Claims infringed by the making, using, or selling of Modifications made by that Contributor either alone and/or in combination with its Contributor Version (or portions of such combination), to make, use, sell, offer for sale, have made, and/or otherwise dispose of: 1) Modifications made by that Contributor (or portions thereof); and 2) the combination of Modifications made by that Contributor with its Contributor Version (or portions of such combination).

the licenses granted in Sections 2.2 (a) and 2.2 (b) are effective on the date Contributor first makes Commercial Use of the Covered Code.

Notwithstanding Section 2.2 (b) above, no patent license is granted: 1) for any code that Contributor has deleted from the Contributor Version; 2) separate from the Contributor Version; 3) for infringements caused by: i) third party modifications of Contributor Version or ii) the combination of Modifications made by that Contributor with other software (except as part of the Contributor Version) or other devices; or 4) under Patent Claims infringed by Covered Code in the absence of Modifications made by that Contributor.

3. Distribution Obligations.

3.1. Application of License.

The Modifications which You create or to which You contribute are governed by the terms of this License, including without limitation Section 2.2. The Source Code version of Covered Code may be distributed only under the terms of this License or a future version of this License released under Section 6.1, and You must include a copy of this License with every copy of the Source Code You distribute. You may not offer or impose any terms on any Source Code version that alters or restricts the applicable version of this License or the recipients' rights hereunder. However, You may include an additional document offering the additional rights described in Section 3.5.

3.2. Availability of Source Code.

Any Modification which You create or to which You contribute must be made available in Source Code form under the terms of this License either on the same media as an Executable version or via an accepted Electronic Distribution Mechanism to anyone to whom you made an Executable version available; and if made available via Electronic Distribution Mechanism, must remain available for at least twelve (12) months after the date it initially became available, or at least six (6) months after a subsequent version of that particular Modification has been made available to such recipients. You are responsible for ensuring that the Source Code version remains available even if the Electronic Distribution Mechanism is maintained by a third party.

3.3. Description of Modifications.

You must cause all Covered Code to which You contribute to contain a file documenting the changes You made to create that Covered Code and the date of any change. You must include a prominent statement that the Modification is derived, directly or indirectly, from Original Code provided by the Initial Developer and including the name of the Initial Developer in (a) the Source Code, and (b) in any notice in an Executable version or related documentation in which You describe the origin or ownership of the Covered Code.

3.4. Intellectual Property Matters

(a) Third Party Claims

If Contributor has knowledge that a license under a third party's intellectual property rights is required to exercise the rights granted by such Contributor under Sections 2.1 or 2.2, Contributor must include a text file with the Source Code distribution titled "LEGAL" which describes the claim and the party making the claim in sufficient detail that a recipient will know whom to contact. If Contributor obtains such knowledge after the Modification is made available as described in Section 3.2, Contributor shall promptly modify the LEGAL file in all copies Contributor makes available thereafter and shall take other steps (such as notifying appropriate mailing lists or newsgroups) reasonably calculated to inform those who received the Covered Code that new knowledge has been obtained.

(b) Contributor APIs

If Contributor's Modifications include an application programming interface and Contributor has knowledge of patent licenses which are reasonably necessary to implement that API, Contributor must also include this information in the legal file.

(c) Representations.

Contributor represents that, except as disclosed pursuant to Section 3.4 (a) above, Contributor believes that Contributor's Modifications are Contributor's

original creation(s) and/or Contributor has sufficient rights to grant the rights conveyed by this License.

3.5. Required Notices.

You must duplicate the notice in Exhibit A in each file of the Source Code. If it is not possible to put such notice in a particular Source Code file due to its structure, then You must include such notice in a location (such as a relevant directory) where a user would be likely to look for such a notice. If You created one or more Modification(s) You may add your name as a Contributor to the notice described in Exhibit A. You must also duplicate this License in any documentation for the Source Code where You describe recipients' rights or ownership rights relating to Covered Code. You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Code. However, You may do so only on Your own behalf, and not on behalf of the Initial Developer or any Contributor. You must make it absolutely clear than any such warranty, support, indemnity or liability obligation is offered by You alone, and You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of warranty, support, indemnity or liability terms You offer.

3.6. Distribution of Executable Versions.

You may distribute Covered Code in Executable form only if the requirements of Sections 3.1, 3.2, 3.3, 3.4 and 3.5 have been met for that Covered Code, and if You include a notice stating that the Source Code version of the Covered Code is available under the terms of this License, including a description of how and where You have fulfilled the obligations of Section 3.2. The notice must be conspicuously included in any notice in an Executable version, related documentation or collateral in which You describe recipients' rights relating to the Covered Code. You may distribute the Executable version of Covered Code or ownership rights under a license of Your choice, which may contain terms different from this License, provided that You are in compliance with the terms of this License and that the license for the Executable version does not attempt to limit or alter the recipient's rights in the Source Code version from the rights set forth in this License. If You distribute the Executable version under a different license You must make it absolutely clear that any terms which differ from this License are offered by You alone, not by the Initial Developer or any Contributor. You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of any such terms You offer.

3.7. Larger Works.

You may create a Larger Work by combining Covered Code with other code not governed by the terms of this License and distribute the Larger Work as a single

product. In such a case, You must make sure the requirements of this License are fulfilled for the Covered Code.

4. Inability to Comply Due to Statute or Regulation.

If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Code due to statute, judicial order, or regulation then You must: (a) comply with the terms of this License to the maximum extent possible; and (b) describe the limitations and the code they affect. Such description must be included in the legal file described in Section 3.4 and must be included with all distributions of the Source Code. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

5. Application of this License.

This License applies to code to which the Initial Developer has attached the notice in Exhibit A and to related Covered Code.

6. Versions of the License.

6.1. New Versions

Netscape Communications Corporation ("Netscape") may publish revised and/or new versions of the License from time to time. Each version will be given a distinguishing version number.

6.2. Effect of New Versions

Once Covered Code has been published under a particular version of the License, You may always continue to use it under the terms of that version. You may also choose to use such Covered Code under the terms of any subsequent version of the License published by Netscape. No one other than Netscape has the right to modify the terms applicable to Covered Code created under this License.

6.3. Derivative Works

If You create or use a modified version of this License (which you may only do in order to apply it to code which is not already Covered Code governed by this License), You must (a) rename Your license so that the phrases "Mozilla", "MOZILLAPL", "MOZPL", "Netscape", "MPL", "NPL" or any confusingly similar phrase do not appear in your license (except to note that your license differs from this License) and (b) otherwise make it clear that Your version of the license contains terms which differ from the Mozilla Public License and Netscape Public License. (Filling in the name of the Initial Developer, Original Code or Contributor in the notice described in Exhibit A shall not of themselves be deemed to be modifications of this License.)

7. Disclaimer of warranty

Covered code is provided under this license on an "as is" basis, without warranty of any kind, either expressed or implied, including, without limitation, warranties that the covered code is free of defects, merchantable, fit for a particular purpose or non-infringing. The entire risk as to the quality and performance of the covered code is with you. Should any covered code prove defective in any respect, you (not the initial developer or any other contributor) assume the cost of any necessary servicing, repair or correction. This disclaimer of warranty constitutes an essential part of this license. No use of any covered code is authorized hereunder except under this disclaimer.

8. Termination

8.1. This License and the rights granted hereunder will terminate automatically if You fail to comply with terms herein and fail to cure such breach within 30 days of becoming aware of the breach. All sublicenses to the Covered Code which are properly granted shall survive any termination of this License. Provisions which, by their nature, must remain in effect beyond the termination of this License shall survive.

8.2. If You initiate litigation by asserting a patent infringement claim (excluding declatory judgment actions) against Initial Developer or a Contributor (the Initial Developer or Contributor against whom You file such action is referred to as "Participant") alleging that:

such Participant's Contributor Version directly or indirectly infringes any patent, then any and all rights granted by such Participant to You under Sections 2.1 and/ or 2.2 of this License shall, upon 60 days notice from Participant terminate prospectively, unless if within 60 days after receipt of notice You either: (i) agree in writing to pay Participant a mutually agreeable reasonable royalty for Your past and future use of Modifications made by such Participant, or (ii) withdraw Your litigation claim with respect to the Contributor Version against such Participant. If within 60 days of notice, a reasonable royalty and payment arrangement are not mutually agreed upon in writing by the parties or the litigation claim is not withdrawn, the rights granted by Participant to You under Sections 2.1 and/or 2.2 automatically terminate at the expiration of the 60 day notice period specified above.

any software, hardware, or device, other than such Participant's Contributor Version, directly or indirectly infringes any patent, then any rights granted to You by such Participant under Sections 2.1(b) and 2.2(b) are revoked effective as of the date You first made, used, sold, distributed, or had made, Modifications made by that Participant.

8.3. If You assert a patent infringement claim against Participant alleging that such Participant's Contributor Version directly or indirectly infringes any patent

where such claim is resolved (such as by license or settlement) prior to the initiation of patent infringement litigation, then the reasonable value of the licenses granted by such Participant under Sections 2.1 or 2.2 shall be taken into account in determining the amount or value of any payment or license.

8.4. In the event of termination under Sections 8.1 or 8.2 above, all end user license agreements (excluding distributors and resellers) which have been validly granted by You or any distributor hereunder prior to termination shall survive termination.

9. Limitation of liability

Under no circumstances and under no legal theory, whether tort (including negligence), contract, or otherwise, shall you, the initial developer, any other contributor, or any distributor of covered code, or any supplier of any of such parties, be liable to any person for any indirect, special, incidental, or consequential damages of any character including, without limitation, damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses, even if such party shall have been informed of the possibility of such damages. This limitation of liability shall not apply to liability for death or personal injury resulting from such party's negligence to the extent applicable law prohibits such limitation. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so this exclusion and limitation may not apply to you.

10. U.S. government end users

The Covered Code is a "commercial item," as that term is defined in 48 C.F.R. 2.101 (Oct. 1995), consisting of "commercial computer software" and "commercial computer software documentation," as such terms are used in 48 C.F.R. 12.212 (Sept. 1995). Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4 (June 1995), all U.S. Government End Users acquire Covered Code with only those rights set forth herein.

11. Miscellaneous

This License represents the complete agreement concerning subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. This License shall be governed by California law provisions (except to the extent applicable law, if any, provides otherwise), excluding its conflict-of-law provisions. With respect to disputes in which at least one party is a citizen of, or an entity chartered or registered to do business in the United States of America, any litigation relating to this License shall be subject to the jurisdiction of the Federal Courts of the Northern District of California, with venue lying in Santa Clara County, California, with the losing party responsible for costs, including without limitation, court costs and reasonable attorneys' fees and expenses. The

application of the United Nations Convention on Contracts for the International Sale of Goods is expressly excluded. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not apply to this License.

12. Responsibility for claims

As between Initial Developer and the Contributors, each party is responsible for claims and damages arising, directly or indirectly, out of its utilization of rights under this License and You agree to work with Initial Developer and Contributors to distribute such responsibility on an equitable basis. Nothing herein is intended or shall be deemed to constitute any admission of liability.

13. Multiple-licensed code

Initial Developer may designate portions of the Covered Code as "Multiple-Licensed". "Multiple-Licensed" means that the Initial Developer permits you to utilize portions of the Covered Code under Your choice of the MPL or the alternative licenses, if any, specified by the Initial Developer in the file described in Exhibit A.

Exhibit A - Mozilla Public License.

"The contents of this file are subject to the Mozilla Public License Version 1.1 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.mozilla.org/MPL/

Software distributed under the License is distributed on an "AS IS" basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the License for the specific language governing rights and limitations under the License.

The Original Code is _____.

The Initial Developer of the Original Code is _____.

Portions created by _____ are Copyright (C) _____

_____. All Rights Reserved.

Contributor(s): _____.

Alternatively, the contents of this file may be used under the terms of the _____ license (the "[___] License"), in which case the provisions of [_____] License are applicable instead of those above. If you wish to allow use of your version of this file only under the terms of the [____] License and not to allow others to use your version of this file under the MPL, indicate your decision by deleting the provisions above and replace them with the notice and other provisions required

by the [___] License. If you do not delete the provisions above, a recipient may use your version of this file under either the MPL or the [___] License."

NOTE: The text of this Exhibit A may differ slightly from the text of the notices in the Source Code files of the Original Code. You should use the text of this Exhibit A rather than the text found in the Original Code Source Code for Your Modifications.

Note: This Product includes unzip-5.50 and zip-2.3 software under Info-ZIP license

## Info-ZIP license

This is version 2007-Mar-4 of the Info-ZIP license. The definitive version of this document should be available at ftp://ftp.info-zip.org/pub/infozip/license.html indefinitely and a copy at http://www.info-zip.org/pub/infozip/license.html.

Copyright (c) 1990-2007 Info-ZIP. All rights reserved.

For the purposes of this copyright and license, "Info-ZIP" is defined as the following set of individuals:

Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ed Gordon, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Steven M. Schweda, Christian Spieler, Cosmin Truta, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White.

This software is provided "as is," without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the above disclaimer and the following restrictions:

•Redistributions of source code (in whole or in part) must retain the above copyright notice, definition, disclaimer, and this list of conditions.

•Redistributions in binary form (compiled executables and libraries) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.

•Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, versions with modified or added functionality, and dynamic, shared, or static library versions not from Info-ZIP--must be plainly marked as such and must not be misrepresented as being the original source or, if binaries, compiled from the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or the Info-ZIP URL(s), such as to imply Info-ZIP will provide support for the altered versions.

•Info-ZIP retains the right to use the names "Info-ZIP," "Zip," "UnZip," "UnZipSFX," "WiZ," "Pocket UnZip," "Pocket Zip," and "MacZip" for its own source and binary releases.

Note: This Product includes libpcap-0.8.3, libnet-1.1.2.1, net-snmp-5.1.1, libpcap-0.9.4, and openssh-4.3p2 software under BSD license

## BSD

Copyright (c) [dates as appropriate to package]

The Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the University nor of the Laboratory may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR

PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Note: This Product includes libxml2-2.6.8 and Prototype software under the MIT License

## The MIT License

Copyright (c) <year> <copyright holders>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Note: This Product includes openldap-2.1.10 software under the OpenLDAP License

## The Public License

Version 2.8, 17 August 2003

Redistribution and use of this software and associated documentation("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions in source form must retain copyright statements and notices,

tributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution, and

3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time.Each revision is distinguished by a version number. You may use this Software under terms of this license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S) OR OWNER(S) OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission.Title to copyright in this Software shall at all times remain with copyright holders.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Copyright 1999-2003 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved. Permission to copy and distribute verbatim copies of this document is granted.

Note: This Product includes gd-2.0.36RC1 software under the below License

Portions copyright 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002 by Cold Spring Harbor Laboratory. Funded under Grant P41-RR02188 by the National Institutes of Health.

Portions copyright 1996, 1997, 1998, 1999, 2000, 2001, 2002 by Boutell.Com, Inc.

Portions relating to GD2 format copyright 1999, 2000, 2001, 2002 Philip Warner.

Portions relating to PNG copyright 1999, 2000, 2001, 2002 Greg Roelofs.

Portions relating to gdttf.c copyright 1999, 2000, 2001, 2002 John Ellson (ellson@lucent.com).

Portions relating to gdft.c copyright 2001, 2002 John Ellson (ellson@lucent.com).

Portions copyright 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007Pierre-Alain Joye (pierre@libgd.org).

Portions relating to JPEG and to color quantization copyright 2000, 2001, 2002, Doug Becker and copyright (C) 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002, Thomas G. Lane. This software is based in part on the work of the Independent JPEG Group. See the file README-JPEG.TXT for more information.

Portions relating to WBMP copyright 2000, 2001, 2002 Maurice Szmurlo and Johan Van den Brande.

Permission has been granted to copy, distribute and modify gd in any context without fee, including a commercial application, provided that this notice is present in user-accessible supporting documentation.

This does not affect your ownership of the derived work itself, and the intent is to assure proper credit for the authors of gd, not to interfere with your productive use of gd. If you have questions, ask. "Derived works" includes all programs that utilize the library. Credit must be given in user-accessible documentation.

This software is provided "AS IS." The copyright holders disclaim all warranties, either express or implied, including but not limited to implied warranties of merchantability and fitness for a particular purpose, with respect to this code and accompanying documentation.

Although their code does not appear in gd, the authors wish to thank David Koblas, David Rowley, and Hutchison Avenue Software Corporation for their prior contributions.

Note: This Product includes Tablekit software under the below License

Copyright (c) 2007 Andrew Tetlaw & Millstream Web Softwarehttp://www.millstream.com.au/view/code/tablekit/ Version: 1.2.1 2007-03-11
Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:
The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.
THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Note: This Product includes libmd5-rfc software under the below License

Copyright (C) 1999, 2000, 2002 Aladdin Enterprises. All rights reserved.

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.
Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:
1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.
L. Peter Deutschghost@aladdin.com

Note: This Product includes ftp-tls-1.0.0 software under the below License

Copyright (C) 1997 and 1998 WIDE Project. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the project nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
Copyright (c) 1985, 1989, 1993, 1994 The Regents of the University of California. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.
THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE

POSSIBILITY OF SUCH DAMAGE.
Copyright (c) 1997 The NetBSD Foundation, Inc. All rights reserved.
This code is derived from software contributed to The NetBSD Foundation by Luke Mewburn.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
This product includes software developed by the NetBSD Foundation, Inc. and its contributors.
4. Neither the name of The NetBSD Foundation nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.
THIS SOFTWARE IS PROVIDED BY THE NETBSD FOUNDATION, INC. AND CONTRIBUTORS ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE FOUNDATION OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Note: Some components of the ZyWALL USG 100/200 incorporate source code covered under the Apache License, GPL License, LGPL License, BSD License, Open SSL License, Internet Software Consortium and Nominum License, ISC License, OpenLDAP License, X11-style License, A 3 clause BSD License, NTP License, Expat License, PPP License, Netkit-telnet License, MIT License, Info-ZIP license, BSD like License and other licenses presented above. To obtain the source code covered under those Licenses, please contact ZyXEL Communications Corporation at: ZyXEL Technical Support.

## End-User License Agreement for “ZyWALL USG 100/200”

**WARNING:** ZyXEL Communications Corp. IS WILLING TO LICENSE THE ENCLOSED SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY BEFORE COMPLETING THE INSTALLATION PROCESS AS INSTALLING THE SOFTWARE WILL INDICATE YOUR ASSENT TO THEM. IF YOU DO NOT AGREE TO THESE TERMS, THEN ZyXEL, INC. IS UNWILLING TO LICENSE THE SOFTWARE TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE UNINSTALLED SOFTWARE AND PACKAGING TO THE PLACE FROM WHICH IT WAS ACQUIRED, AND YOUR MONEY WILL BE REFUNDED.

1.Grant of License for Personal Use

ZyXEL Communications Corp. ("ZyXEL") grants you a non-exclusive, non-sublicense, non-transferable license to use the program with which this license is distributed (the "Software"), including any documentation files accompanying the

Software ("Documentation"), for internal business use only, for up to the number of users specified in sales order and invoice. You have the right to make one backup copy of the Software and Documentation solely for archival, back-up or disaster recovery purposes. You shall not exceed the scope of the license granted hereunder. Any rights not expressly granted by ZyXEL to you are reserved by ZyXEL, and all implied licenses are disclaimed.

2.Ownership

You have no ownership rights in the Software. Rather, you have a license to use the Software as long as this License Agreement remains in full force and effect. Ownership of the Software, Documentation and all intellectual property rights therein shall remain at all times with ZyXEL. Any other use of the Software by any other entity is strictly forbidden and is a violation of this License Agreement.

3.Copyright

The Software and Documentation contain material that is protected by United States Copyright Law and trade secret law, and by international treaty provisions. All rights not granted to you herein are expressly reserved by ZyXEL. You may not remove any proprietary notice of ZyXEL or any of its licensors from any copy of the Software or Documentation.

4.Restrictions

You may not publish, display, disclose, sell, rent, lease, modify, store, loan, distribute, or create derivative works of the Software, or any part thereof. You may not assign, sublicense, convey or otherwise transfer, pledge as security or otherwise encumber the rights and licenses granted hereunder with respect to the Software. You may not copy, reverse engineer, decompile, reverse compile, translate, adapt, or disassemble the Software, or any part thereof, nor shall you attempt to create the source code from the object code for the Software. You may not market, co-brand, private label or otherwise permit third parties to link to the Software, or any part thereof. You may not use the Software, or any part thereof, in the operation of a service bureau or for the benefit of any other person or entity. You may not cause, assist or permit any third party to do any of the foregoing.

5.Confidentiality

You acknowledge that the Software contains proprietary trade secrets of ZyXEL and you hereby agree to maintain the confidentiality of the Software using at least as great a degree of care as you use to maintain the confidentiality of your own most confidential information. You agree to reasonably communicate the terms and conditions of this License Agreement to those persons employed by you who come into contact with the Software, and to use reasonable best efforts to ensure their compliance with such terms and conditions, including, without limitation, not

knowingly permitting such persons to use any portion of the Software for the purpose of deriving the source code of the Software.

6.No Warranty

THE SOFTWARE IS PROVIDED "AS IS." TO THE MAXIMUM EXTENT PERMITTED BY LAW, ZyXEL DISCLAIMS ALL WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. ZyXEL DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET ANY REQUIREMENTS OR NEEDS YOU MAY HAVE, OR THAT THE SOFTWARE WILL OPERATE ERROR FREE, OR IN AN UNINTERUPTED FASHION, OR THAT ANY DEFECTS OR ERRORS IN THE SOFTWARE WILL BE CORRECTED, OR THAT THE SOFTWARE IS COMPATIBLE WITH ANY PARTICULAR PLATFORM. SOME JURISDICTIONS DO NOT ALLOW THE WAIVER OR EXCLUSION OF IMPLIED WARRANTIES SO THEY MAY NOT APPLY TO YOU. IF THIS EXCLUSION IS HELD TO BE UNENFORCEABLE BY A COURT OF COMPETENT JURISDICTION, THEN ALL EXPRESS AND IMPLIED WARRANTIES SHALL BE LIMITED IN DURATION TO A PERIOD OF THIRTY (30) DAYS FROM THE DATE OF PURCHASE OF THE SOFTWARE, AND NO WARRANTIES SHALL APPLY AFTER THAT PERIOD.

7.Limitation of Liability

IN NO EVENT WILL ZyXEL BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, INDIRECT, SPECIAL, PUNITIVE, OR EXEMPLARY DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THE PROGRAM, OR FOR ANY CLAIM BY ANY OTHER PARTY, EVEN IF ZyXEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. ZyXEL'S AGGREGATE LIABILITY WITH RESPECT TO ITS OBLIGATIONS UNDER THIS AGREEMENT OR OTHERWISE WITH RESPECT TO THE SOFTWARE AND DOCUMENTATION OR OTHERWISE SHALL BE EQUAL TO THE PURCHASE PRICE, BUT SHALL IN NO EVENT EXCEED THE AMOUNT OF THE PRODUCT. BECAUSE SOME STATES/ COUNTRIES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

8.Export Restrictions

THIS LICENSE AGREEMENT IS EXPRESSLY MADE SUBJECT TO ANY APPLICABLE LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS ON THE EXPORT OF THE SOFTWARE OR INFORMATION ABOUT SUCH SOFTWARE WHICH MAY BE IMPOSED FROM TIME TO TIME. YOU SHALL NOT EXPORT THE SOFTWARE, DOCUMENTATION OR INFORMATION ABOUT THE SOFTWARE AND DOCUMENTATION WITHOUT COMPLYING WITH SUCH LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS. YOU AGREE TO INDEMNIFY ZyXEL AGAINST

ALL CLAIMS, LOSSES, DAMAGES, LIABILITIES, COSTS AND EXPENSES, INCLUDING REASONABLE ATTORNEYS' FEES, TO THE EXTENT SUCH CLAIMS ARISE OUT OF ANY BREACH OF THIS SECTION 8.

9.Audit Rights

ZyXEL SHALL HAVE THE RIGHT, AT ITS OWN EXPENSE, UPON REASONABLE PRIOR NOTICE, TO PERIODICALLY INSPECT AND AUDIT YOUR RECORDS TO ENSURE YOUR COMPLIANCE WITH THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT.

10.Termination

This License Agreement is effective until it is terminated. You may terminate this License Agreement at any time by destroying or returning to ZyXEL all copies of the Software and Documentation in your possession or under your control. ZyXEL may terminate this License Agreement for any reason, including, but not limited to, if ZyXEL finds that you have violated any of the terms of this License Agreement. Upon notification of termination, you agree to destroy or return to ZyXEL all copies of the Software and Documentation and to certify in writing that all known copies, including backup copies, have been destroyed. All provisions relating to confidentiality, proprietary rights, and non-disclosure shall survive the termination of this Software License Agreement.

12.General

This License Agreement shall be construed, interpreted and governed by the laws of Republic of China without regard to conflicts of laws provisions thereof. The exclusive forum for any disputes arising out of or relating to this License Agreement shall be an appropriate court or Commercial Arbitration Association sitting in ROC, Taiwan. This License Agreement shall constitute the entire Agreement between the parties hereto. This License Agreement, the rights granted hereunder, the Software and Documentation shall not be assigned by you without the prior written consent of ZyXEL. Any waiver or modification of this License Agreement shall only be effective if it is in writing and signed by both parties hereto. If any part of this License Agreement is found invalid or unenforceable by a court of competent jurisdiction, the remainder of this License Agreement shall be interpreted so as to reasonably effect the intention of the parties.

F

# Wireless LANs

## Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

### Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless adapters (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an ad-hoc wireless LAN.

**Figure 625** Peer-to-Peer Communication in an Ad-hoc Network

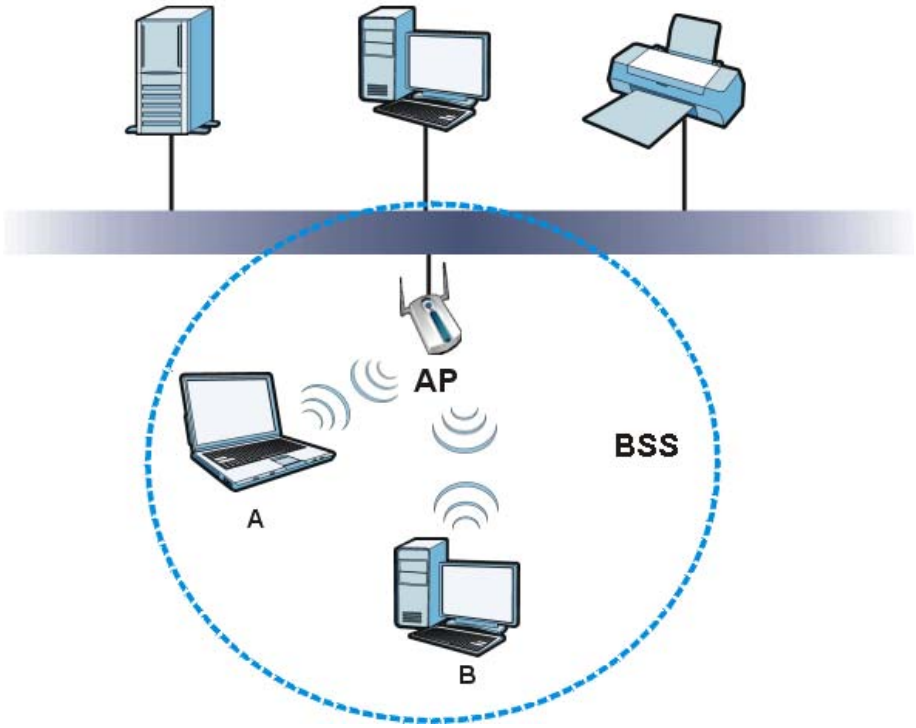
### BSS

A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless client **A** and **B** can access the wired network and communicate

with each other. When Intra-BSS is disabled, wireless client **A** and **B** can still access the wired network but cannot communicate with each other.

**Figure 626** Basic Service Set



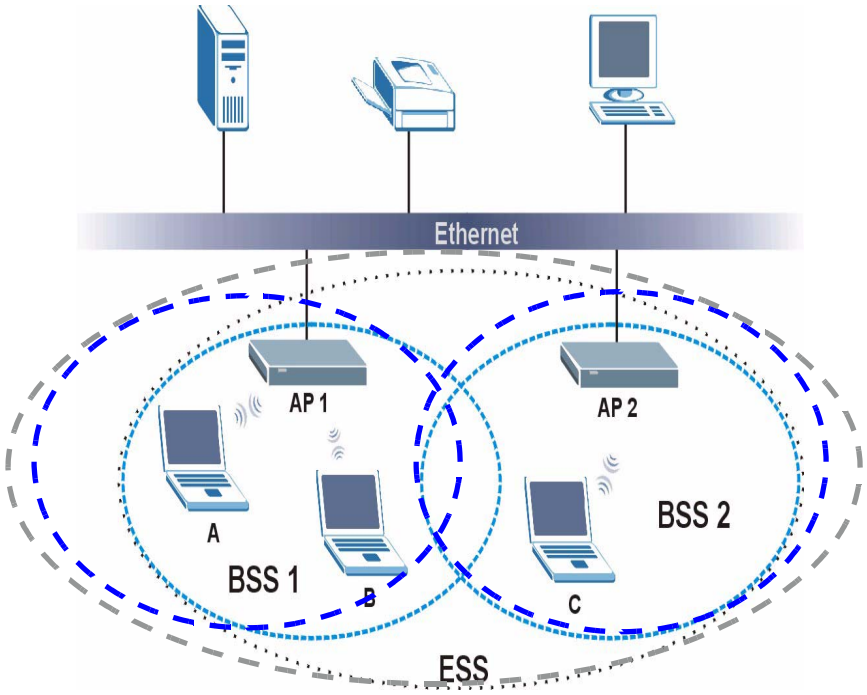

## ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless clients within the same ESS must have the same ESSID in order to communicate.

**Figure 627** Infrastructure WLAN




## Channel

A channel is the radio frequency(ies) used by wireless devices to transmit and receive data. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a channel different from an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

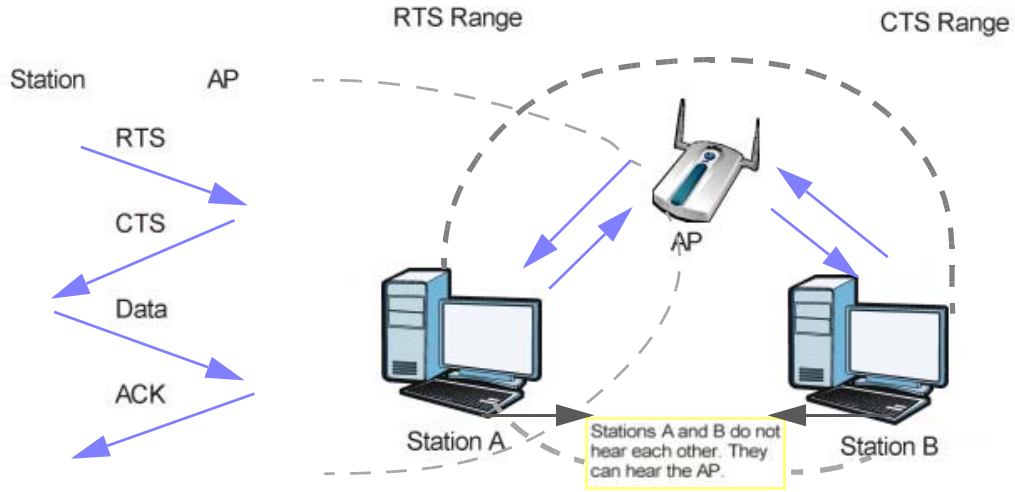
Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

## RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or

wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

**Figure 628** RTS/CTS




When station **A** sends data to the AP, it might not know that the station **B** is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

**RTS/CTS** is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Note: Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

## Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the AP will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

## Preamble Type

Preamble is used to signal that data is coming to the receiver. Short and long refer to the length of the synchronization field in a packet.

Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.11 compliant wireless adapters support long preamble, but not all support short preamble.

Use long preamble if you are unsure what preamble mode other wireless devices on the network support, and to provide more reliable communications in busy wireless networks.

Use short preamble if you are sure all wireless devices on the network support it, and to provide more efficient communications.

Use the dynamic setting to automatically use short preamble when all wireless devices on the network support it, otherwise the ZyWALL uses long preamble.

Note: The wireless devices MUST use the same preamble mode in order to communicate.

## IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point

(and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

**Table 319** IEEE 802.11g

| DATA RATE (MBPS) | MODULATION |
|---|---|
| 1 | DBPSK (Differential Binary Phase Shift Keyed) |
| 2 | DQPSK (Differential Quadrature Phase Shift Keying) |
| 5.5 / 11 | CCK (Complementary Code Keying) |
| 6/9/12/18/24/36/48/54 | OFDM (Orthogonal Frequency Division Multiplexing) |

## Wireless Security Overview

Wireless security is vital to your network to protect wireless communication between wireless clients, access points and the wired network.

Wireless security methods available on the ZyWALL are data encryption, wireless client authentication, restricting access by device MAC address and hiding the ZyWALL identity.

The following figure shows the relative effectiveness of these wireless security methods available on your ZyWALL.

**Table 320** Wireless Security Levels

| SECURITY LEVEL | SECURITY TYPE |
|---|---|
| Least Secure | Unique SSID (Default) |
| | Unique SSID with Hide SSID Enabled |
| | MAC Address Filtering |
| | WEP Encryption |
| | IEEE802.1x EAP with RADIUS Server Authentication |
| | Wi-Fi Protected Access (WPA) |
| Most Secure | WPA2 |

Note: You must enable the same wireless security settings on the ZyWALL and on all wireless clients that you want to associate with it.

## IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional

accounting and control features. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are:

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless clients.

# RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- Authentication

  Determines the identity of the users.
- Authorization

  Determines the network services available to authenticated users once they are connected to the network.
- Accounting

  Keeps track of the client's network activity.

RADIUS is a simple package exchange in which your AP acts as a message relay between the wireless client and the network RADIUS server.

## Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- Access-Request

  Sent by an access point requesting authentication.
- Access-Reject

  Sent by a RADIUS server rejecting access.
- Access-Accept

  Sent by a RADIUS server allowing access.
- Access-Challenge

  Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- Accounting-Request

  Sent by the access point requesting accounting.
- Accounting-Response

  Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

# Types of EAP Authentication

This section discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP. Your wireless LAN device may not support all authentication types.

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server and an intermediary AP(s) that supports IEEE 802.1x. .

For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). A certificate (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

## EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless client. The wireless client 'proves' that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5

authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

### EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless clients for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

### EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

### PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

### LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

## Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the wireless security configuration screen. You may still configure and store keys, but they will not be used while dynamic WEP is enabled.

Note: EAP-MD5 cannot be used with Dynamic WEP Key Exchange

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

**Table 321** Comparison of EAP Authentication Types

| | EAP-MD5 | EAP-TLS | EAP-TTLS | PEAP | LEAP |
|---|---|---|---|---|---|
| Mutual Authentication | No | Yes | Yes | Yes | Yes |
| Certificate – Client | No | Yes | Optional | Optional | No |
| Certificate – Server | No | Yes | Yes | Yes | No |
| Dynamic Key Exchange | No | Yes | Yes | Yes | Yes |
| Credential Integrity | None | Strong | Strong | Strong | Moderate |
| Deployment Difficulty | Easy | Hard | Moderate | Moderate | Moderate |
| Client Identity Protection | No | No | Yes | Yes | No |

# WPA and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA or WPA2 and WEP are improved data encryption and user authentication.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

## Encryption

Both WPA and WPA2 improve data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA and WPA2

use Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP) to offer stronger encryption than TKIP.

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael. They both include a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

WPA and WPA2 regularly change and rotate the encryption keys so that the same encryption key is never used twice.

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), with TKIP and AES it is more difficult to decrypt data on a Wi-Fi network than WEP and difficult for an intruder to break into the network.

The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA(2)-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs a consistent, single, alphanumeric password to derive a PMK which is used to generate unique temporal encryption keys. This prevent all wireless devices sharing the same encryption keys. (a weakness of WEP)

### User Authentication

WPA and WPA2 apply IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. WPA2 reduces the number of key exchange messages from six to four (CCMP 4-way handshake) and shortens the time required to connect to a network. Other WPA2 authentication features that are different from WPA include key caching and pre-

authentication. These two features are optional and may not be supported in all wireless devices.

Key caching allows a wireless client to store the PMK it derived through a successful authentication with an AP. The wireless client uses the PMK when it tries to connect to the same AP and does not need to go with the authentication process again.

Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it.

## Wireless Client WPA Supplicants

A wireless client supplicant is the software that runs on an operating system instructing the wireless client how to use WPA. At the time of writing, the most widely available supplicant is the WPA patch for Windows XP, Funk Software's Odyssey client.

The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

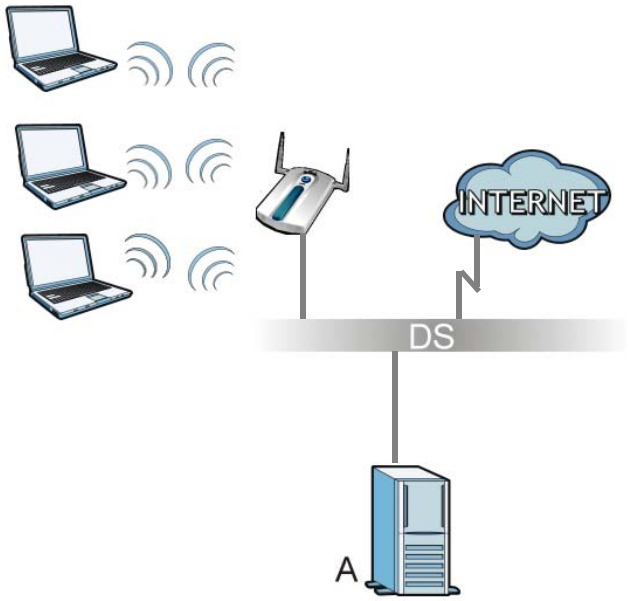
## WPA(2) with RADIUS Application Example

To set up WPA(2), you need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

1. The AP passes the wireless client's authentication request to the RADIUS server.
2. The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
3. A 256-bit Pairwise Master Key (PMK) is derived from the authentication process by the RADIUS server and the client.

4 The RADIUS server distributes the PMK to the AP. The AP then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys. The keys are used to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

**Figure 629** WPA(2) with RADIUS Application Example




## WPA(2)-PSK Application Example

A WPA(2)-PSK application looks as follows.

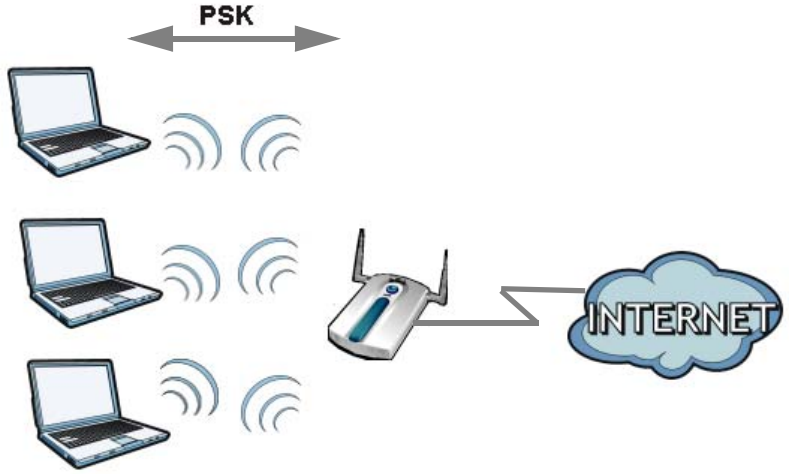
1 First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters or 64 hexadecimal characters (including spaces and symbols).

2 The AP checks each wireless client's password and allows it to join the network only if the password matches.

3 The AP and wireless clients generate a common PMK (Pairwise Master Key). The key itself is not sent over the network, but is derived from the PSK and the SSID.

4 The AP and wireless clients use the TKIP or AES encryption process, the PMK and information exchanged in a handshake to create temporal encryption keys. They use these keys to encrypt data exchanged between them.

**Figure 630** WPA(2)-PSK Authentication




## Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each authentication method or key management protocol type. MAC address filters are not dependent on how you configure these security features.

**Table 322** Wireless Security Relational Matrix

| AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL | ENCRYPTION METHOD | ENTER MANUAL KEY | IEEE 802.1X |
|---|---|---|---|
| Open | None | No | Disable |
| | | | Enable without Dynamic WEP Key |
| Open | WEP | No | Enable with Dynamic WEP Key |
| | | Yes | Enable without Dynamic WEP Key |
| | | Yes | Disable |
| Shared | WEP | No | Enable with Dynamic WEP Key |
| | | Yes | Enable without Dynamic WEP Key |
| | | Yes | Disable |
| WPA | TKIP/AES | No | Enable |
| WPA-PSK | TKIP/AES | Yes | Disable |
| WPA2 | TKIP/AES | No | Enable |
| WPA2-PSK | TKIP/AES | Yes | Disable |

# Antenna Overview

An antenna couples RF signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air.

Positioning the antennas properly increases the range and coverage area of a wireless LAN.

# Antenna Characteristics

## Frequency

An antenna in the frequency of 2.4GHz (IEEE 802.11b and IEEE 802.11g) or 5GHz (IEEE 802.11a) is needed to communicate efficiently in a wireless LAN

## Radiation Pattern

A radiation pattern is a diagram that allows you to visualize the shape of the antenna's coverage area.

## Antenna Gain

Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately 2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately 5%. Actual results may vary depending on the network environment.

Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

# Types of Antennas for WLAN

There are two types of antennas used for wireless LAN applications.

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.
- Directional antennas concentrate the RF signal in a beam, like a flashlight does with the light from its bulb. The angle of the beam determines the width of the coverage pattern. Angles typically range from 20 degrees (very directional) to 120 degrees (less directional). Directional antennas are ideal for hallways and outdoor point-to-point applications.

## Positioning Antennas

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to–point application, position both antennas at the same height and in a direct line of sight to each other to attain the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.

# G

# Legal Information

## Copyright



### Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

### Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

## Certifications (Class B)

### Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.

- This device must accept any interference received, including interference that may cause undesired operations.

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this device does cause harmful interference to radio/television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and the receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help.

### FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

## 注意 !

依據　低功率電波輻射性電機管理辦法

第十二條　經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條　低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

### Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

### Viewing Certifications

1 Go to http://www.zyxel.com.

2 Select your product on the ZyXEL home page to go to that product's page.

3 Select the certification you wish to view from this page.

## ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

### Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

### Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com.

# Index

## Symbols

## Numerics



## A

## B

## C

## D

## E



## F

## G

## H



## I

## J



## K



## L

## M

## N



## O

## P

## Q



## R

## S

## T

## U

## V

## W

## Z