# *ZyWALL 5/35/70 Series*

*Internet Security Appliance*

# *User's Guide*

Version 4.04
03/2008
Edition 1

| DEFAULT LOGIN | |
|---|---|
| **IP Address** | **http://192.168.1.1** |
| **Password** | **1234** |


**www.zyxel.com**

# About This User's Guide

## Intended Audience

This manual is intended for people who want to configure the ZyWALL using the web configurator or System Management Terminal (SMT). You should have at least a basic knowledge of TCP/IP networking concepts and topology.

## Related Documentation

- Quick Start Guide

  The Quick Start Guide is designed to help you get up and running right away. It contains information on setting up your network and configuring for Internet access.
- Web Configurator Online Help

  Embedded web help for descriptions of individual screens and supplementary information.
- CLI Reference Guide

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

  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

# 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.

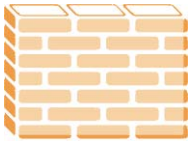
Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

### Syntax Conventions

- The ZyWALL 5/35/70 series may be referred to as the "ZyWALL", the "device" or the "system" 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

For your safety, be sure to read and follow all warning notices and instructions.

- 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 the power adaptor or cord 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 power outlet.
- 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.
- Fuse Warning! Replace a fuse only with a fuse of the same type and rating.

This product is recyclable. Dispose of it properly.

# Contents Overview

# Table of Contents

# List of Figures

# List of Tables

# PART I
# Introduction

# 1

# Getting to Know Your ZyWALL

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

## 1.1 ZyWALL Internet Security Appliance Overview

The ZyWALL is loaded with security features including VPN, firewall, content filtering, anti-spam, IDP (Intrusion Detection and Prevention), anti-virus and certificates. The ZyWALL's De-Militarized Zone (DMZ) increases LAN security by providing separate ports for connecting publicly accessible servers. The ZyWALL is designed for small and medium sized business that need the increased throughput and reliability of dual WAN interfaces and load balancing. The ZyWALL 35 and ZyWALL 5 provide the option to change port roles from LAN to DMZ.

You can also deploy the ZyWALL as a transparent firewall in an existing network with minimal configuration.

The ZyWALL provides bandwidth management, NAT, port forwarding, policy routing, DHCP server and many other powerful features.

You can add an IEEE 802.11b/g-compliant wireless LAN by either inserting a wireless LAN card into the PCMCIA/CardBus slot or connecting an access point (AP) to an Ethernet port in a WLAN port role. If you insert a wireless LAN card to add a WLAN, the ZyWALL offers highly secured wireless connectivity to your wired network with IEEE 802.1x, WEP data encryption, WPA (Wi-Fi Protected Access) and MAC address filtering. You can use the wireless card as part of the LAN, DMZ or WLAN.

## 1.2 ZyWALL Features

The following table lists model specific features.

See Chapter 55 on page 769 for a complete list of features.

**Table 1** ZyWALL Model Specific Features

| FEATURE / MODEL # | 70 | 35 | 5 |
|---|---|---|---|
| Two WAN Ports | Y | Y | |
| 3G Card Supported | | | Y |
| Load Balancing | Y | Y | Y |
| Changing Port Roles between LAN and DMZ | | Y | Y |
| Changing Port Roles between LAN and WLAN | Y | Y | Y |

Table Key: A Y in a model's column shows that the model has the specified feature. The information in this table was correct at the time of writing, although it may be subject to change.

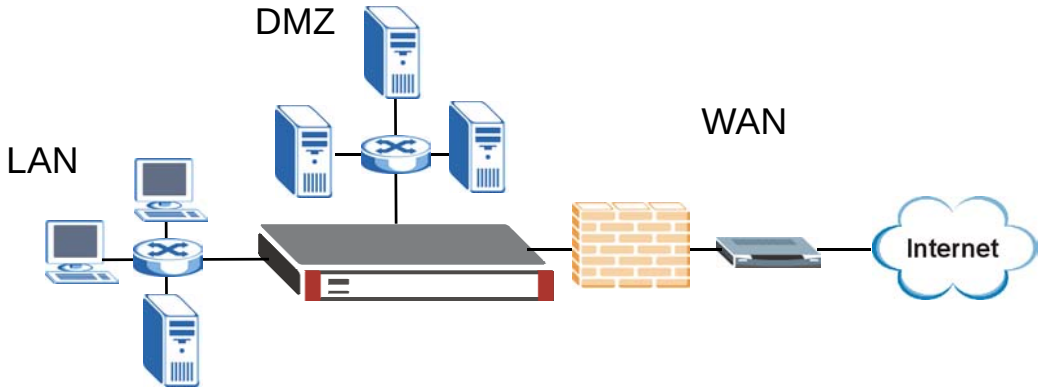
## 1.3 Applications for the ZyWALL

Here are some examples of what you can do with your ZyWALL.

### 1.3.1 Secure Broadband Internet Access via Cable or DSL Modem

You can connect a cable modem, DSL or wireless modem to the ZyWALL for broadband Internet access via an Ethernet or wireless port on the modem. The ZyWALL guarantees not only high speed Internet access, but secure internal network protection and traffic management as well.

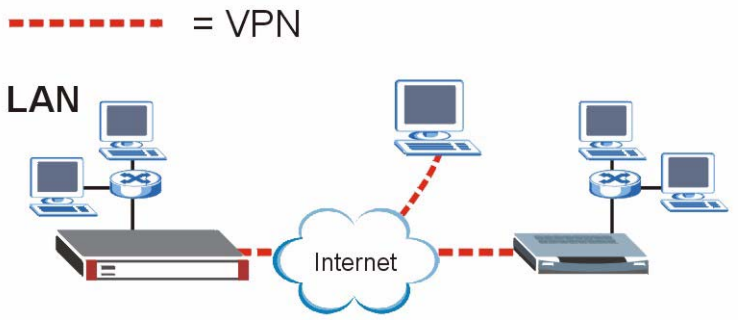
**Figure 1** Secure Internet Access via Cable, DSL or Wireless Modem



### 1.3.2 VPN Application

ZyWALL VPN is an ideal cost-effective way to securely connect branch offices, business partners and telecommuters over the Internet without the need (and expense) for leased lines between sites.

**Figure 2** VPN Application



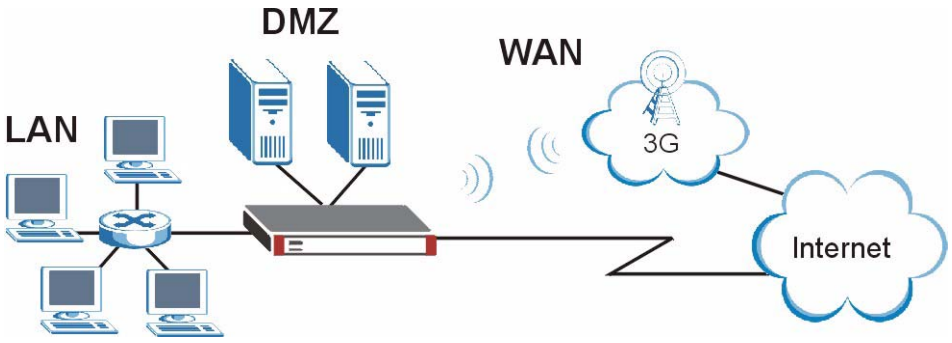

### 1.3.3 3G WAN Application (ZyWALL 5 Only)

Insert a 3G card to have the ZyWALL (in router mode) wirelessly access the Internet via a 3G base station.

At the time of writing, only ZyWALL 5 supports 3G, so all 3G descriptions relate to ZyWALL 5 only. See Section 9.4 on page 192 for more information about 3G.

With both the primary WAN (physical WAN port) and 3G WAN connections enabled, you can use load balancing to improve quality of service and maximize bandwidth utilization or set one of the WAN connections as a backup.

**Figure 3** 3G WAN Application



## 1.4 Ways to Manage the ZyWALL

Use any of the following methods to manage the ZyWALL.

- Web Configurator. This is recommended for everyday management of the ZyWALL using a (supported) web browser.
- Command Line Interface. Line commands are mostly used for troubleshooting by service engineers. See the Command Reference Guide for more information about the CLI.
- SMT. System Management Terminal is a text-based configuration menu that you can use to configure your device.
- FTP for firmware upgrades and configuration backup/restore.
- SNMP. The device can be monitored by an SNMP manager. See the SNMP chapter in this User's Guide.
- Vantage CNM (Centralized Network Management). The device can be remotely managed using a Vantage CNM server.

## 1.5 Good Habits for Managing the ZyWALL

Do the following things regularly to make the ZyWALL more secure and to manage the ZyWALL more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the ZyWALL to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the ZyWALL. You could simply restore your last configuration.

# 2

# Hardware Installation

The ZyWALL can be placed on a desktop or rack-mounted on a standard EIA rack. Use the brackets in a rack-mounted installation.

## 2.1 General Installation Instructions

Read all the safety warnings in the beginning of this User's Guide before you begin and make sure you follow them.

Perform the installation as follows:

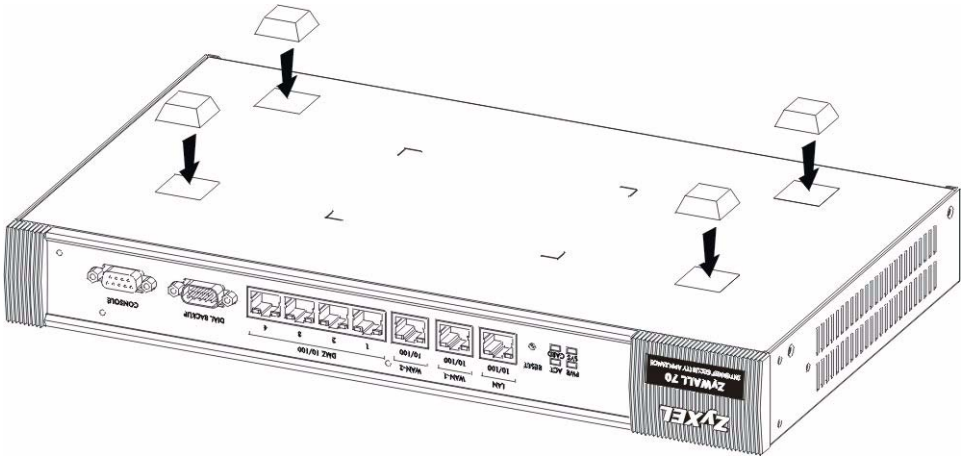
1. Make sure the ZyWALL is off.
2. Install the hardware first.
3. See the Quick Start Guide for instructions on making power and panel connections and turning on the ZyWALL.

For proper ventilation, allow at least 4 inches (10 cm) of clearance at the front and two sides and 3.4 inches (8 cm) at the back of the ZyWALL. This is especially important for enclosed rack installations.

## 2.2 Desktop Installation

1. Make sure the ZyWALL is clean and dry.
2. Set the ZyWALL on a smooth, level surface strong enough to support the weight of the ZyWALL and the connected cables. Make sure there is a power outlet nearby.
3. Make sure there is enough clearance around the ZyWALL to allow air circulation and the attachment of cables and the power cord or power adaptor.
4. Remove the adhesive backing from the rubber feet.
5. Attach the rubber feet to each corner on the bottom of the ZyWALL. These rubber feet help protect the ZyWALL from shock or vibration and ensure space between devices when stacking.

**Figure 4** Attaching Rubber Feet



Do not block the ventilation holes. Leave space between ZyWALLs when stacking.

## 2.3 Rack-mounted Installation Requirements

The ZyWALL can be mounted on an EIA standard size, 19-inch rack or in a wiring closet with other equipment. Follow the steps below to mount your ZyWALL on a standard EIA rack using a rack-mounting kit.

Make sure the rack will safely support the combined weight of all the equipment it contains.
Make sure the position of the ZyWALL does not make the rack unstable or top-heavy. Take all necessary precautions to anchor the rack securely before installing the unit.

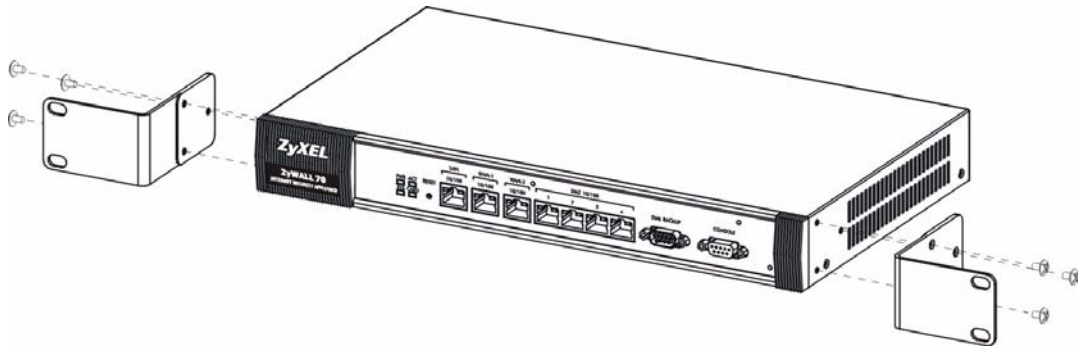
Use a #2 Phillips screwdriver to install the screws.

Failure to use the proper screws may damage the unit.

## 2.4 Rack-Mounted Installation

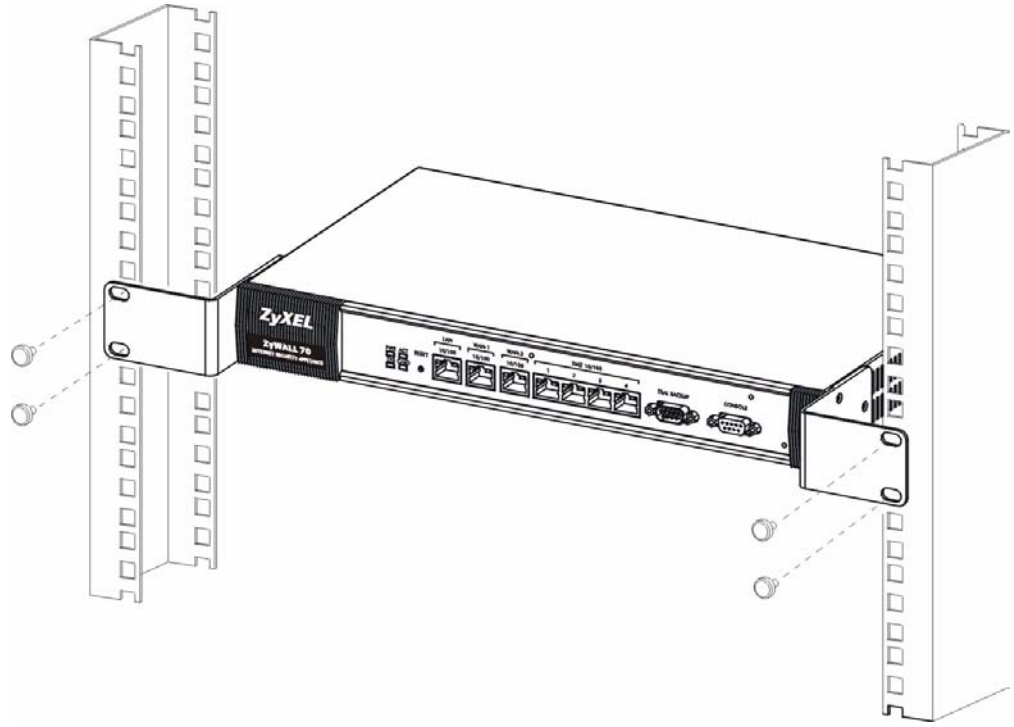
1. Align one bracket with the holes on one side of the ZyWALL and secure it with the bracket screws (smaller than the rack-mounting screws).
2. Attach the other bracket in a similar fashion.

**Figure 5** Attaching Mounting Brackets and Screws




3. After attaching both mounting brackets, position the ZyWALL in the rack by lining up the holes in the brackets with the appropriate holes on the rack. Secure the ZyWALL to the rack with the rack-mounting screws.

**Figure 6** Rack Mounting



## 2.5 3G Card, WLAN Card and ZyWALL Turbo Card Installation

Do not insert or remove a card with the ZyWALL turned on.

Make sure the ZyWALL is off before inserting or removing an 802.11b/g-compliant wireless LAN PCMCIA or CardBus card, 3G card or ZyWALL Turbo Card (to avoid damage). Slide the connector end of the card into the slot as shown next.

Only certain ZyXEL wireless LAN cards or 3G card are compatible with the ZyWALL. Only the ZyWALL 5 can use a 3G card.
Do not force, bend or twist the wireless LAN card, 3G card or ZyWALL Turbo Card.

**Figure 7** WLAN Card Installation

## 2.6 Front Panel Lights

**Figure 8** ZyWALL 70 Front Panel

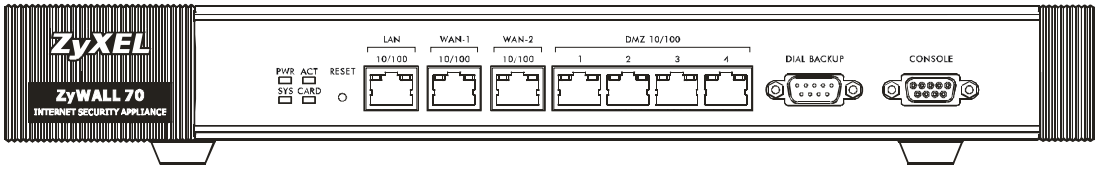



**Figure 9** ZyWALL 35 Front Panel

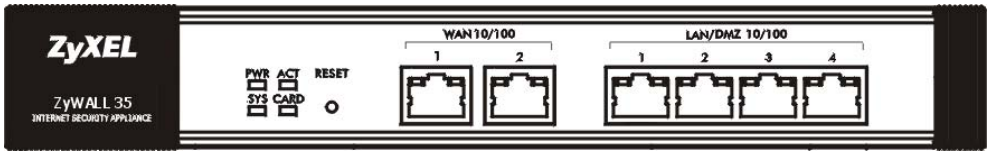
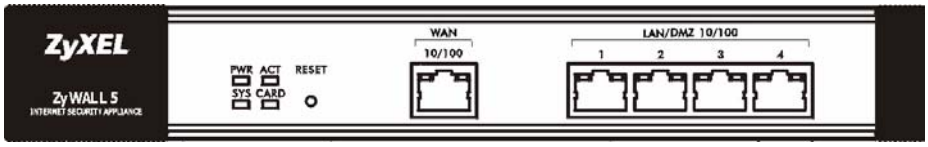



**Figure 10** ZyWALL 5 Front Panel




The following table describes the lights.

**Table 2** Front Panel Lights

| LED | COLOR | STATUS | DESCRIPTION |
|---|---|---|---|
| **PWR** | | Off | The ZyWALL is turned off. |
| | Green | On | The ZyWALL is turned on. |
| | Red | On | The power to the ZyWALL is too low. |
| **SYS** | Green | Off | The ZyWALL is not ready or has failed. |
| | | On | The ZyWALL is ready and running. |
| | | Flashing | The ZyWALL is restarting. |
| **ACT** | Green | Off | The backup port is not connected. |
| | | Flashing | The backup port is sending or receiving packets. |
| **CARD** | Green | Off | The wireless LAN or 3G card is not ready, or has failed. |
| | | On | The wireless LAN or 3G card is ready. |
| | | Flashing | The wireless LAN or 3G card is sending or receiving packets. |
| **LAN 10/100** (ZyWALL 70 only) | | Off | The LAN is not connected. |
| | Green | On | The ZyWALL has a successful 10 Mbps Ethernet connection. |
| | | Flashing | The 10 M LAN is sending or receiving packets. |
| | Orange | On | The ZyWALL has a successful 100 Mbps Ethernet connection. |
| | | Flashing | The 100 M LAN is sending or receiving packets. |

**Table 2** Front Panel Lights (continued)

| LED | COLOR | STATUS | DESCRIPTION |
|---|---|---|---|
| **WAN1/2 10/100** or **WAN 10/100** | | Off | The WAN connection is not ready, or has failed. |
| | Green | On | The ZyWALL has a successful 10 Mbps WAN connection. |
| | | Flashing | The 10M WAN is sending or receiving packets. |
| | Orange | On | The ZyWALL has a successful 100 Mbps WAN connection. |
| | | Flashing | The 100M WAN is sending or receiving packets. |
| **DMZ 10/100** (ZyWALL 70 only) | | Off | The LAN/DMZ is not connected. |
| | Green | On | The ZyWALL has a successful 10 Mbps Ethernet connection. |
| | | Flashing | The 10M DMZ is sending or receiving packets. |
| | Orange | On | The ZyWALL has a successful 100 Mbps Ethernet connection. |
| | | Flashing | The 100M /DMZ is sending or receiving packets. |
| **LAN/DMZ 10/100** (ZyWALL 35 and ZyWALL 5) | | Off | The LAN/DMZ is not connected. |
| | Green | On | The ZyWALL has a successful 10 Mbps Ethernet connection. |
| | | Flashing | The 10 M LAN/DMZ is sending or receiving packets. |
| | Orange | On | The ZyWALL has a successful 100 Mbps Ethernet connection. |
| | | Flashing | The 100 M LAN/DMZ is sending or receiving packets. |

# 3

# Introducing the Web Configurator

This chapter describes how to access the ZyWALL web configurator and provides an overview of its screens.

## 3.1 Web Configurator Overview

The web configurator is an HTML-based management interface that allows easy ZyWALL setup and management via Internet browser. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

See Appendix B on page 785 if you want to make sure these functions are allowed in Internet Explorer or Netscape Navigator.

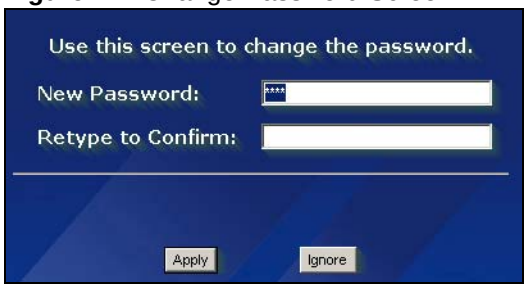
## 3.2 Accessing the ZyWALL Web Configurator

By default, the packets from WLAN to WLAN/ZyWALL are dropped and users cannot configure the ZyWALL wirelessly.

1. Make sure your ZyWALL hardware is properly connected and prepare your computer/ computer network to connect to the ZyWALL (refer to the Quick Start Guide).
2. Launch your web browser.
3. Type "192.168.1.1" as the URL.
4. Type "1234" (default) as the password and click **Login**. In some versions, the default password appears automatically - if this is the case, click **Login**.

5 You should see a screen asking you to change your password (highly recommended) as shown next. Type a new password (and retype it to confirm) and click **Apply** or click **Ignore**.

**Figure 11** Change Password Screen




6 Click **Apply** in the **Replace Certificate** screen to create a certificate using your ZyWALL's MAC address that will be specific to this device.

If you do not replace the default certificate here or in the **CERTIFICATES** screen, this screen displays every time you access the web configurator.

**Figure 12** Replace Certificate Screen


7 You should now see the **HOME** screen (see Figure 15 on page 65).

The management session automatically times out when the time period set in the **Administrator Inactivity Timer** field expires (default five minutes). Simply log back into the ZyWALL if this happens to you.

## 3.3 Resetting the ZyWALL

If you forget your password or cannot access the web configurator, you will need to reload the factory-default configuration file or use the **RESET** button on the back of the ZyWALL. Uploading this configuration file replaces the current configuration file with the factory-default configuration file. This means that you will lose all configurations that you had previously and the speed of the console port will be reset to the default of 9600bps with 8 data bit, no parity, one stop bit and flow control set to none. The password will be reset to 1234, also.

### 3.3.1 Procedure To Use The Reset Button

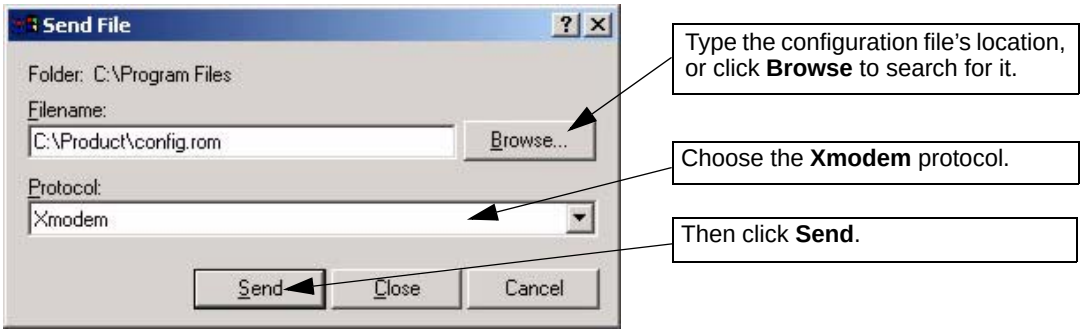
Make sure the **SYS** LED is on (not blinking) before you begin this procedure.

1. Press the **RESET** button for ten seconds, and then release it. If the **SYS** LED begins to blink, the defaults have been restored and the ZyWALL restarts. Otherwise, go to step 2.
2. Turn the ZyWALL off.
3. While pressing the **RESET** button, turn the ZyWALL on.
4. Continue to hold the **RESET** button. The **SYS** LED will begin to blink and flicker very quickly after about 20 seconds. This indicates that the defaults have been restored and the ZyWALL is now restarting.
5. Release the **RESET** button and wait for the ZyWALL to finish restarting.

### 3.3.2 Uploading a Configuration File Via Console Port

1. Download the default configuration file from the ZyXEL FTP site, unzip it and save it in a folder.
2. Turn off the ZyWALL, begin a terminal emulation software session and turn on the ZyWALL again. When you see the message "Press Any key to enter Debug Mode within 3 seconds", press any key to enter debug mode.
3. Enter "y" at the prompt below to go into debug mode.
4. Enter "atlc" after "Enter Debug Mode" message.
5. Wait for "Starting XMODEM upload" message before activating Xmodem upload on your terminal. This is an example Xmodem configuration upload using HyperTerminal.

**Figure 13** Example Xmodem Upload




6. After successful firmware upload, enter "atgo" to restart the router.

# 3.4 Navigating the ZyWALL Web Configurator

The following summarizes how to navigate the web configurator from the **HOME** screen. This guide uses the ZyWALL 70 screenshots as an example. The screens may vary slightly for different ZyWALL models.

**Figure 14** HOME Screen


As illustrated above, the main screen is divided into these parts:

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

## 3.4.1 Title Bar

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

The icons provide the following functions.

**Table 3** Title Bar: Web Configurator Icons

| ICON | DESCRIPTION |
|---|---|
| WIZARD | **Wizards**: Click this icon to open one of the web configurator wizards. See Chapter 4 on page 87 for more information. |
| HELP | **Help**: Click this icon to open the help page for the current screen. |

## 3.4.2 Main Window

The main window shows the screen you select in the navigation panel. It is discussed in more detail in the rest of this document.

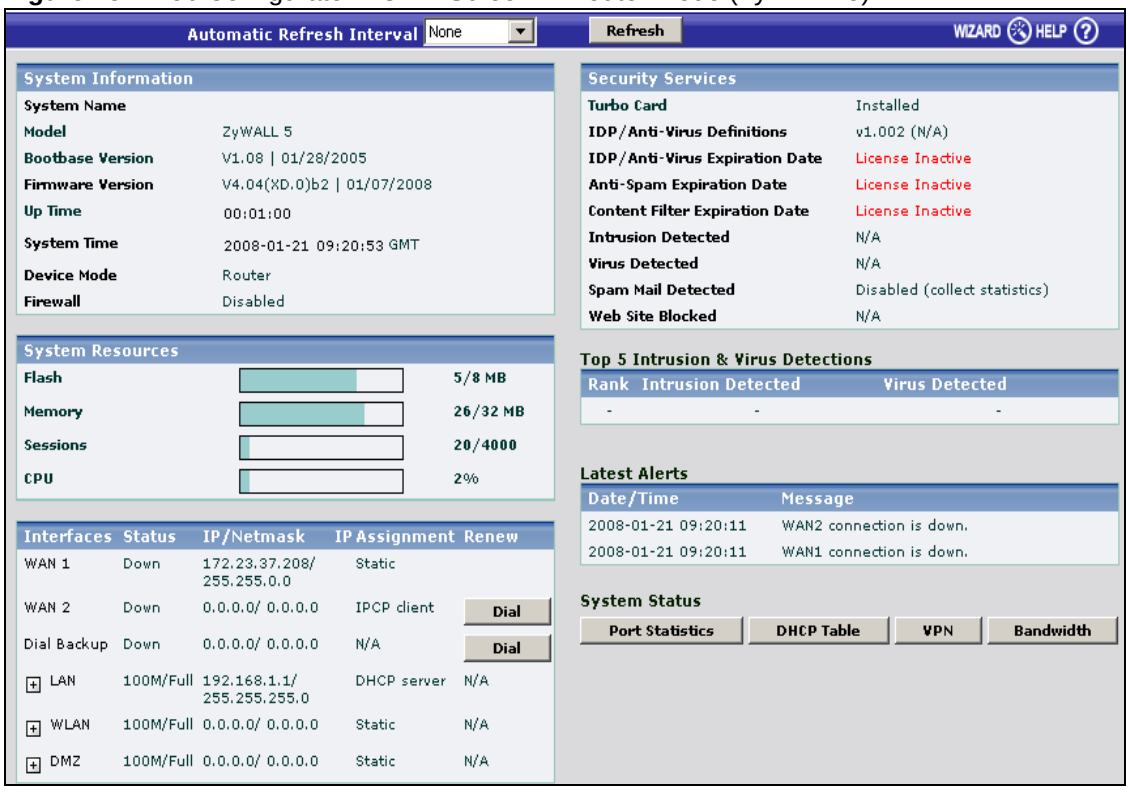
Right after you log in, the **HOME** screen is displayed. The screen varies according to the device mode you select in the **MAINTENANCE > Device Mode** screen.

## 3.4.3 HOME Screen: Router Mode

The following screen displays when the ZyWALL is set to router mode. This screen displays general status information about the ZyWALL. The ZyWALL is set to router mode by default. Not all fields are available on all models.

WAN 2 refers to either the physical WAN 2 port on a ZyWALL with multiple WAN ports or the 3G card on a single WAN ZyWALL in router mode.

**Figure 15** Web Configurator HOME Screen in Router Mode (ZyWALL 5)




The following table describes the labels in this screen.

**Table 4** Web Configurator HOME Screen in Router Mode

| LABEL | DESCRIPTION |
|---|---|
| Automatic Refresh Interval | Select a number of seconds or **None** from the drop-down list box to update all screen statistics automatically at the end of every time interval or to not update the screen statistics. |
| Refresh | Click this button to update the status screen statistics immediately. |
| System Information | |

**Table 4** Web Configurator HOME Screen in Router Mode (continued)

| LABEL | DESCRIPTION |
|---|---|
| System Name | This is the **System Name** you enter in the **MAINTENANCE > General** screen. It is for identification purposes. Click the field label to go to the screen where you can specify a name for this ZyWALL. |
| Model | This is the model name of your ZyWALL. |
| Bootbase Version | This is the bootbase version and the date created. |
| Firmware Version | This is the ZyNOS Firmware version and the date created. ZyNOS is ZyXEL's proprietary Network Operating System design. Click the field label to go to the screen where you can upload a new firmware file. |
| Up Time | This field displays how long the ZyWALL has been running since it last started up. The ZyWALL starts up when you turn it on, when you restart it (**MAINTENANCE > Restart**), or when you reset it (see Section 3.3 on page 63). |
| System Time | This field displays your ZyWALL's present date (in yyyy-mm-dd format) and time (in hh:mm:ss format) along with the difference from the Greenwich Mean Time (GMT) zone. The difference from GMT is based on the time zone. It is also adjusted for Daylight Saving Time if you set the ZyWALL to use it. Click the field label to go to the screen where you can modify the ZyWALL's date and time settings. |
| Device Mode | This displays whether the ZyWALL is functioning as a router or a bridge. Click the field label to go to the screen where you can configure the ZyWALL as a router or a bridge. |
| Firewall | This displays whether or not the ZyWALL's firewall is activated. Click the field label to go to the screen where you can turn the firewall on or off. |
| System Resources | |
| Flash | The first number shows how many megabytes of the flash the ZyWALL is using. |
| Memory | The first number shows how many megabytes of the heap memory the ZyWALL is using. Heap memory refers to the memory that is not used by ZyNOS (ZyXEL Network Operating System) and is thus available for running processes like NAT, VPN and the firewall.<br>The second number shows the ZyWALL's total heap memory (in megabytes).<br>The bar displays what percent of the ZyWALL's heap memory is in use. The bar turns from green to red when the maximum is being approached. |
| Sessions | The first number shows how many sessions are currently open on the ZyWALL. This includes all sessions that are currently traversing the ZyWALL, terminating at the ZyWALL or Initiated from the ZyWALL<br>The second number is the maximum number of sessions that can be open at one time.<br>The bar displays what percent of the maximum number of sessions is in use. The bar turns from green to red when the maximum is being approached. |
| CPU | This field displays what percentage of the ZyWALL's processing ability is currently used. When this percentage is close to 100%, the ZyWALL is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications (for example, using bandwidth management. |
| Interfaces | This is the port type.<br>Click "+" to expand or "-" to collapse the IP alias drop-down lists.<br>Hold your cursor over an interface's label to display the interface's MAC Address.<br>Click an interface's label to go to the screen where you can configure settings for that interface. |

**Table 4** Web Configurator HOME Screen in Router Mode (continued)

| LABEL | DESCRIPTION |
|---|---|
| Status | For the LAN, DMZ and WLAN ports, this displays the port speed and duplex setting. Ethernet port connections can be in half-duplex or full-duplex mode. Full-duplex refers to a device's ability to send and receive simultaneously, while half-duplex indicates that traffic can flow in only one direction at a time. The Ethernet port must use the same speed or duplex mode setting as the peer Ethernet port in order to connect.<br>For the WAN interface(s) and the Dial Backup port, it displays the port speed and duplex setting if you're using Ethernet encapsulation or the remote node name (configured through the SMT) for a PPP connection and **Down** (line is down or not connected), **Idle** (line (ppp) idle), **Dial** (starting to trigger a call) or **Drop** (dropping a call) if you're using PPPoE encapsulation. |
| IP/Netmask | This shows the port's IP address and subnet mask. |
| IP Assignment | For the WAN, if the ZyWALL gets its IP address automatically from an ISP, this displays **DHCP client** when you're using Ethernet encapsulation and **IPCP Client** when you're using PPPoE or PPTP encapsulation. **Static** displays if the WAN port is using a manually entered static (fixed) IP address.<br>For the LAN, WLAN or DMZ, **DHCP server** displays when the ZyWALL is set to automatically give IP address information to the computers connected to the LAN. **DHCP relay** displays when the ZyWALL is set to forward IP address assignment requests to another DHCP server. Static displays if the LAN port is using a manually entered static (fixed) IP address. In this case, you must have another DHCP server on your LAN, or else the computers must be manually configured.<br>For the dial backup port, this shows **N/A** when dial backup is disabled and **IPCP client** when dial backup is enabled. |
| Renew | If you are using Ethernet encapsulation and the WAN port is configured to get the IP address automatically from the ISP, click **Renew** to release the WAN port's dynamically assigned IP address and get the IP address afresh. Click **Dial** to dial up the PPTP, PPPoE or dial backup connection. Click **Drop** to disconnect the PPTP, PPPoE, 3G WAN or dial backup connection. |
| Security Services | |
| Turbo Card | This field displays whether or not a ZyWALL Turbo Card is installed.<br>Note: The ZyWALL must have a Turbo Card installed and a valid service subscription to use the IDP and anti-virus features. |
| IDP/Anti-Virus Definitions | This is the version number of the signatures set that the ZyWALL is using and the date and time that the set was released. Click the field label to go to the screen where you can update the signatures. N/A displays when there is no Turbo Card installed or the service subscription has expired. |
| IDP/Anti-Virus Expiration Date | This is the date the IDP/anti-virus service subscription expires. Click the field label to go to the screen where you can update your service subscription. |
| Anti-Spam Expiration Date | This is the date the anti-spam service subscription expires. Click the field label to go to the screen where you can update your service subscription. |
| Content Filter Expiration Date | This is the date the category-based content filtering service subscription expires. Click the field label to go to the screen where you can update your service subscription. |
| Intrusion Detected | This displays how many intrusions the ZyWALL has detected since it last started up. N/A displays when the ZyWALL has never had an IDP subscription or there is no Turbo Card installed. Disable displays when IDP threat statistics collection is disabled.<br>Click the field label to go to the related screen. |

**Table 4** Web Configurator HOME Screen in Router Mode (continued)

| LABEL | DESCRIPTION |
|---|---|
| Virus Detected | This displays how many virus-infected files the ZyWALL has detected since it last started up. It also displays the percentage of virus-infected files out of the total number of files that the ZyWALL has scanned (since it last started up). N/A displays when the ZyWALL has never had an anti-virus subscription or there is no Turbo Card installed. Disable displays when anti-virus threat statistics collection is disabled.<br>Click the field label to go to the related screen. |
| Spam Mail Detected | This displays how many spam e-mails the ZyWALL has detected since it last started up. It also displays the percentage of spam e-mail out of the total number of e-mails that the ZyWALL has scanned (since it last started up). Disable displays when anti-spam threat statistics collection is disabled.<br>Click the field label to go to the related screen. |
| Web Site Blocked | This displays how many web site hits the ZyWALL has blocked since it last started up. N/A displays when the ZyWALL has never had an external database content filtering service subscription. Disable (collect statistics) displays when the ZyWALL has been subscribed to the external database content filtering service, but content filtering is not active.<br>Click the field label to go to the related screen. |
| Top 5 Intrusion & Virus Detections | 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. |
| 3G WAN Interface Status | These fields display when a 3G card is inserted and the 3G connection is enabled. |
| show detail / hide detail | Click show detail to see more information about the 3G connection. Click hide detail to |
| 3G Connection Status | **WAN2** (the remote node name configured through the SMT) displays when the 3G connection is up.<br>**Ready to Connect** displays when the 3G card is inserted and enabled.<br>**Connecting** displays when the ZyWALL is trying to bring the 3G connection up.<br>**Connected** displays when the 3G connection is up.<br>**Down** displays when the 3G connection is down or not activated.<br>**Idle** displays when the 3G connection is idle.<br>**Init** displays when the ZyWALL is initializing the 3G card.<br>**Drop** displays when the ZyWALL is dropping a call.<br>This field also displays the type of the network to which the ZyWALL is connected. The network type varies depending on the 3G card you inserted and could be **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. |
| Service Provider | This displays the name of your network service provider or **Limited Service** when the signal strength is too low. |
| Signal Strength | 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. You can see a signal strength indication even when the ZyWALL does not have a 3G connection (because the signal is still there even when the ZyWALL is not using it). |

**Table 4** Web Configurator HOME Screen in Router Mode (continued)

| LABEL | DESCRIPTION |
|---|---|
| Last Connection Up Time | This displays how long the 3G connection has been up. |
| Tx Bytes | This displays the total number of data frames transmitted. |
| Rx Bytes | This displays the total number of data frames received. |
| 3G Card Manufacturer | This displays the manufacturer of your 3G card. |
| 3G Card Model | This displays the model name of your 3G card. |
| 3G Card Firmware Revision | This displays the version of the firmware currently used in the 3G card. |
| 3G Card IMEI | This displays the International Mobile Equipment Number (IMEI) which is the serial number of the 3G wireless card. IMEI is a unique 15-digit number used to identify a mobile device. |
| SIM Card IMSI | This displays the International Mobile Subscriber Identity (IMSI) stored in the SIM (Subscriber Identity Module) card. The SIM card is installed in a mobile device and used for authenticating a customer to the carrier network. IMSI is a unique 15-digit number used to identify a user on a network. |
| 3G Card ESN | This field is available only when you insert a CDMA (Code Division Multiple Access) 3G card.<br>This shows the ESN (Electronic Serial Number) of the inserted CDMA 3G card. The ESN is the serial number of a CDMA 3G card and is similar to the IMEI on a GSM or UMTS 3G card. |
| Enter PIN code again | If the PIN code you specified in the **3G (WAN 2)** screen is not the right one for the card you inserted, this field displays allowing you to enter the correct PIN code. Enter the PIN code (four to eight digits) for the inserted 3G card. |
| Apply | Click **Apply** to save the correct PIN code and replace the one you specified in the **3G (WAN 2)** screen. |
| PUK Code | If you enter the PIN code incorrectly three times, the SIM card will be blocked by your ISP and you cannot use the account to access the Internet. You should get the PUK (Personal Unblocking Key) code (four to eight digits) from your ISP. Enter the PUK code to enable the SIM card. If an incorrect PUK code is entered 10 times, the SIM card will be disabled permanently. You then need to contact your ISP for a new SIM card. |
| New PIN Code | Configure a PIN code for the SIM card. You can specify any four to eight digits to have a new PIN code or enter the previous PIN code. |
| Confirm New PIN Code | Enter the PIN code again for confirmation. |
| Apply | Click **Apply** to save your changes in this section. |
| Reset budget counters, resume budget control | This field displays if you have enabled budget control but insert a 3G card with a different user account from the one for which you configured budget control.<br>Select this option to have the ZyWALL do budget calculation starting from 0 but use the previous settings. |
| Resume budget control | This field displays if you have enabled budget control but insert a 3G card with a different user account from the one for which you configured budget control.<br>Select this option to have the ZyWALL keep the existing statistics and continue counting. |

**Table 4** Web Configurator HOME Screen in Router Mode (continued)

| LABEL | DESCRIPTION |
|---|---|
| Disable budget control | This field displays if you have enabled budget control but insert a 3G card with a different user account from the one for which you configured budget control.<br>Select this option to disable budget control.<br>If you want to enable and configure new budget control settings for the new user account, go to the **3G (WAN 2)** screen.<br>The ZyWALL keeps the existing statistics if you do not change the budget control settings. You could reinsert the original card and enable budget control to have the ZyWALL continue counting the budget control statistics. |
| Apply | Click **Apply** to save your changes in this section. |
| Enter modem unlock code | This field only displays when you insert a 3G card and the internal modem on the 3G card is blocked.<br>Enter a key to enable the internal modem on your 3G card. By default, the key is the last four digits of your phone number used to dial up the 3G connection. Otherwise, you need to get the key from your service provider. |
| Apply | Click **Apply** to save your changes in this section. |
| Remaining Time Budget | This displays when you enable budget control in the **3G (WAN 2)** screen.<br>This shows the amount of time the 3G connection can still be used before the ZyWALL takes the actions you specified in the **3G (WAN 2)** screen. |
| Remaining Data Budget | This displays when you enable budget control in the **3G (WAN 2)** screen.<br>This shows how much data (in bytes) can still be transmitted through the 3G connection before the ZyWALL takes the actions you specified in the **3G (WAN 2)** screen.<br>Note: The budget counters will not be reset when you restore the factory defaults. The budget counters are saved to the flash every hour or when the 3G connection is dropped. If you restart the ZyWALL within one hour, any change in the counters will not be saved. |
| Reset time and data budget counters | This displays when you enable budget control in the **Network > WAN > 3G (WAN 2)** screen.<br>Click this button to reset the time and data budgets immediately. The count starts over with the 3G connection's full configured monthly time and data budgets. This does not affect the normal monthly budget restart. |
| Latest Alerts | This table displays the five most recent alerts recorded by the ZyWALL. You can see more information in the **View Log** screen, such as the source and destination IP addresses and port numbers of the incoming packets. |
| Date/Time | This is the date and time the alert was recorded. |
| Message | This is the reason for the alert. |
| System Status | |
| Port Statistics | Click **Port Statistics** to see router performance statistics such as the number of packets sent and number of packets received for each port. |
| DHCP Table | Click **DHCP Table** to show current DHCP client information. |
| VPN | Click **VPN** to display the active VPN connections. |
| Bandwidth | Click **Bandwidth** to view the ZyWALL's bandwidth usage and allotments. |

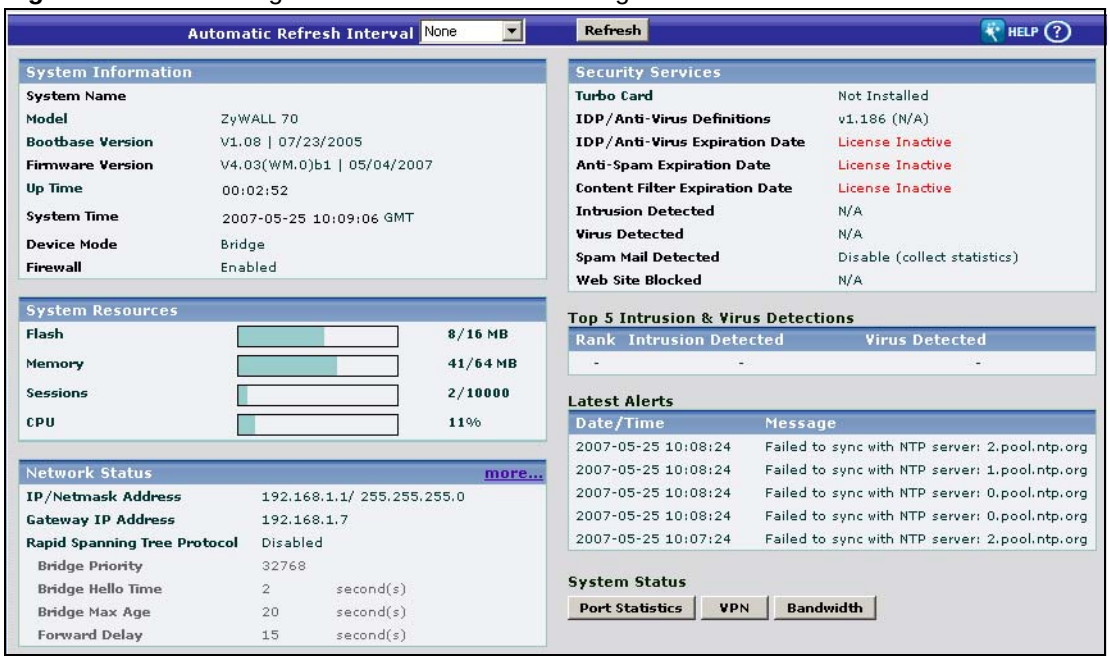
## 3.4.4 HOME Screen: Bridge Mode

The following screen displays when the ZyWALL is set to bridge mode. In bridge mode, the ZyWALL functions as a transparent firewall (also known as a bridge firewall). The ZyWALL bridges traffic traveling between the ZyWALL's interfaces and still filters and inspects packets. You do not need to change the configuration of your existing network.

In bridge mode, the ZyWALL cannot get an IP address from a DHCP server. The LAN, WAN, DMZ and WLAN interfaces all have the same (static) IP address and subnet mask. You can configure the ZyWALL's IP address in order to access the ZyWALL for management. If you connect your computer directly to the ZyWALL, you also need to assign your computer a static IP address in the same subnet as the ZyWALL's IP address in order to access the ZyWALL.

You can use the firewall and VPN in bridge mode. See the user's guide for a list of other features that are available in bridge mode.

**Figure 16** Web Configurator HOME Screen in Bridge Mode




The following table describes the labels in this screen.

**Table 5** Web Configurator HOME Screen in Bridge Mode

| LABEL | DESCRIPTION |
|---|---|
| Automatic Refresh Interval | Select a number of seconds or **None** from the drop-down list box to update all screen statistics automatically at the end of every time interval or to not update the screen statistics. |
| Refresh | Click this button to update the screen's statistics immediately. |
| System Information | |
| System Name | This is the **System Name** you enter in the **MAINTENANCE > General** screen. It is for identification purposes. Click the field label to go to the screen where you can specify a name for this ZyWALL. |
| Model | This is the model name of your ZyWALL. |

**Table 5** Web Configurator HOME Screen in Bridge Mode (continued)

| LABEL | DESCRIPTION |
|---|---|
| Bootbase Version | This is the bootbase version and the date created. |
| Firmware Version | This is the ZyNOS Firmware version and the date created. ZyNOS is ZyXEL's proprietary Network Operating System design. Click the field label to go to the screen where you can upload a new firmware file. |
| Up Time | This field displays how long the ZyWALL has been running since it last started up. The ZyWALL starts up when you turn it on, when you restart it (**MAINTENANCE > Restart**), or when you reset it (see Section 3.3 on page 63). |
| System Time | This field displays your ZyWALL's present date (in yyyy-mm-dd format) and time (in hh:mm:ss format) along with the difference from the Greenwich Mean Time (GMT) zone. The difference from GMT is based on the time zone. It is also adjusted for Daylight Saving Time if you set the ZyWALL to use it. Click the field label to go to the screen where you can modify the ZyWALL's date and time settings. |
| Device Mode | This displays whether the ZyWALL is functioning as a router or a bridge. Click the field label to go to the screen where you can configure the ZyWALL as a router or a bridge. |
| Firewall | This displays whether or not the ZyWALL's firewall is activated. Click the field label to go to the screen where you can turn the firewall on or off. |
| System Resources | |
| Flash | The first number shows how many megabytes of the flash the ZyWALL is using. |
| Memory | The first number shows how many megabytes of the heap memory the ZyWALL is using. Heap memory refers to the memory that is not used by ZyNOS (ZyXEL Network Operating System) and is thus available for running processes like NAT, VPN and the firewall.<br>The second number shows the ZyWALL's total heap memory (in megabytes).<br>The bar displays what percent of the ZyWALL's heap memory is in use. The bar turns from green to red when the maximum is being approached. |
| Sessions | The first number shows how many sessions are currently open on the ZyWALL. This includes all sessions that are currently traversing the ZyWALL, terminating at the ZyWALL or initiated from the ZyWALL<br>The second number is the maximum number of sessions that can be open at one time.<br>The bar displays what percent of the maximum number of sessions is in use. The bar turns from green to red when the maximum is being approached. |
| CPU | This field displays what percentage of the ZyWALL's processing ability is currently used. When this percentage is close to 100%, the ZyWALL is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications (for example, using bandwidth management. |
| Network Status | Click **more** to display information about the individual interfaces. |
| IP/Netmask Address | This is the IP address and subnet mask of your ZyWALL in dotted decimal notation. |
| Gateway IP Address | This is the gateway IP address. |
| Rapid Spanning Tree Protocol | This shows whether RSTP (Rapid Spanning Tree Protocol) is active or not. The following labels or values relative to RSTP do not apply when RSTP is disabled. |
| Bridge Priority | This is the bridge priority of the ZyWALL. The bridge (or switch) with the lowest bridge priority value in the network is the root bridge (the base of the spanning tree). |

**Table 5** Web Configurator HOME Screen in Bridge Mode (continued)

| LABEL | DESCRIPTION |
|---|---|
| Bridge Hello Time | This is the interval of BPDUs (Bridge Protocol Data Units) from the root bridge. |
| Bridge Max Age | This is the predefined interval that a bridge waits to get a Hello message (BPDU) from the root bridge. |
| Forward Delay | This is the forward delay interval. |
| Bridge Port | This is the port type. Port types are: **WAN** (or **WAN1**, **WAN2**), **LAN**, **Wireless Card**, **DMZ** and **WLAN Interface**. |
| Port Status | For the WAN, LAN, DMZ, and WLAN Interfaces, this displays the port speed and duplex setting. For the WAN port, it displays **Down** when the link is not ready or has failed. For the wireless card, it displays the transmission rate when a wireless LAN card is inserted and WLAN is enabled or **Down** when a wireless LAN is not inserted or WLAN is disabled. |
| RSTP Status | This is the RSTP status of the corresponding port. |
| RSTP Active | This shows whether or not RSTP is active on the corresponding port. |
| RSTP Priority | This is the RSTP priority of the corresponding port. |
| RSTP Path Cost | This is the cost of transmitting a frame from the root bridge to the corresponding port. |
| Security Services | |
| Turbo Card | This field displays whether or not a ZyWALL Turbo Card is installed.<br>Note: The ZyWALL must have a Turbo Card installed and a valid service subscription to use the IDP and anti-virus features. |
| IDP/Anti-Virus Definitions | This is the version number of the signatures set that the ZyWALL is using and the date and time that the set was released. Click the field label to go to the screen where you can update the signatures. N/A displays when there is no Turbo Card installed or the service subscription has expired. |
| IDP/Anti-Virus Expiration Date | This is the date the IDP/anti-virus service subscription expires. Click the field label to go to the screen where you can update your service subscription. |
| Anti-Spam Expiration Date | This is the date the anti-spam service subscription expires. Click the field label to go to the screen where you can update your service subscription. |
| Content Filter Expiration Date | This is the date the category-based content filtering service subscription expires. Click the field label to go to the screen where you can update your service subscription. |
| Intrusion Detected | This displays how many intrusions the ZyWALL has detected since it last started up.<br>**N/A** displays when there is no valid license or there is no Turbo Card installed.<br>**Disable** displays when the IDP threat statistics collection is disabled.<br>Click the field label to go to the screen where you can turn the statistics collection on or off. |
| Virus Detected | This displays how many virus-infected files the ZyWALL has detected since it last started up. It also displays the percentage of virus-infected files out of the total number of files that the ZyWALL has scanned (since it last started up).<br>**N/A** displays when there is no valid license or there is no Turbo Card installed.<br>**Disable** displays when the anti-virus threat statistics collection is disabled.<br>Click the field label to go to the screen where you can turn the statistics collection on or off. |

**Table 5** Web Configurator HOME Screen in Bridge Mode (continued)

| LABEL | DESCRIPTION |
|---|---|
| Spam Mail Detected | This displays how many spam e-mails the ZyWALL has detected since it last started up. It also displays the percentage of spam e-mail out of the total number of e-mails that the ZyWALL has scanned (since it last started up).<br>**Disable** displays when the anti-spam threat statistics collection is disabled.<br>Click the field label to go to the screen where you can turn the statistics collection on or off. |
| Web Site Blocked | This displays how many web site hits the ZyWALL has blocked since it last started up.<br>**N/A** displays when there is no valid license.<br>**Disable (collect statistics)** displays when the content filtering feature is disabled.<br>Click the field label to go to the screen where you can turn content filtering on or off. |
| Top 5 Intrusion & Virus Detections | 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. |
| Latest Alerts | This table displays the five most recent alerts recorded by the ZyWALL. You can see more information in the **View Log** screen, such as the source and destination IP addresses and port numbers of the incoming packets. |
| Date/Time | This is the date and time the alert was recorded. |
| Message | This is the reason for the alert. |
| System Status | |
| Port Statistics | Click **Port Statistics** to see router performance statistics such as the number of packets sent and number of packets received for each port. |
| VPN | Click **VPN** to display the active VPN connections. |
| Bandwidth | Click **Bandwidth** to view the ZyWALL's bandwidth usage and allotments. |

## 3.4.5 Navigation Panel

After you enter the password, use the sub-menus on the navigation panel to configure ZyWALL features.

The following table lists the features available for each device mode. Not all ZyWALLs have all features listed in this table.

**Table 6** Bridge and Router Mode Features Comparison

| FEATURE | BRIDGE MODE | ROUTER MODE |
|---|---|---|
| Internet Access Wizard | | Y |
| VPN Wizard | Y | Y |
| DHCP Table | | Y |
| System Statistics | Y | Y |
| Registration | Y | Y |
| LAN | | Y |

**Table 6** Bridge and Router Mode Features Comparison

| FEATURE | BRIDGE MODE | ROUTER MODE |
|---|---|---|
| WAN | | Y |
| DMZ | | Y |
| Bridge | Y | |
| WLAN | | Y |
| Wireless Card | Y | Y |
| Firewall | Y | Y |
| IDP | Y | Y |
| Anti-Virus | Y | Y |
| Anti-Spam | Y | Y |
| Content Filter | Y | Y |
| VPN | Y | Y |
| Certificates | Y | Y |
| Authentication Server | Y | Y |
| NAT | | Y |
| Static Route | | Y |
| Policy Route | | Y |
| Bandwidth Management | Y | Y |
| DNS | | Y |
| Remote Management | Y | Y |
| UPnP | | Y |
| Custom Application | Y | Y |
| ALG | Y | Y |
| Reports | Y | Y |
| Logs | Y | Y |
| Maintenance | Y | Y |

Table Key: A Y in a mode's column shows that the device mode has the specified feature. The information in this table was correct at the time of writing, although it may be subject to change.

The following table describes the sub-menus.

**Table 7** Screens Summary

| LINK | TAB | FUNCTION |
|---|---|---|
| HOME | | This screen shows the ZyWALL's general device and network status information. Use this screen to access the wizards, statistics and DHCP table. |
| REGISTRATION | Registration | Use this screen to register your ZyWALL and activate the trial service subscriptions. |
| | Service | Use this to manage and update the service status and license information. |
| NETWORK | | |

**Table 7** Screens Summary (continued)

| LINK | TAB | FUNCTION |
|---|---|---|
| LAN | LAN | Use this screen to configure LAN DHCP and TCP/IP settings. |
| | Static DHCP | Use this screen to assign fixed IP addresses on the LAN. |
| | IP Alias | Use this screen to partition your LAN interface into subnets. |
| | Port Roles (ZyWALL 5 and ZyWALL 35) | Use this screen to change the LAN/DMZ/WLAN port roles. |
| BRIDGE | Bridge | Use this screen to change the bridge settings on the ZyWALL. |
| | Port Roles | Use this screen to change the DMZ/WLAN port roles on the ZyWALL 70 or the LAN/DMZ/WLAN port roles on the ZyWALL 5 or ZyWALL 35. |
| WAN | General | This screen allows you to configure load balancing, route priority and traffic redirect properties. |
| | WAN1 | Use this screen to configure the WAN1 connection for Internet access. |
| | WAN2 | Use this screen to configure the WAN2 connection for Internet access. |
| | 3G (WAN2) | Use this screen to configure the 3G WAN2 connection for Internet access (ZyWALL 5 only). |
| | Traffic Redirect | Use this screen to configure your traffic redirect properties and parameters. |
| | Dial Backup | Use this screen to configure the backup WAN dial-up connection. |
| DMZ | DMZ | Use this screen to configure your DMZ connection. |
| | Static DHCP | Use this screen to assign fixed IP addresses on the DMZ. |
| | IP Alias | Use this screen to partition your DMZ interface into subnets. |
| | Port Roles | Use this screen to change the DMZ/WLAN port roles on the ZyWALL 70 or the LAN/DMZ/WLAN port roles on the ZyWALL 5 or ZyWALL 35. |
| WLAN | WLAN | Use this screen to configure your WLAN connection. |
| | Static DHCP | Use this screen to assign fixed IP addresses on the WLAN. |
| | IP Alias | Use this screen to partition your WLAN interface into subnets. |
| | Port Roles | Use this screen to change the DMZ/WLAN port roles on the ZyWALL 70 or the LAN/DMZ/WLAN port roles on the ZyWALL 5 or ZyWALL 35. |
| WIRELESS | | |
| 3G (WAN2) | | This is the same as WAN > 3G (WAN2). |
| Wi-Fi | Wireless Card | Use this screen to configure the wireless LAN settings and WLAN authentication/security settings. |
| | MAC Filter | Use this screen to change MAC filter settings on the ZyWALL |
| SECURITY | | |

**Table 7** Screens Summary (continued)

| LINK | TAB | FUNCTION |
|---|---|---|
| FIREWALL | Default Rule | Use this screen to activate/deactivate the firewall and the direction of network traffic to which to apply the rule |
| | Rule Summary | This screen shows a summary of the firewall rules, and allows you to edit/add a firewall rule. |
| | Anti-Probing | Use this screen to change your anti-probing settings. |
| | Threshold | Use this screen to configure the threshold for DoS attacks. |
| | Service | Use this screen to configure custom services. |
| IDP | General | Use this screen to enable IDP on the ZyWALL and choose what interface(s) you want to protect from intrusions. |
| | Signature | Use these screens to view signatures by attack type or search for signatures by signature name, ID, severity, target operating system, action etc. You can also configure signature actions here. |
| | Anomaly | Use this screen to configure anomaly detection settings. |
| | Update | Use this screen to download new signature downloads. It is important to do this as new intrusions evolve. |
| | Backup & Restore | Use this screen to back up, restore or revert to the default signatures' actions. |
| ANTI-VIRUS | General | Use this screen to activate AV scanning on the interface(s) and specify actions when a virus is detected. |
| | Signature | Use these screens to search for signatures by signature name or attributes and configure how the ZyWALL uses them. |
| | Update | Use this screen to view the version number of the current signatures and configure the signature update schedule. |
| | Backup & Restore | Use this screen to back up, restore or revert to the default signatures' actions. |
| ANTI-SPAM | General | Use this screen to turn the anti-spam feature on or off and set how the ZyWALL treats spam. |
| | External DB | Use this screen to enable or disable the use of the anti-spam external database. |
| | Lists | Use this screen to configure the whitelist to identify legitimate e-mail and configure the blacklist to identify spam e-mail. |
| CONTENT FILTER | General | This screen allows you to enable content filtering and block certain web features. |
| | Policy | Use these screens to configure content filtering policies for particular source IP addresses or ranges of IP addresses. Select web features and categories of web pages to block. You can also configure schedules for applying the content filtering. |
| | Object | Use this screen to configure a master list of trusted web sites, forbidden web sites, and keywords. Then you can use the objects in individual policies. |
| | Cache | Use this screen to view and configure the ZyWALL's URL caching. |
| VPN | VPN Rules (IKE) | Use this screen to configure VPN connections using IKE key management and view the rule summary. |
| | VPN Rules (Manual) | Use this screen to configure VPN connections using manual key management and view the rule summary. |
| | SA Monitor | Use this screen to display and manage active VPN connections. |
| | Global Setting | Use this screen to configure the IPSec timer settings. |

**Table 7** Screens Summary (continued)

| LINK | TAB | FUNCTION |
|---|---|---|
| CERTIFICATES | My Certificates | Use this screen to view a summary list of certificates and manage certificates and certification requests. |
| | Trusted CAs | Use this screen to view and manage the list of the trusted CAs. |
| | Trusted Remote Hosts | Use this screen to view and manage the certificates belonging to the trusted remote hosts. |
| | Directory Servers | Use this screen to view and manage the list of the directory servers. |
| AUTH SERVER | Local User Database | Use this screen to configure the local user account(s) on the ZyWALL. |
| | RADIUS | Configure this screen to use an external server to authenticate wireless and/or VPN users. |
| ADVANCED | | |
| NAT | NAT Overview | Use this screen to enable NAT. |
| | Address Mapping | Use this screen to configure network address translation mapping rules. |
| | Port Forwarding | Use this screen to configure servers behind the ZyWALL. |
| | Port Triggering | Use this screen to change your ZyWALL's port triggering settings. |
| STATIC ROUTE | IP Static Route | Use this screen to configure IP static routes. |
| POLICY ROUTE | Policy Route Summary | Use this screen to view a summary list of all the policies and configure policies for use in IP policy routing. |
| BW MGMT | Summary | Use this screen to enable bandwidth management on an interface. |
| | Class Setup | Use this screen to set up the bandwidth classes. |
| | Monitor | Use this screen to view the ZyWALL's bandwidth usage and allotments. |
| DNS | System | Use this screen to configure the address and name server records. |
| | Cache | Use this screen to configure the DNS resolution cache. |
| | DHCP | Use this screen to configure LAN/DMZ/WLAN DNS information. |
| | DDNS | Use this screen to set up dynamic DNS. |

**Table 7** Screens Summary (continued)

| LINK | TAB | FUNCTION |
|---|---|---|
| REMOTE MGMT | WWW | Use this screen to configure through which interface(s) and from which IP address(es) users can use HTTPS or HTTP to manage the ZyWALL. |
| | SSH | Use this screen to configure through which interface(s) and from which IP address(es) users can use Secure Shell to manage the ZyWALL. |
| | TELNET | Use this screen to configure through which interface(s) and from which IP address(es) users can use Telnet to manage the ZyWALL. |
| | FTP | Use this screen to configure through which interface(s) and from which IP address(es) users can use FTP to access the ZyWALL. |
| | SNMP | Use this screen to configure your ZyWALL's settings for Simple Network Management Protocol management. |
| | DNS | Use this screen to configure through which interface(s) and from which IP address(es) users can send DNS queries to the ZyWALL. |
| | CNM | Use this screen to configure and allow your ZyWALL to be managed by the Vantage CNM server. |
| UPnP | UPnP | Use this screen to enable UPnP on the ZyWALL. |
| | Ports | Use this screen to view the NAT port mapping rules that UPnP creates on the ZyWALL. |
| Custom APP | Custom APP | Use this screen to specify port numbers for the ZyWALL to monitor for FTP, HTTP, SMTP, POP3, H323, and SIP traffic. |
| ALG | ALG | Use this screen to allow certain applications to pass through the ZyWALL. |
| REPORTS | | |
| | Reports | Use this screen to have the ZyWALL record and display network usage reports. |
| | IDP | Use this screen to collect and display statistics on the intrusions that the ZyWALL has detected. |
| | Anti-Virus | Use this screen to collect and display statistics on the viruses that the ZyWALL has detected. |
| | Anti-Spam | Use this screen to collect and display statistics on spam mail that the ZyWALL has detected. |
| | E-mail Report | Use this screen to have reports emailed in a single file. |
| LOGS | View Log | Use this screen to view the logs for the categories that you selected. |
| | Log Settings | Use this screen to change your ZyWALL's log settings. |

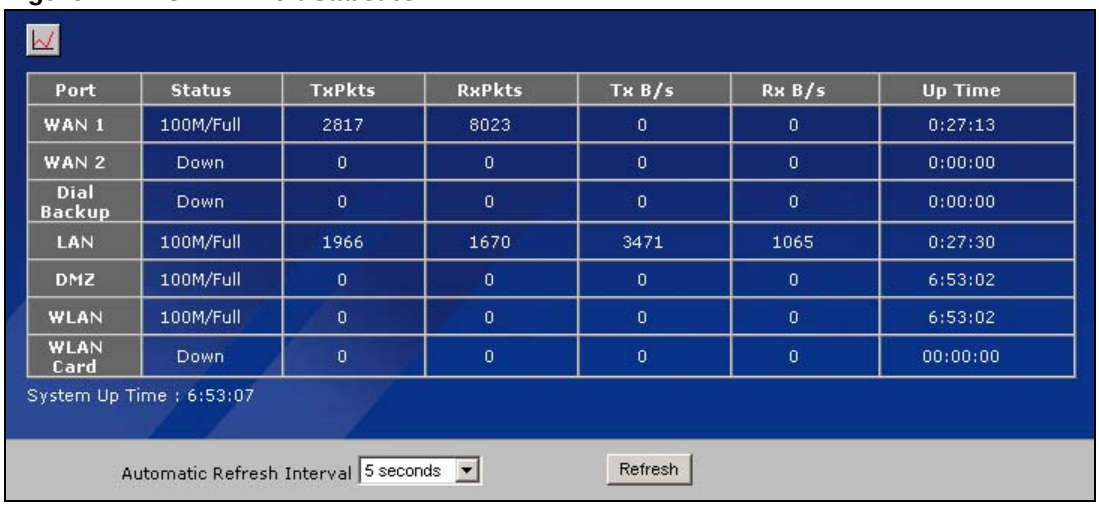
**Table 7** Screens Summary (continued)

| LINK | TAB | FUNCTION |
|---|---|---|
| MAINTENANCE | General | This screen contains administrative. |
| | Password | Use this screen to change your password. |
| | Time and Date | Use this screen to change your ZyWALL's time and date. |
| | Device Mode | Use this screen to configure and have your ZyWALL work as a router or a bridge. |
| | F/W Upload | Use this screen to upload firmware to your ZyWALL |
| | Backup & Restore | Use this screen to backup and restore the configuration or reset the factory defaults to your ZyWALL. |
| | Restart | This screen allows you to reboot the ZyWALL without turning the power off. |
| | Diagnosis | Use this screen to have the ZyWALL generate and send diagnostic files by e-mail and/or the console port. |
| LOGOUT | | Click this label to exit the web configurator. |

## 3.4.6 Port Statistics

Click **Port Statistics** in the **HOME** screen. Read-only information here includes port status and packet specific statistics. The **Poll Interval(s)** field is configurable. Not all items described are available on all models.

**Figure 17** HOME > Port Statistics




The following table describes the labels in this screen.

**Table 8** HOME > Port Statistics

| LABEL | DESCRIPTION |
|---|---|
|  | Click the icon to display the chart of throughput statistics. |
| Port | These are the ZyWALL's interfaces. |

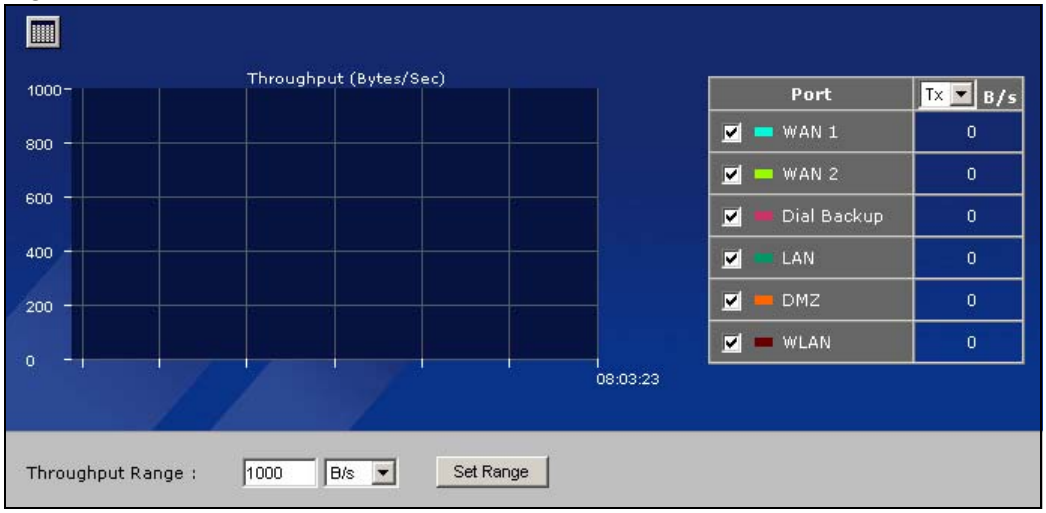
**Table 8** HOME > Port Statistics (continued)

| LABEL | DESCRIPTION |
|---|---|
| Status | For the WAN interface(s) and the Dial Backup port, this displays the port speed and duplex setting if you're using Ethernet encapsulation or the remote node name for a PPP connection and **Down** (line is down or not connected), **Idle** (line (ppp) idle), **Dial** (starting to trigger a call) or **Drop** (dropping a call) if you're using PPPoE encapsulation. Dial backup is not available in bridge mode.<br>For the LAN, DMZ and WLAN ports, this displays the port speed and duplex setting.<br>For the WLAN card, this displays the transmission rate when a wireless LAN card is inserted and WLAN is enabled or **Down** when a wireless LAN is not inserted or WLAN is disabled. |
| TxPkts | This is the number of transmitted packets on this port. |
| RxPkts | This is the number of received packets on this port. |
| Tx B/s | This displays the transmission speed in bytes per second on this port. |
| Rx B/s | This displays the reception speed in bytes per second on this port. |
| Up Time | This is the total amount of time the line has been up. |
| System Up Time | This is the total time the ZyWALL has been on. |
| Automatic Refresh Interval | Select a number of seconds or **None** from the drop-down list box to update all screen statistics automatically at the end of every time interval or to not update the screen statistics. |
| Refresh | Click this button to update the screen's statistics immediately. |

## 3.4.7 Show Statistics: Line Chart

Click the icon in the **Show Statistics** screen. This screen shows you a line chart of each port's throughput statistics.

**Figure 18** HOME > Show Statistics > Line Chart



The following table describes the labels in this screen.

**Table 9** HOME > Show Statistics > Line Chart

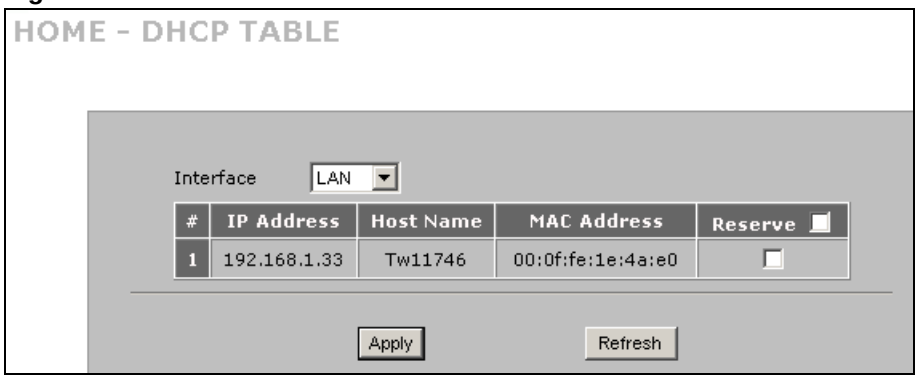
| LABEL | DESCRIPTION |
|---|---|
|  | Click the icon to go back to the **Show Statistics** screen. |
| Port | Select the check box(es) to display the throughput statistics of the corresponding interface(s). |
| B/s | Specify the direction of the traffic for which you want to show throughput statistics in this table.<br>Select **Tx** to display transmitted traffic throughput statistics and the amount of traffic (in bytes). Select **Rx** to display received traffic throughput statistics and the amount of traffic (in bytes). |
| Throughput Range | Set the range of the throughput (in **B/s**, **KB/s** or **MB/s**) to display.<br>Click **Set Range** to save this setting back to the ZyWALL. |

## 3.4.8 DHCP Table

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the ZyWALL as a DHCP server or disable it. When configured as a server, the ZyWALL provides the TCP/IP configuration for the clients. If DHCP service is disabled, you must have another DHCP server on your LAN, or else the computer must be manually configured.

Click **Show DHCP Table** in the **HOME** screen when the ZyWALL is set to router mode. Read-only information here relates to your DHCP status. The DHCP table shows current DHCP client information (including **IP Address**, **Host Name** and **MAC Address**) of all network clients using the ZyWALL's DHCP server.

**Figure 19** HOME > Show DHCP Table




The following table describes the labels in this screen.

**Table 10** HOME > Show DHCP Table

| LABEL | DESCRIPTION |
|---|---|
| Interface | Select **LAN**, **DMZ** or **WLAN** to show the current DHCP client information for the specified interface. |
| # | This is the index number of the host computer. |
| IP Address | This field displays the IP address relative to the # field listed above. |
| Host Name | This field displays the computer host name. |

**Table 10** HOME > Show DHCP Table (continued)

| LABEL | DESCRIPTION |
|---|---|
| MAC Address | The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal notation).<br>A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address. |
| Reserve | Select the check box in the heading row to automatically select all check boxes or select the check box(es) in each entry to have the ZyWALL always assign the selected entry(ies)'s IP address(es) to the corresponding MAC address(es) (and host name(s)). You can select up to 128 entries in this table. After you click **Apply**, the MAC address and IP address also display in the corresponding **LAN**, **DMZ** or **WLAN Static DHCP** screen (where you can edit them). |
| Refresh | Click **Refresh** to reload the DHCP table. |

## 3.4.9 VPN Status

Click **VPN** in the **HOME** screen. This screen displays read-only information about the active VPN connections. The **Poll Interval(s)** field is configurable. A Security Association (SA) is the group of security settings related to a specific VPN tunnel.

**Figure 20** HOME > VPN Status


The following table describes the labels in this screen.

**Table 11** HOME > VPN Status

| LABEL | DESCRIPTION |
|---|---|
| # | This is the security association index number. |
| Name | This field displays the identification name for this VPN policy. |
| Local Network | This field displays the IP address of the computer using the VPN IPSec feature of your ZyWALL. |
| Remote Network | This field displays IP address (in a range) of computers on the remote network behind the remote IPSec router. |
| Encapsulation | This field displays **Tunnel** or **Transport** mode. |

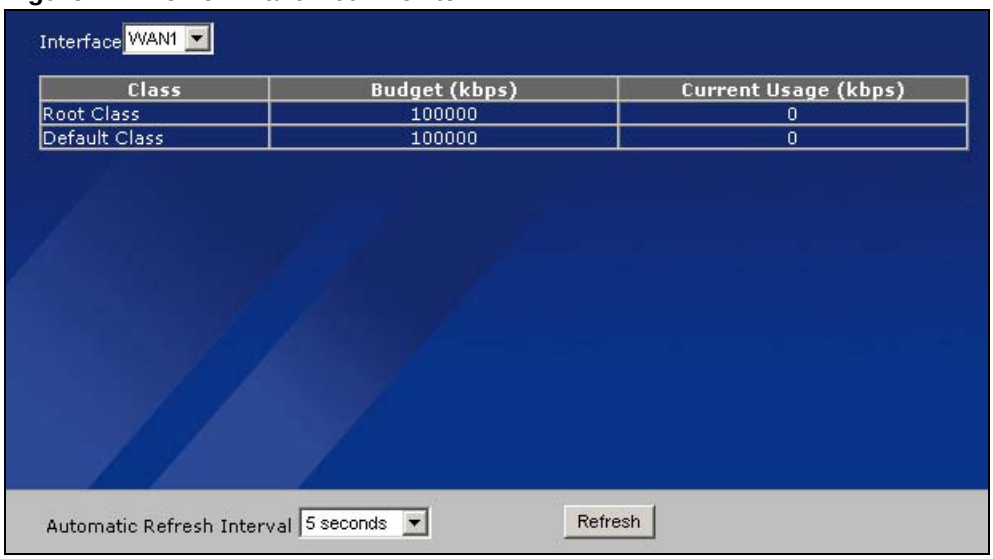
**Table 11** HOME > VPN Status

| LABEL | DESCRIPTION |
|---|---|
| IPSec Algorithm | This field displays the security protocols used for an SA.<br>Both AH and ESP increase ZyWALL processing requirements and communications latency (delay). |
| Automatic Refresh Interval | Select a number of seconds or **None** from the drop-down list box to update all screen statistics automatically at the end of every time interval or to not update the screen statistics. |
| Refresh | Click this button to update the screen's statistics immediately. |

## 3.4.10 Bandwidth Monitor

Click **Bandwidth** in the **HOME** screen to display the bandwidth monitor. This screen displays the device's bandwidth usage and allotments.

**Figure 21** Home > Bandwidth Monitor




The following table describes the labels in this screen.

**Table 12** ADVANCED > BW MGMT > Monitor

| LABEL | DESCRIPTION |
|---|---|
| Interface | Select an interface from the drop-down list box to view the bandwidth usage of its bandwidth classes. |
| Class | This field displays the name of the bandwidth class.<br>A **Default Class** automatically displays for all the bandwidth in the **Root Class** that is not allocated to bandwidth classes. If you do not enable maximize bandwidth usage on an interface, the ZyWALL uses the bandwidth in this default class to send traffic that does not match any of the bandwidth classes.[A] |
| Budget (kbps) | This field displays the amount of bandwidth allocated to the bandwidth class. |
| Current Usage (kbps) | This field displays the amount of bandwidth that each bandwidth class is using. |

**Table 12** ADVANCED > BW MGMT > Monitor

| LABEL | DESCRIPTION |
|---|---|
| Automatic Refresh Interval | Select a number of seconds or **None** from the drop-down list box to update all screen statistics automatically at the end of every time interval or to not update the screen statistics. |
| Refresh | Click this button to update the screen's statistics immediately. |

A. If you allocate all the root class's bandwidth to the bandwidth classes, the default class still displays a budget of 2 kbps (the minimum amount of bandwidth that can be assigned to a bandwidth class).

# 4

# Wizard Setup

This chapter provides information on the **Wizard Setup** screens in the web configurator. The Internet access wizard is only applicable when the ZyWALL is in router mode.

## 4.1 Wizard Setup Overview

The web configurator's setup wizards help you configure Internet and VPN connection settings.

In the **HOME** screen, click the **Wizard** icon  to open the **Wizard Setup Welcome** screen. The following summarizes the wizards you can select:

- **Internet Access Setup**
  Click this link to open a wizard to set up an Internet connection for **WAN1** on a ZyWALL with multiple WAN ports or the WAN port on a ZyWALL with a single WAN port.
- **VPN Setup**
  Use **VPN Setup** to configure a VPN connection that uses a pre-shared key. If you want to set the rule to use a certificate, please go to the VPN screens for configuration. See Section 4.3 on page 96.
- **Anti-Spam Setup**
  Use **Anti-Spam Setup** to select which traffic directions the anti-spam feature checks for unsolicited commercial or junk e-mail (spam). See Section 4.3 on page 96.

**Figure 22** Wizard Setup Welcome

# 4.2 Internet Access

The Internet access wizard screen has three variations 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.

## 4.2.1 ISP Parameters

The ZyWALL offers three choices of encapsulation. They are **Ethernet**, **PPTP** or **PPPoE**.

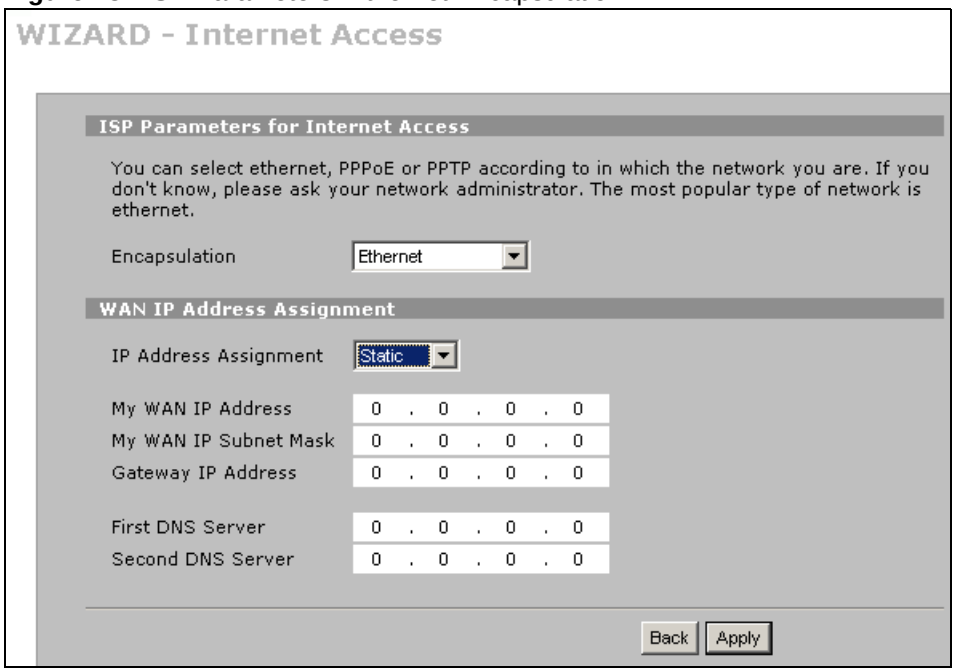
The wizard screen varies according to the type of encapsulation that you select in the **Encapsulation** field.

### 4.2.1.1 Ethernet

For ISPs (such as Telstra) that send UDP heartbeat packets to verify that the customer is still online, please create a **WAN-to-WAN/ZyWALL** firewall rule for those packets. Contact your ISP to find the correct port number.

Choose **Ethernet** when the WAN port is used as a regular Ethernet.

**Figure 23** ISP Parameters: Ethernet Encapsulation




The following table describes the labels in this screen.

**Table 13** ISP Parameters: Ethernet Encapsulation

| LABEL | DESCRIPTION |
|---|---|
| ISP Parameters for Internet Access | |
| Encapsulation | You must choose the **Ethernet** option when the WAN port is used as a regular Ethernet. Otherwise, choose **PPPoE** or **PPTP** for a dial-up connection. |
| WAN IP Address Assignment | |

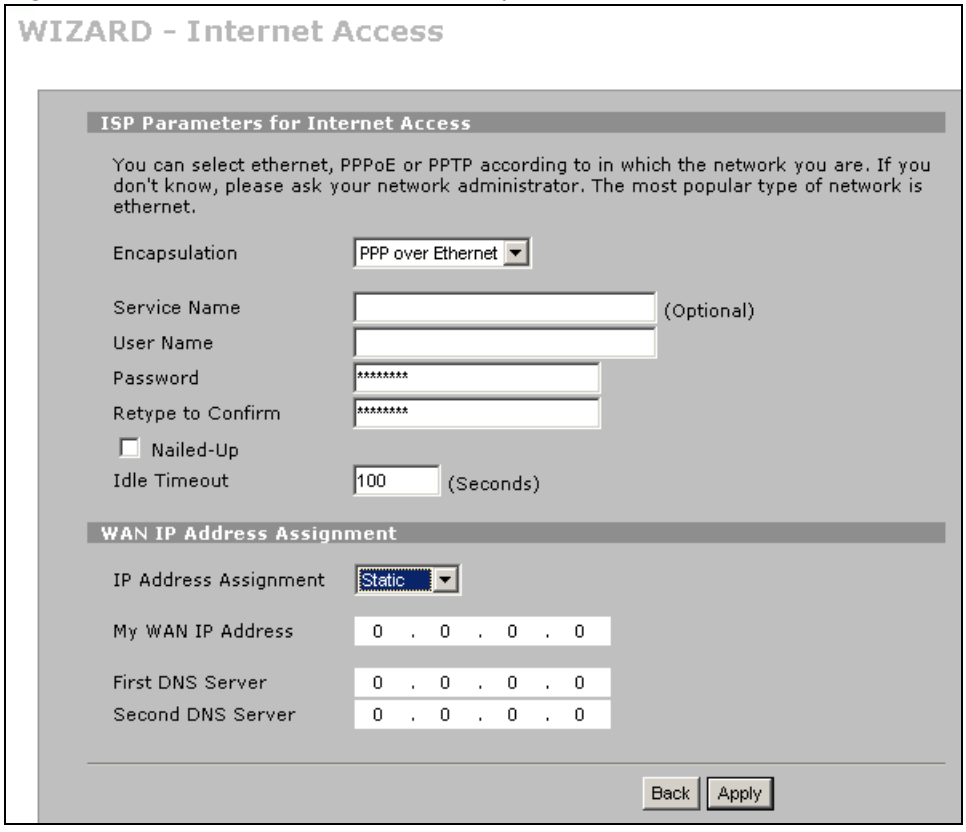
**Table 13** ISP Parameters: Ethernet Encapsulation

| LABEL | DESCRIPTION |
|---|---|
| IP Address Assignment | Select **Dynamic** If your ISP did not assign you a fixed IP address. This is the default selection.<br>Select **Static** If the ISP assigned a fixed IP address.<br>The fields below are available only when you select **Static**. |
| My WAN IP Address | Enter your WAN IP address in this field. |
| My WAN IP Subnet Mask | Enter the IP subnet mask in this field. |
| Gateway IP Address | Enter the gateway IP address in this field. |
| First DNS Server<br>Second DNS Server | 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 wizard screen. |
| Apply | Click **Apply** to save your changes and go to the next screen. |

### 4.2.1.2 PPPoE Encapsulation

Point-to-Point Protocol over Ethernet (PPPoE) functions as a dial-up connection. PPPoE is an IETF (Internet Engineering Task Force) standard specifying how a host personal computer interacts with a broadband modem (for example DSL, cable, wireless, etc.) to achieve access to high-speed data networks.

**Figure 24** ISP Parameters: PPPoE Encapsulation



The following table describes the labels in this screen.

**Table 14** ISP Parameters: PPPoE Encapsulation

| LABEL | DESCRIPTION |
|---|---|
| ISP Parameter for Internet Access | |
| Encapsulation | Choose an encapsulation method from the pull-down list box. **PPP over Ethernet** forms a dial-up connection. |
| Service Name | Type the name of your service provider. |
| User Name | Type the user name given to you by your ISP. |
| Password | Type the password associated with the user name above. |
| 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 Assignment | |
| IP Address Assignment | Select **Dynamic** If your ISP did not assign you a fixed IP address. This is the default selection.<br>Select **Static** If the ISP assigned a fixed IP address.<br>The fields below are available only when you select **Static**. |
| My WAN IP Address | Enter your WAN IP address in this field. |
| First DNS Server<br>Second DNS Server | 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 wizard screen. |
| Apply | Click **Apply** to save your changes and go to the next screen. |

#### 4.2.1.3 PPTP Encapsulation

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables transfers of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks.

PPTP supports on-demand, multi-protocol, and virtual private networking over public networks, such as the Internet.

The ZyWALL supports one PPTP server connection at any given time.

**Figure 25** ISP Parameters: PPTP Encapsulation


The following table describes the labels in this screen.

**Table 15** ISP Parameters: PPTP Encapsulation

| LABEL | DESCRIPTION |
|---|---|
| ISP Parameters for Internet Access | |
| Encapsulation | Select **PPTP** from the drop-down list box. To configure a PPTP client, you must configure the **User Name** and **Password** fields for a PPP connection and the PPTP parameters for a PPTP connection. |
| User Name | Type the user name given to you by your ISP. |
| Password | Type the password associated with the User Name above. |
| 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 | |
| My IP Address | Type the (static) IP address assigned to you by your ISP. |
| My IP Subnet Mask | Type the subnet mask assigned to you by your ISP (if given). |
| Server IP Address | Type the IP address of the PPTP server. |
| Connection ID/ Name | 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.<br>This field is optional and depends on the requirements of your xDSL modem. |

**Table 15** ISP Parameters: PPTP Encapsulation

| LABEL | DESCRIPTION |
|---|---|
| WAN IP Address Assignment | |
| IP Address Assignment | Select **Dynamic** If your ISP did not assign you a fixed IP address. This is the default selection.<br>Select **Static** If the ISP assigned a fixed IP address.<br>The fields below are available only when you select **Static**. |
| My WAN IP Address | Enter your WAN IP address in this field. |
| First DNS Server<br>Second DNS Server | 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 wizard screen. |
| Apply | Click **Apply** to save your changes and go to the next screen. |

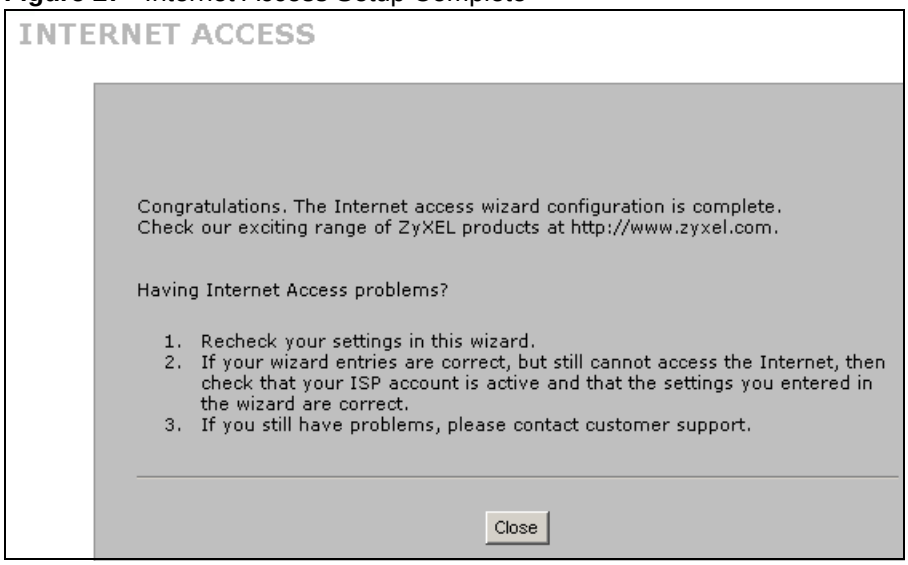
## 4.2.2 Internet Access Wizard: Second Screen

Click **Next** to go to the screen where you can register your ZyWALL and activate the free content filtering, anti-spam, anti-virus and IDP trial applications. Otherwise, click **Skip** to display the congratulations screen and click **Close** to complete the Internet access setup.

Make sure you have installed the ZyWALL Turbo Card before you activate the IDP and anti-virus subscription services.
Turn the ZyWALL off before you install or remove the ZyWALL Turbo Card.

**Figure 26** Internet Access Wizard: Second Screen

**Figure 27** Internet Access Setup Complete



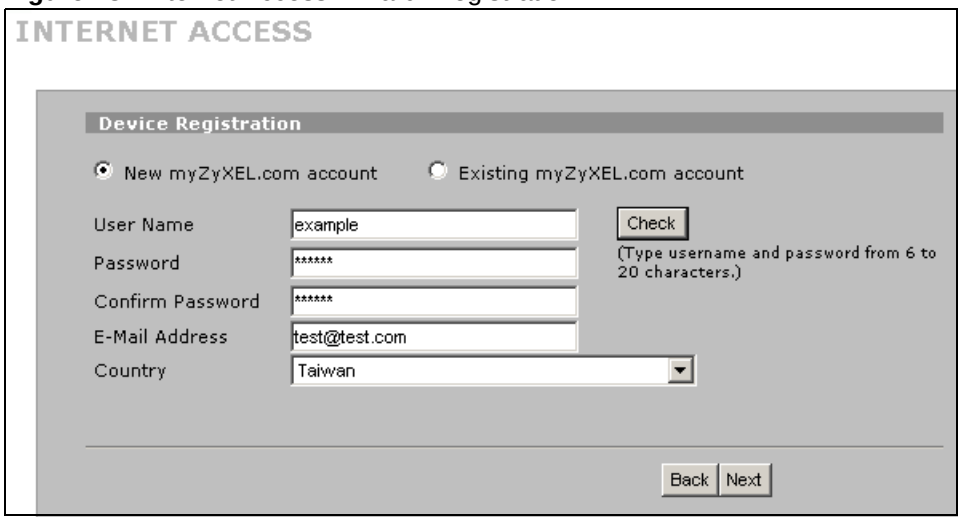

## 4.2.3 Internet Access Wizard: Registration

If you clicked **Next** in the previous screen (see Figure 26 on page 92), the following screen displays.

Use this screen to register the ZyWALL with myZyXEL.com. You must register your ZyWALL before you can activate trial applications of services like content filtering, anti-spam, anti-virus and IDP.

If you want to activate a standard service with your iCard's PIN number (license key), use the **REGISTRATION > Service** screen.

**Figure 28** Internet Access Wizard: Registration



The following table describes the labels in this screen.

**Table 16** Internet Access Wizard: 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. |
| User Name | 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 | Select your country from the drop-down box list. |
| Back | Click **Back** to return to the previous screen. |
| Next | Click **Next** to continue. |

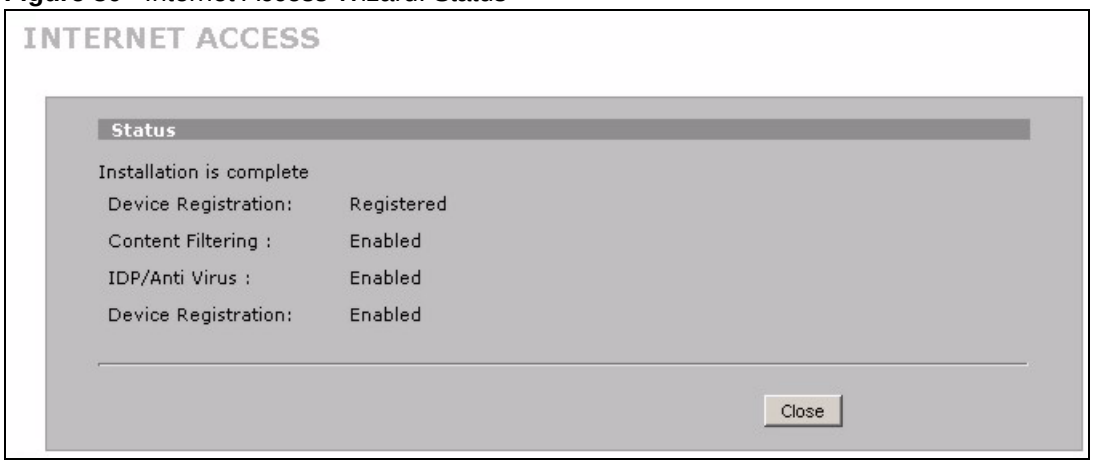
After you fill in the fields and click **Next**, the following screen shows indicating the registration is in progress. Wait for the registration progress to finish.

**Figure 29** Internet Access Wizard: Registration in Progress


## 4.2.4 Internet Access Wizard: Status

This screen shows your device registration and service subscription status. Click **Close** to leave the wizard screen when the registration and activation are done.

**Figure 30** Internet Access Wizard: Status




A screen similar to the following appears if the registration was not successful. Click **Return** to go back to the **Device Registration** screen and check your settings.

**Figure 31** Internet Access Wizard: Registration Failed


## 4.2.5 Internet Access Wizard: Service Activation

If the ZyWALL has been registered, the **Device Registration** screen is read-only and the **Service Activation** screen appears indicating what trial applications are activated after you click **Next**.

**Figure 32** Internet Access Wizard: Registered Device

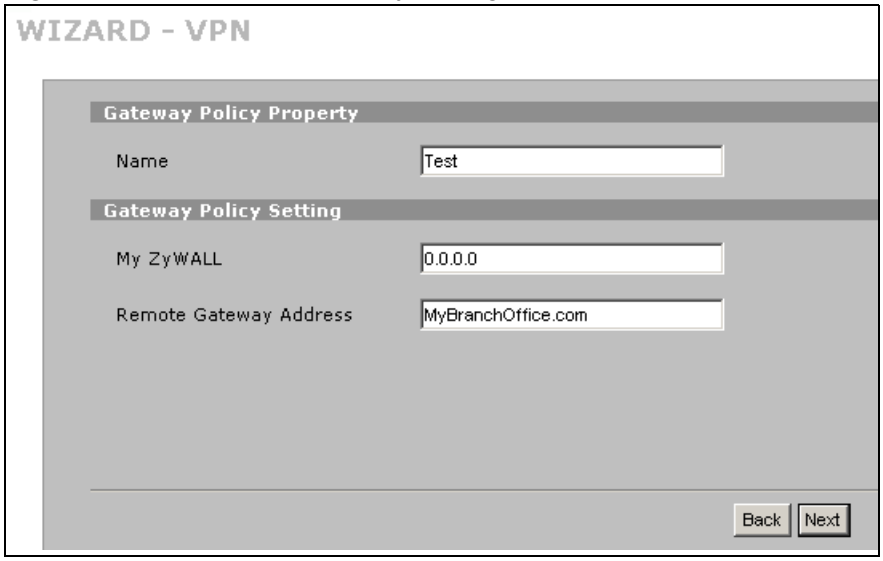
**Figure 33** Internet Access Wizard: Activated Services


## 4.3 VPN Wizard Gateway Setting

Use this screen to name the VPN gateway policy (IKE SA) and identify the IPSec routers at either end of the VPN tunnel.

Click **VPN Setup** in the **Wizard Setup Welcome** screen (Figure 22 on page 87) to open the VPN configuration wizard. The first screen displays as shown next.

**Figure 34** VPN Wizard: Gateway Setting




The following table describes the labels in this screen.

**Table 17** VPN Wizard: Gateway Setting

| LABEL | DESCRIPTION |
|---|---|
| Gateway Policy Property | |
| Name | Type up to 32 characters to identify this VPN gateway policy. You may use any character, including spaces, but the ZyWALL drops trailing spaces. |

**Table 17** VPN Wizard: Gateway Setting

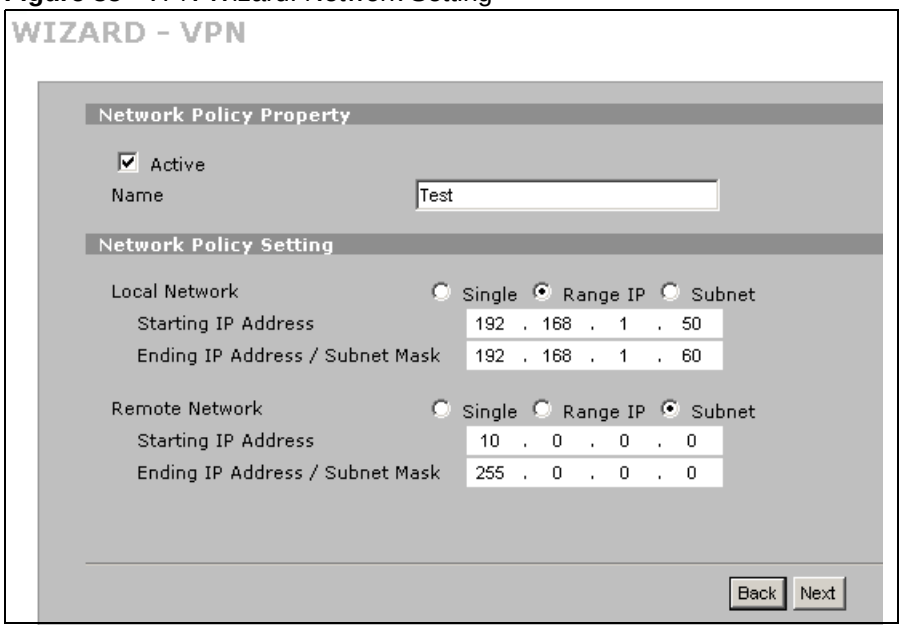
| LABEL | DESCRIPTION |
|---|---|
| My ZyWALL | When the ZyWALL is in router mode, enter the WAN IP address or the domain name of your ZyWALL or leave the field set to **0.0.0.0**.<br>The following applies if the **My ZyWALL** field is configured as **0.0.0.0**:<br>When the WAN interface operation mode is set to **Active/Passive**, the ZyWALL uses the IP address (static or dynamic) of the WAN interface that is in use.<br>When the WAN interface operation mode is set to **Active/Active**, the ZyWALL uses the IP address (static or dynamic) of the primary (highest priority) WAN interface to set up the VPN tunnel as long as the corresponding WAN1 or WAN2 connection is up. If the corresponding WAN1 or WAN2 connection goes down, the ZyWALL uses the IP address of the other WAN port.<br>If both WAN connections go down, the ZyWALL uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect. See the chapter on WAN for details on dial backup and traffic redirect.<br>When the ZyWALL is in bridge mode, this field is read-only and displays the ZyWALL's IP address. |
| Remote Gateway Address | 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. |
| Back | Click **Back** to return to the previous screen. |
| Next | Click **Next** to continue. |

## 4.4 VPN Wizard Network Setting

Use this screen to name the VPN network policy (IPSec SA) and identify the devices behind the IPSec routers at either end of a VPN tunnel.

Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.

**Figure 35** VPN Wizard: Network Setting




The following table describes the labels in this screen.

**Table 18** VPN Wizard: Network Setting

| LABEL | DESCRIPTION |
|---|---|
| Network Policy Property | |
| Active | If the **Active** check box is selected, packets for the tunnel trigger the ZyWALL to build the tunnel.<br>Clear the **Active** check box to turn the network policy off. The ZyWALL does not apply the policy. Packets for the tunnel do not trigger the tunnel. |
| Name | Type up to 32 characters to identify this VPN network policy. You may use any character, including spaces, but the ZyWALL drops trailing spaces. |
| Network Policy Setting | |
| Local Network | Local IP addresses must be static and correspond to the remote IPSec router's configured remote IP addresses.<br>Select **Single** for a single IP address. Select **Range IP** for a specific range of IP addresses. Select **Subnet** to specify IP addresses on a network by their subnet mask. |
| Starting IP Address | When the **Local Network** field is configured to **Single**, enter a (static) IP address on the LAN behind your ZyWALL. When the **Local Network** field is configured to **Range IP**, enter the beginning (static) IP address, in a range of computers on the LAN behind your ZyWALL. When the **Local Network** field is configured to **Subnet**, this is a (static) IP address on the LAN behind your ZyWALL. |
| Ending IP Address/ Subnet Mask | When the **Local Network** field is configured to **Single**, this field is N/A. When the **Local Network** field is configured to **Range IP**, enter the end (static) IP address, in a range of computers on the LAN behind your ZyWALL. When the **Local Network** field is configured to **Subnet**, this is a subnet mask on the LAN behind your ZyWALL. |
| Remote Network | Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses.<br>Select **Single** for a single IP address. Select **Range IP** for a specific range of IP addresses. Select **Subnet** to specify IP addresses on a network by their subnet mask. |

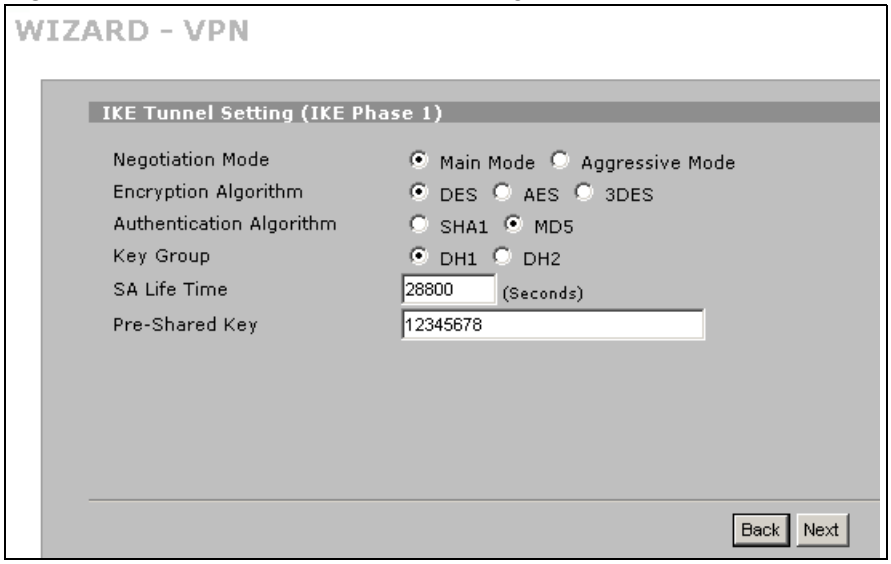
**Table 18** VPN Wizard: Network Setting

| LABEL | DESCRIPTION |
|---|---|
| Starting IP Address | When the **Remote Network** field is configured to **Single**, enter a (static) IP address on the network behind the remote IPSec router. When the **Remote Network** field is configured to **Range IP**, enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Remote Network** field is configured to **Subnet**, enter a (static) IP address on the network behind the remote IPSec router |
| Ending IP Address/ Subnet Mask | When the **Remote Network** field is configured to **Single**, this field is N/A. When the **Remote Network** field is configured to **Range IP**, enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Remote Network** field is configured to **Subnet**, enter a subnet mask on the network behind the remote IPSec router. |
| Back | Click **Back** to return to the previous screen. |
| Next | Click **Next** to continue. |

## 4.5 VPN Wizard IKE Tunnel Setting (IKE Phase 1)

Use this screen to specify the authentication, encryption and other settings needed to negotiate a phase 1 IKE SA.

**Figure 36** VPN Wizard: IKE Tunnel Setting



The following table describes the labels in this screen.

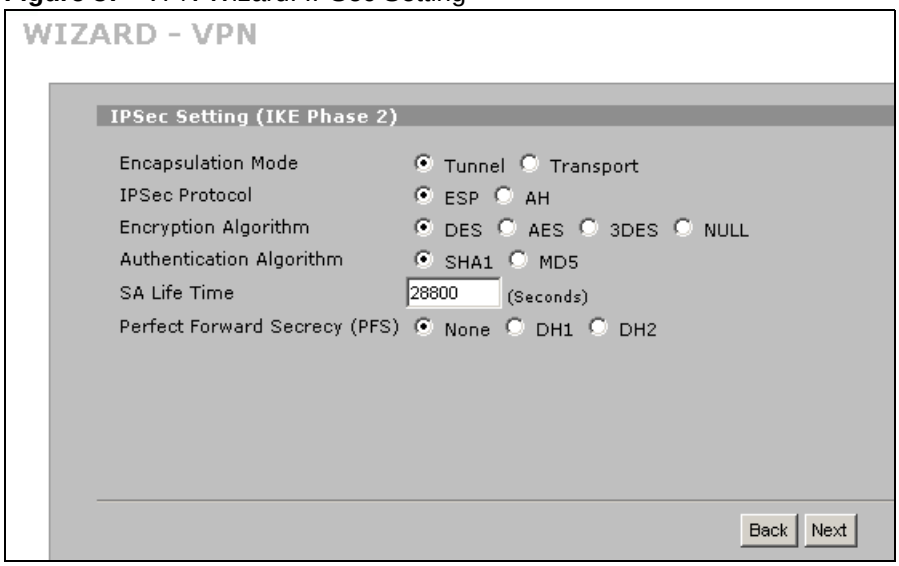
**Table 19** VPN Wizard: IKE Tunnel Setting

| LABEL | DESCRIPTION |
|---|---|
| Negotiation Mode | Select **Main Mode** for identity protection. Select **Aggressive Mode** 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. |
| 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. This implementation of **AES** uses a 128-bit key. **AES** is faster than **3DES**. |
| 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 **SHA-1** 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 (1 Kb) 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 180 seconds.<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. |
| 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 from 16 to 62 hexadecimal ("0-9", "A-F") characters. You must precede a hexadecimal key with a "0x (zero x), which is not counted as part of the 16 to 62 character range for the key. For example, in "0x0123456789ABCDEF", 0x denotes that the key is hexadecimal and 0123456789ABCDEF is the key itself.<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. |
| Back | Click **Back** to return to the previous screen. |
| Next | Click **Next** to continue. |

## 4.6 VPN Wizard IPSec Setting (IKE Phase 2)

Use this screen to specify the authentication, encryption and other settings needed to negotiate a phase 2 IPSec SA.

**Figure 37** VPN Wizard: IPSec Setting




The following table describes the labels in this screen.

**Table 20** VPN Wizard: IPSec Setting

| LABEL | DESCRIPTION |
|---|---|
| Encapsulation Mode | **Tunnel** is compatible with NAT, **Transport** is not.<br>Tunnel mode encapsulates the entire IP packet to transmit it securely. A 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). |
| IPSec Protocol | Select the security protocols used for an SA.<br>Both **AH** and **ESP** increase ZyWALL processing requirements and communications latency (delay). |
| 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. This implementation of **AES** uses a 128-bit key. **AES** is faster than **3DES**. Select **NULL** to set up a tunnel without encryption. When you select **NULL**, you do not enter an encryption key. |
| 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 **SHA-1** for maximum security. |
| SA Life Time (Seconds) | Define the length of time before an IKE SA automatically renegotiates in this field. The minimum value is 180 seconds.<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. |

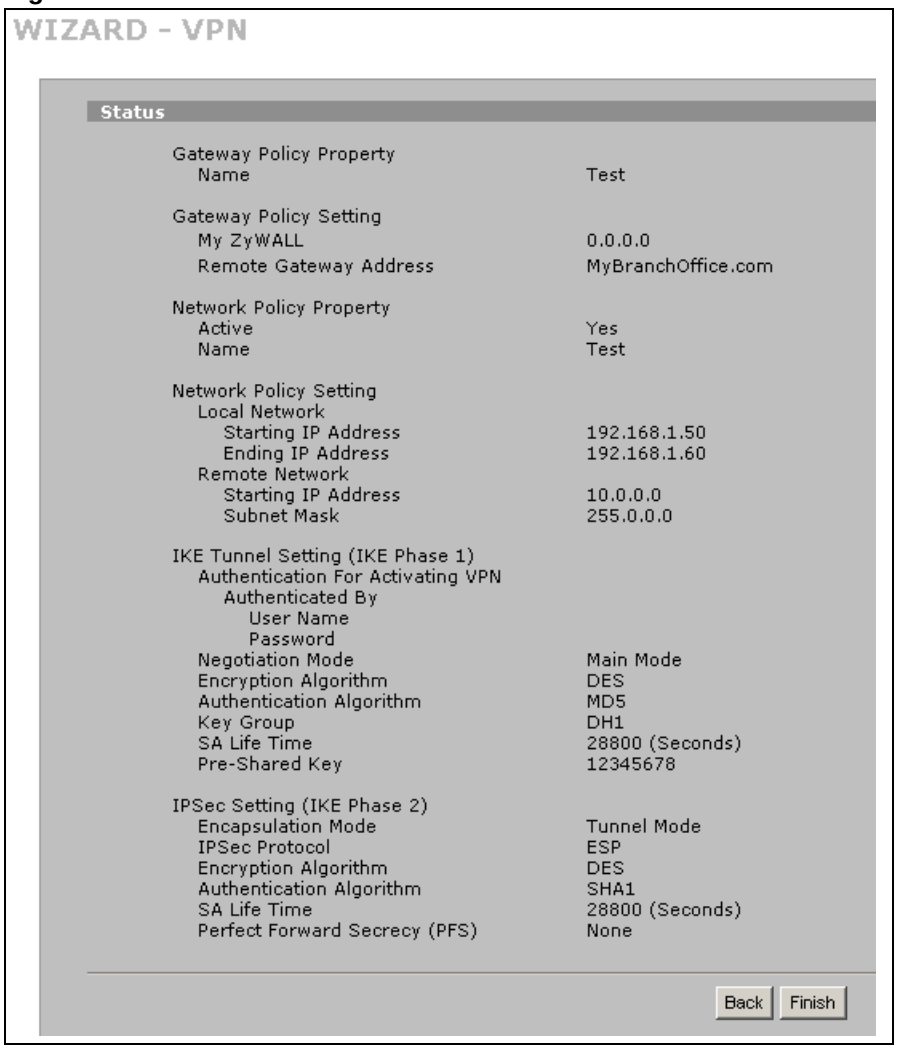
**Table 20** VPN Wizard: IPSec Setting (continued)

| LABEL | DESCRIPTION |
|---|---|
| Perfect Forward Secret (PFS) | Perfect Forward Secrecy (PFS) is disabled (**None**) by default in phase 2 IPSec SA setup. This allows faster IPSec setup, but is not so secure.<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 (more secure, yet slower). **DH5** refers to Diffie-Hellman Group 5 a 1536-bit random number. |
| Back | Click **Back** to return to the previous screen. |
| Next | Click **Next** to continue. |

## 4.7 VPN Wizard Status Summary

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 38** VPN Wizard: VPN Status



The following table describes the labels in this screen.

**Table 21** VPN Wizard: VPN Status

| LABEL | DESCRIPTION |
|---|---|
| Gateway Policy Property | |
| Name | This is the name of this VPN gateway policy. |
| Gateway Policy Setting | |
| My ZyWALL | This is the WAN IP address or the domain name of your ZyWALL in router mode or the ZyWALL's IP address in bridge mode. |
| Remote Gateway Address | This is the IP address or the domain name used to identify the remote IPSec router. |
| Network Policy Property | |
| Active | This displays whether this VPN network policy is enabled or not. |
| Name | This is the name of this VPN network policy. |
| Network Policy Setting | |
| Local Network | |
| Starting IP Address | This is a (static) IP address on the LAN behind your ZyWALL. |
| Ending IP Address/ Subnet Mask | When the local network is configured for a single IP address, this field is N/A. When the local network is configured for a range IP address, this is the end (static) IP address, in a range of computers on the LAN behind your ZyWALL. When the local network is configured for a subnet, this is a subnet mask on the LAN behind your ZyWALL. |
| Remote Network | |
| Starting IP Address | This is a (static) IP address on the network behind the remote IPSec router. |
| Ending IP Address/ Subnet Mask | When the remote network is configured for a single IP address, this field is N/A. When the remote network is configured for a range IP address, this is the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the remote network is configured for a subnet, this is a subnet mask on the network behind the remote IPSec router. |
| IKE Tunnel Setting (IKE Phase 1) | |
| Negotiation Mode | This shows **Main Mode** or **Aggressive Mode**. Multiple SAs connecting through a secure gateway must have the same negotiation mode. |
| Encryption Algorithm | This is the method of data encryption. Options can be **DES**, **3DES** or **AES**. |
| Authentication Algorithm | **MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. |
| Key Group | This is the key group you chose for phase 1 IKE setup. |
| SA Life Time (Seconds) | This is the length of time before an IKE SA automatically renegotiates. |
| Pre-Shared Key | This is a pre-shared key identifying a communicating party during a phase 1 IKE negotiation. |
| IPSec Setting (IKE Phase 2) | |
| Encapsulation Mode | This shows **Tunnel** mode or **Transport** mode. |

**Table 21** VPN Wizard: VPN Status (continued)

| LABEL | DESCRIPTION |
|---|---|
| IPSec Protocol | **ESP** or **AH** are the security protocols used for an SA. |
| Encryption Algorithm | This is the method of data encryption. Options can be **DES**, **3DES**, **AES** or **NULL**. |
| Authentication Algorithm | **MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. |
| SA Life Time (Seconds) | This is the length of time before an IKE SA automatically renegotiates. |
| Perfect Forward Secret (PFS) | Perfect Forward Secret (PFS) is disabled (**None**) by default in phase 2 IPSec SA setup. Otherwise, **DH1, DH2** or **DH5** are selected to enable PFS. |
| Back | Click **Back** to return to the previous screen. |
| Finish | Click **Finish** to complete and save the wizard setup. |

## 4.8 VPN Wizard Setup Complete

Congratulations! You have successfully set up the VPN rule for your ZyWALL. If you already had VPN rules configured, the wizard adds the new VPN rule after the last existing VPN rule.

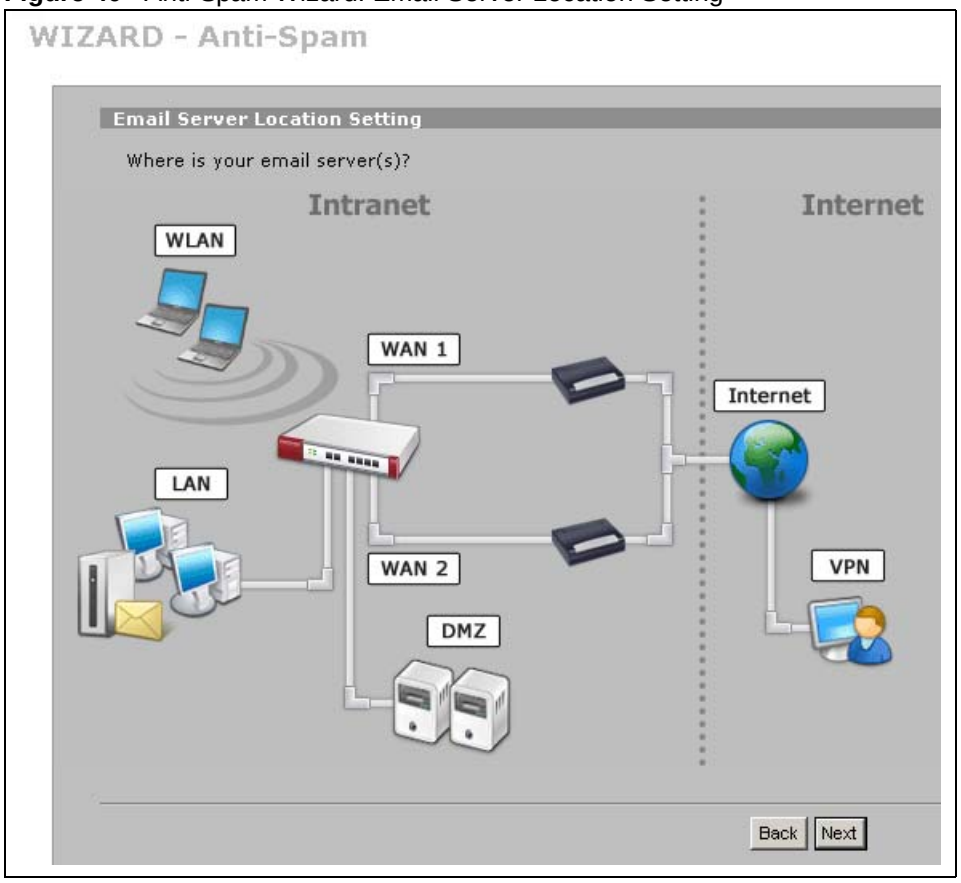
**Figure 39** VPN Wizard Setup Complete


## 4.9 Anti-Spam Wizard: Email Server Location Setting

Use this screen to select the locations where you have e-mail servers. An icon of an e-mail server appears at each spot you select.

The anti-spam wizard does NOT enable anti-spam.

**Figure 40** Anti-Spam Wizard: Email Server Location Setting




The following table describes the labels in this screen.

**Table 22** Anti-Spam Wizard: Email Server Location Setting

| LABEL | DESCRIPTION |
|---|---|
| Intranet | These are the networks directly connected to the ZyWALL.<br>• Select **WLAN** if you have an e-mail server(s) connected to the ZyWALL's WLAN.<br>• Select **WAN 1** if you have an e-mail server(s) connected to the ZyWALL's WAN 1.<br>• Select **LAN** if you have an e-mail server(s) connected to the ZyWALL's LAN.<br>• Select **WAN 2** if you have an e-mail server(s) connected to the ZyWALL's WAN.<br>• Select **DMZ** if you have an e-mail server(s) connected to the ZyWALL's DMZ. |
| Internet | These are the networks that the ZyWALL connects to through an Internet connection.<br>• Select **Internet** if the e-mail server(s) you use are on the Internet.<br>• Select **VPN** if you use a VPN tunnel to connect to an e-mail server(s). |
| Back | Click **Back** to return to the previous screen. |
| Next | Click **Next** to continue. |

## 4.10 Anti-Spam Wizard: Direction Recommendations

This screen displays recommended traffic flows to scan for spam based on the locations of your e-mail servers.

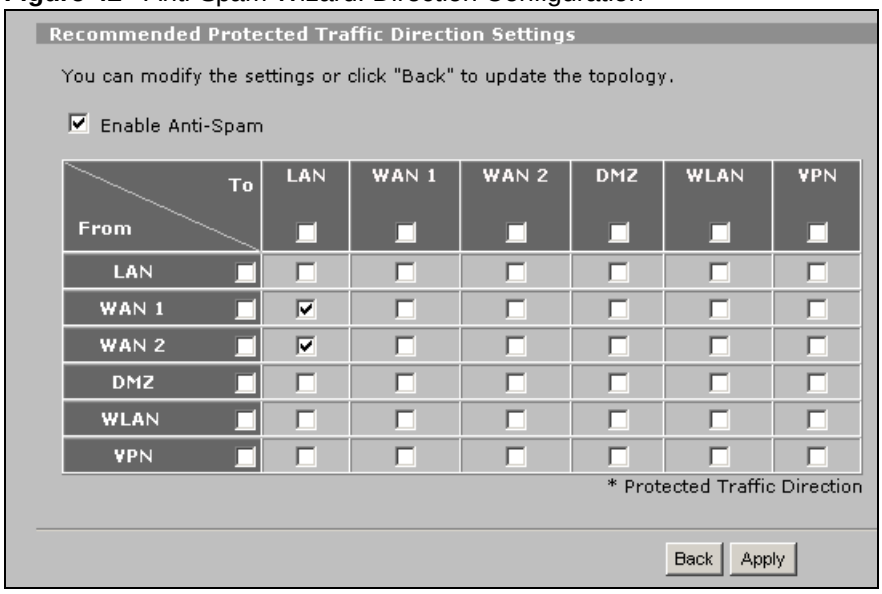
**Figure 41** Anti-Spam Wizard: Direction Recommendations


- For e-mail servers on the LAN, DMZ, or WLAN the ZyWALL recommends checking traffic that comes from the WAN to the zone(s) where the e-mail server is located. This is to check for spam coming to the ZyWALL's e-mail server from outside e-mail servers.
- For e-mail servers on the Internet, the ZyWALL recommends checking traffic that comes from the WAN to the LAN, DMZ, and WLAN zones. This is to check for spam coming to the ZyWALL's local users from the outside e-mail server.
- For e-mail servers located at the other end of a VPN tunnel, the ZyWALL recommends checking traffic that comes from the VPN to the LAN, DMZ, and WLAN zones. This is to check for spam coming to the ZyWALL's local users from the e-mail server at the VPN peer.
- If you have (your) e-mail server at the WAN zone, the ZyWALL recommends having anti-spam functionality installed on another device between the e-mail server and the Internet. Another option would be to move the e-mail server to the LAN, DMZ, or WLAN.
- Click **Back** to return to the previous screen.
- Click **Next** to continue.

## 4.11 Anti-Spam Wizard: Direction Configuration

Use this screen to select which traffic directions the anti-spam feature checks for spam.

**Figure 42** Anti-Spam Wizard: Direction Configuration




The following table describes the labels in this screen.

**Table 23** Anti-Spam Wizard: Direction Configuration

| LABEL | DESCRIPTION |
|---|---|
| Enable Anti-Spam | Select this check box to check traffic for spam SMTP (TCP port 25 and POP3 (TCP port 110) e-mail. |
| From, To | Select the directions of travel of packets that you want to check. Select or clear a row or column's first check box (with the interface label) to select or clear the interface's whole row or column.<br>You could for example have the ZyWALL check packets traveling in from the WAN to the interface your e-mail server is on. For example, **From WAN1 To DMZ**, or **From WAN2 To DMZ**.<br>**From LAN To LAN** means packets traveling from a computer on one LAN subnet to a computer on another LAN subnet via the LAN interface of the ZyWALL. The ZyWALL does not check packets traveling from a LAN computer to another LAN computer on the same subnet.<br>**From WAN1 To WAN1** means packets that come in through the WAN 1 interface and the ZyWALL routes back out through the WAN 1 interface.<br>**From VPN** means traffic that came into the ZyWALL through a VPN tunnel and is going to the selected "to" interface. For example, **From VPN To LAN** specifies the VPN traffic that is going to the LAN or terminating at the ZyWALL's LAN interface. The ZyWALL checks the traffic after decrypting it.<br>**To VPN** is traffic that comes in through the selected "from" interface and goes out through any VPN tunnel. For example, **From LAN To VPN** specifies the traffic that is coming from the LAN and going out through a VPN tunnel. The ZyWALL checks the traffic before encrypting it.<br>**From VPN To VPN** means traffic that comes in through a VPN tunnel and goes out through (another) VPN tunnel. This is the case when the ZyWALL is the hub in a hub-and-spoke VPN. The ZyWALL checks the traffic after decrypting it (before encrypting it again).<br>Note: The VPN connection directions apply to the traffic going to or from the ZyWALL's VPN tunnels. They do not apply to other VPN traffic for which the ZyWALL is not one of the gateways (VPN pass-through traffic). |

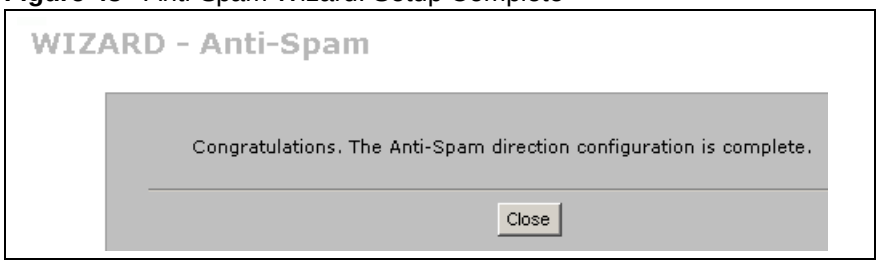
**Table 23** Anti-Spam Wizard: Direction Configuration

| LABEL | DESCRIPTION |
|---|---|
| Back | Click **Back** to return to the previous screen. |
| Next | Click **Next** to continue. |

## 4.12 Anti-Spam Wizard: Setup Complete

Congratulations! You have successfully set up the directions that the anti-spam feature checks for spam. This does not enable the anti-spam feature. Go to the **SECURITY > ANTI-SPAM** screens to enable anti-spam.

**Figure 43** Anti-Spam Wizard: Setup Complete



# 5

# Tutorials

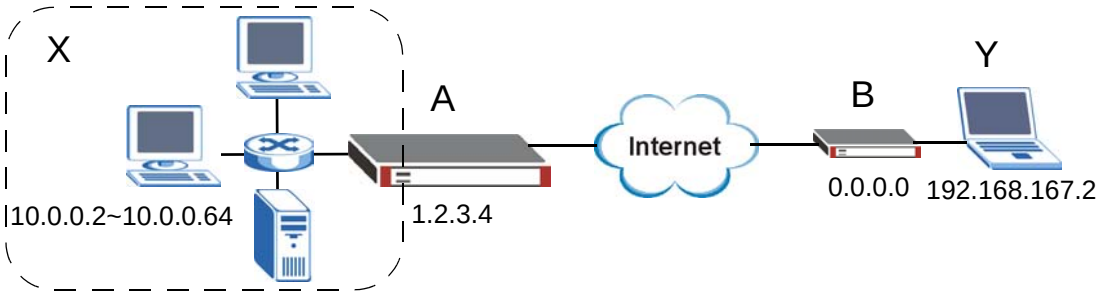
This chapter gives examples of how to configure some of your ZyWALL's key features. See the related chapter on a feature for more details.

## 5.1 Dynamic VPN Rule Configuration

Dynamic VPN rules allow VPN connections from IPSec routers with dynamic WAN IP addresses. This tutorial shows how to configure a basic VPN (Virtual Private Network) tunnel to allow a traveling sales manager named Bob (**Y** in the figure) using a ZyWALL P1 (**B**) to securely connect to computers and servers on the office network **X** behind a ZyWALL 70 (**A**).

- The ZyWALLs are peers.
- ZyWALL **B** has a dynamically-assigned WAN IP addresses (represented by 0.0.0.0), so only ZyWALL **B** can initiate (trigger) the VPN tunnel.
- ZyWALL **B** automatically initiates a VPN tunnel to ZyWALL A whenever **Y** tries to connect to an IP address from 10.0.0.2 to 10.0.0.64 and passes the identification authentication.

**Figure 44** Dynamic VPN Rule Example




This example uses the following settings.

**Table 24** Dynamic VPN Rule Tutorial Settings

| FIELD | ZYWALL A (COMPANY) | ZYWALL B (BOB) |
|---|---|---|
| Gateway Policy Property Name (identifies the VPN rule) | A-B_Gateways | A-B_Gateways |
| My ZyWALL (ZyWALL's WAN IP address) | 1.2.3.4 | 0.0.0.0 |
| Primary Remote Gateway Address (peer ZyWALL's WAN IP address) | 0.0.0.0 | 1.2.3.4 |
| Network Policy Property Name (name of the policy that identifies the networks behind the ZyWALLs) | X-Y_Networks | X-Y_Networks |

**Table 24** Dynamic VPN Rule Tutorial Settings

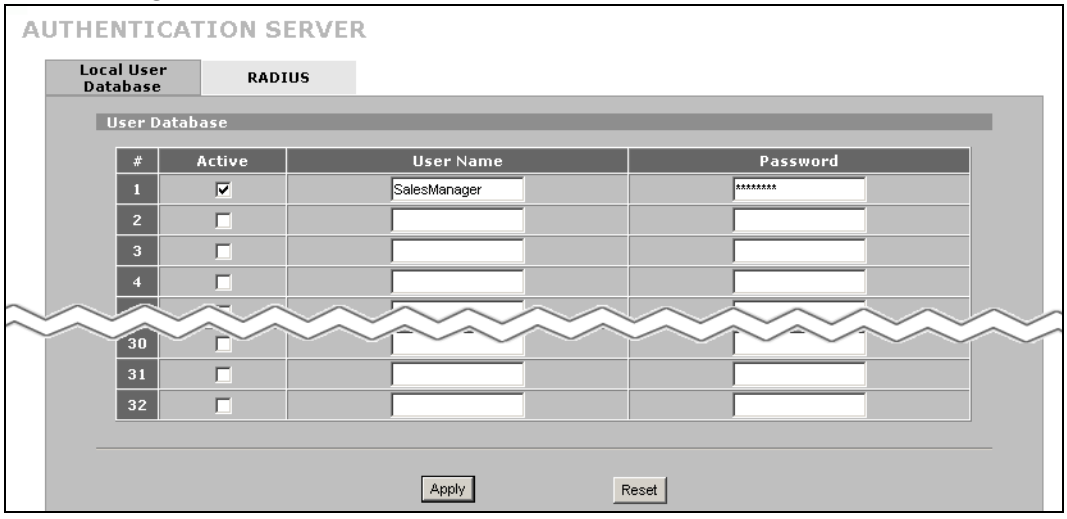
| FIELD | ZYWALL A (COMPANY) | ZYWALL B (BOB) |
|---|---|---|
| Local Network (network behind the local ZyWALL)<br><br>Note: Use static IP addresses or static DHCP to make sure the computers behind the ZyWALLs always use these IP addresses. | 10.0.0.2 ~10.0.0.64 | 192.168.167.2 |
| Remote Network (network behind the peer ZyWALL) | 0.0.0.0 | 10.0.0.2 ~10.0.0.64 |
| Pre-Shared Key (password) | MyPre-123!@# | MyPre-123!@# |
| Extended Authentication | Enabled, Server Mode | Enabled, Client Mode |
| Extended Authentication Username and Password | (in Local User Database)<br>SalesManager, Manager1234 | (in VPN Gateway Policy Edit)<br>SalesManager, Manager1234 |

## 5.1.1 Configure Bob's User Account

This example includes extended authentication. Bob has to enter the correct username and password to use the ZyWALL tunnel. This keeps others from using Bob's ZyWALL if it is lost or stolen. ZyWALL A needs to check the VPN tunnel requests that come in from ZyWALL B. In this example, you configure a local user database account named "SalesManager" on ZyWALL A.

1 Go to **SECURITY** > **AUTH SERVER**.

2 Add and activate accounts for the users. In this example, enter "SalesManager" with "Manager1234".




3 Click **Apply**.

## 5.1.2 VPN Gateway and Network Policy Configuration

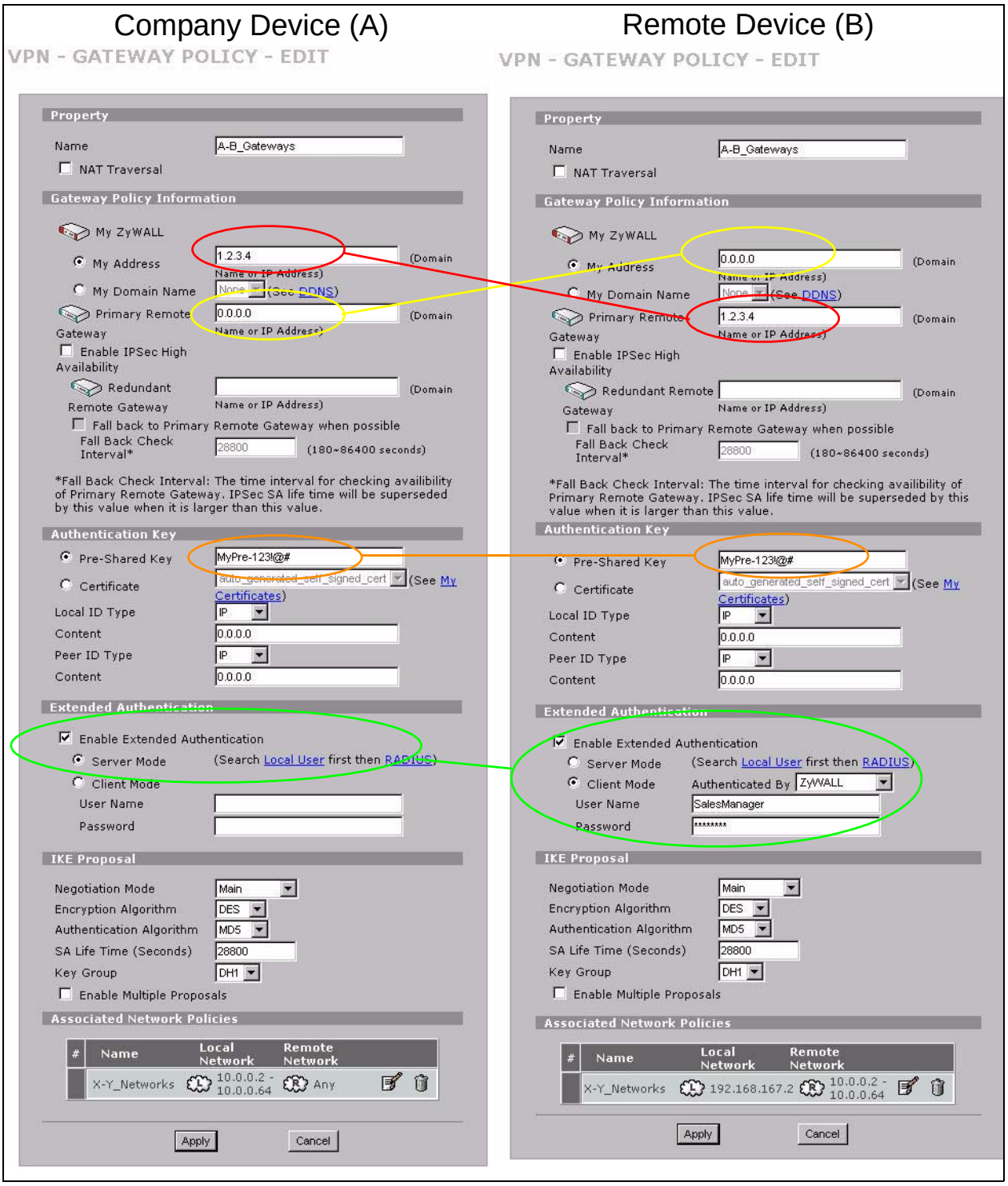
This section covers how to configure the company's ZyWALL (A) and the telecommuter's ZyWALL (B).

1 Click **SECURITY** > **VPN** > **VPN Rules (IKE)**, and then the add gateway policy ( ) icon to display the **Edit Gateway Policy** screen. Use this screen to configure the VPN gateway policy that identifies the ZyWALLs.

The company's ZyWALL (A) and the telecommuter's ZyWALL (B) gateway policy edit screens are shown next.

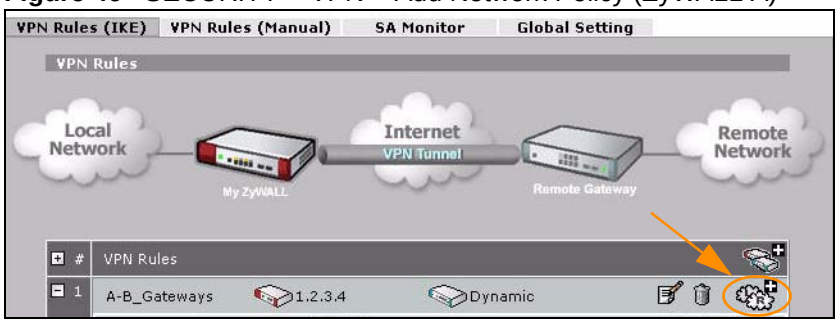
- The information that identifies the ZyWALL 70 (A) is circled in red.
- The information that identifies the ZyWALL P1 (B) is circled in yellow.
- Information that is the same in both is circled in orange.
- Extended authentication settings are in green.

**Figure 45** VPN Gateway Policy Edit Screens




2 After you click **Apply**, the A-B_Gateways gateway policy displays as shown next. Click **SECURITY** > **VPN** and the A-B_Gateways' add network policy ( ) icon. The following figure shows ZyWALL A's screen.

**Figure 46** SECURITY > VPN > Add Network Policy (ZyWALL A)

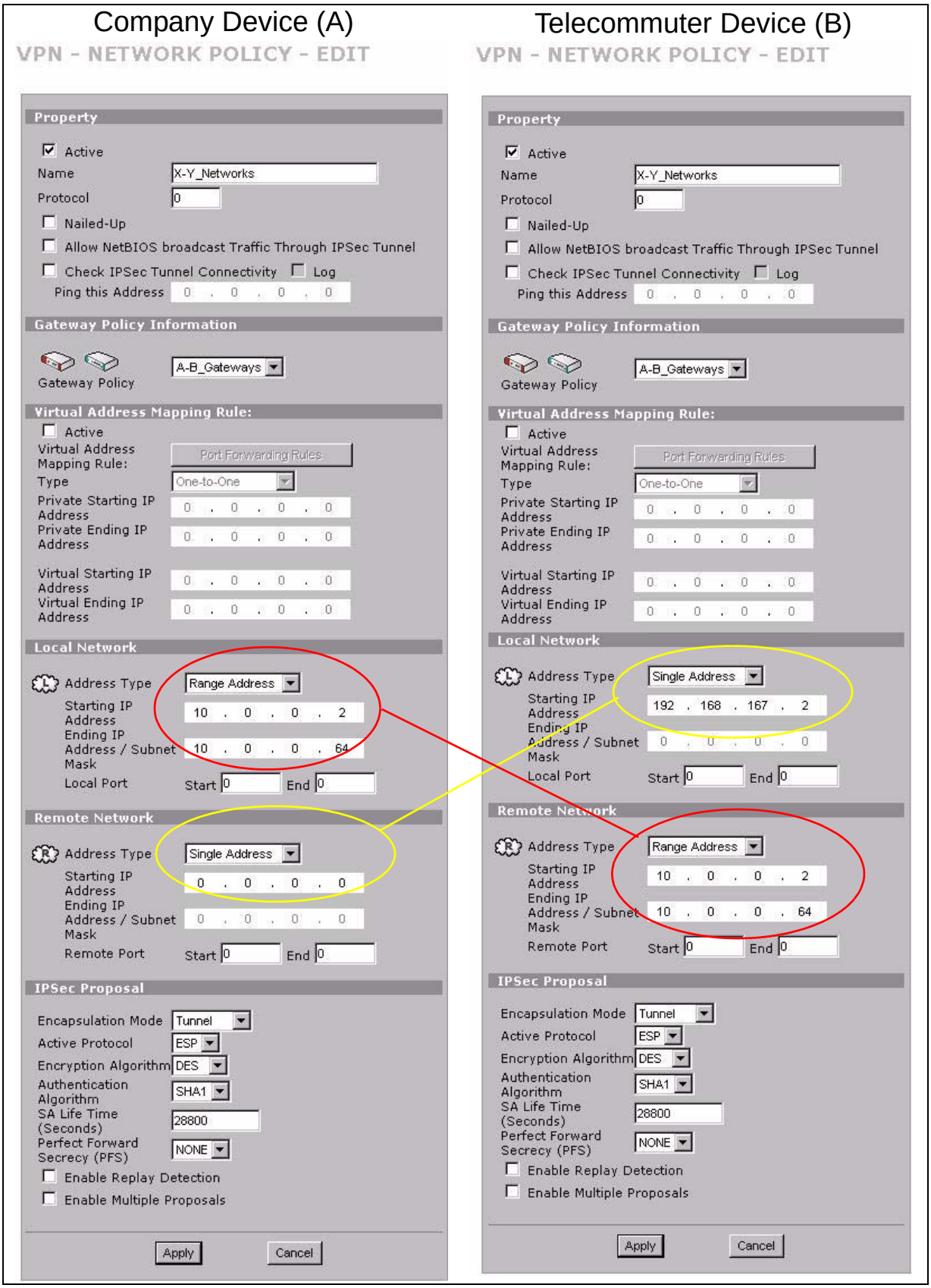



3 Edit the **VPN-Network Policy -Edit** screen to configure network policies. A network policy identifies the devices behind the IPSec routers at either end of a VPN tunnel and specifies the authentication, encryption and other settings needed to negotiate a phase 2 IPSec SA.

Here are the company's ZyWALL (A) and the telecommuter's ZyWALL (B) network policy edit screens.

- The information that identifies network X is circled in red.
- The information that identifies network Y is circled in yellow.

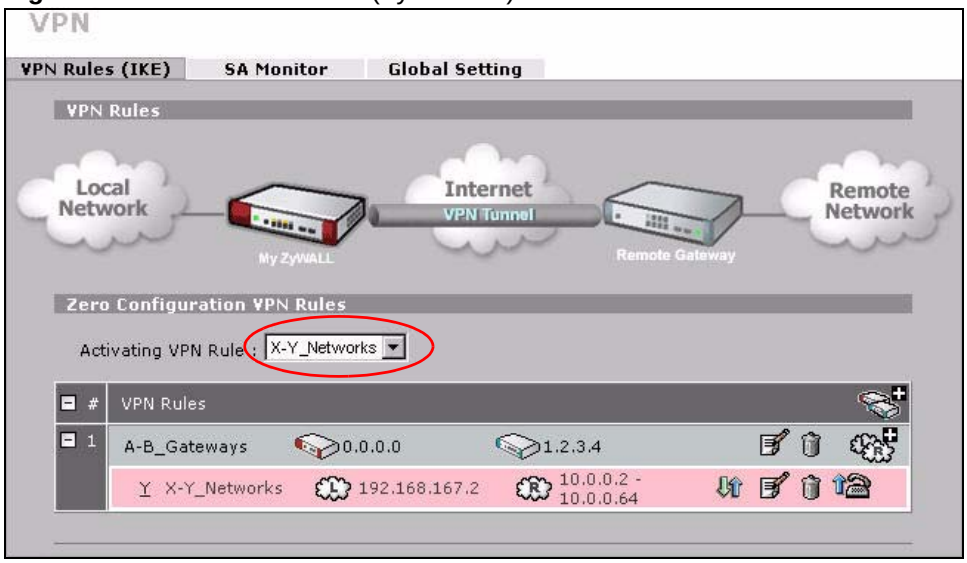
**Figure 47** VPN Network Policy Edit Screens



4 After you click **Apply**, the network policy displays with the gateway policy.

5 In the ZyWALL B, select "X-Y_Networks" in the **Activating VPN Rule** field to activate the VPN rule. The color of "X-Y_Networks" VPN policy changes to pink.

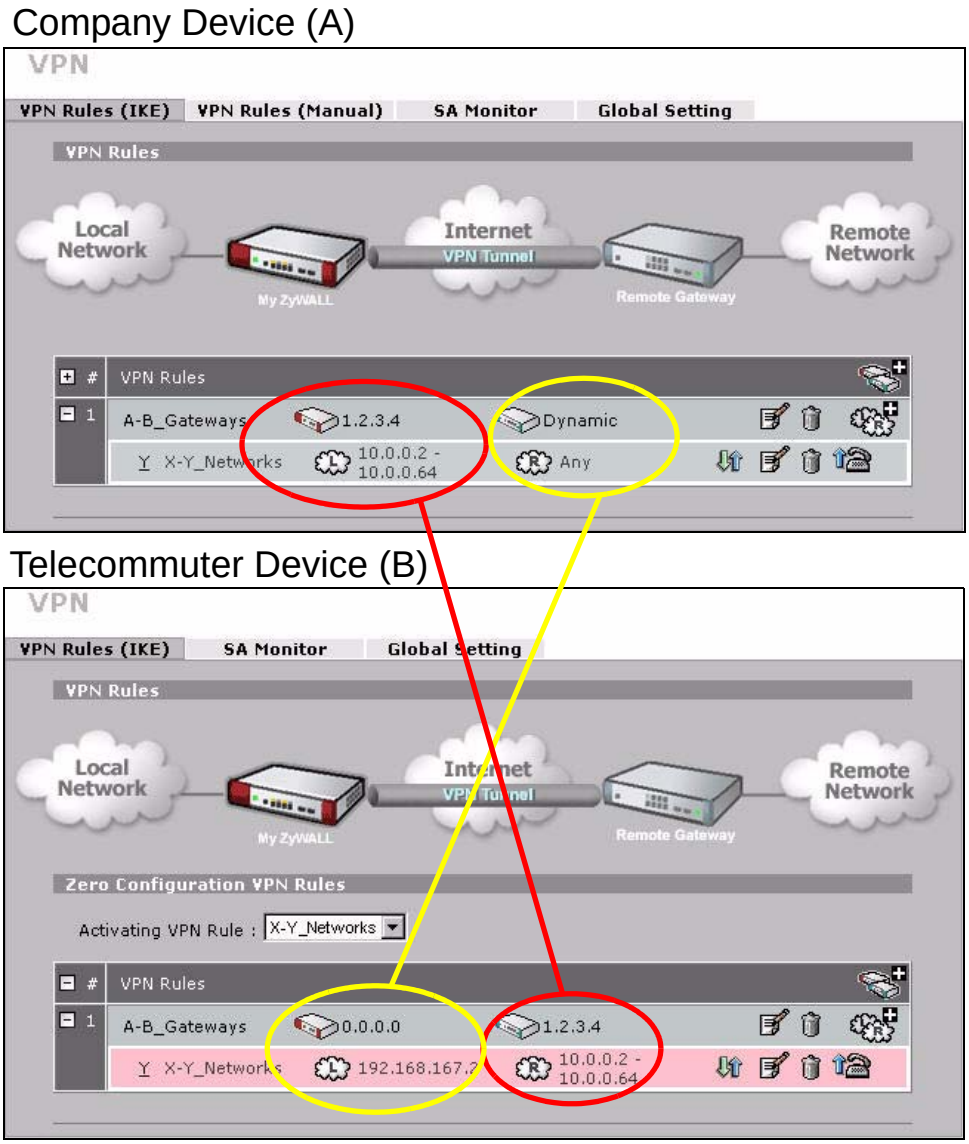
**Figure 48** Activate VPN Rule (ZyWALL B)




6 Review the settings on both ZyWALLs as shown next.

- The information that identifies the ZyWALL 70 (A) and network X is circled in red.
- The information that identifies the ZyWALL P1 (B) and network Y is circled in yellow.

**Figure 49** Tutorial: VPN Summary Screens Comparison Example



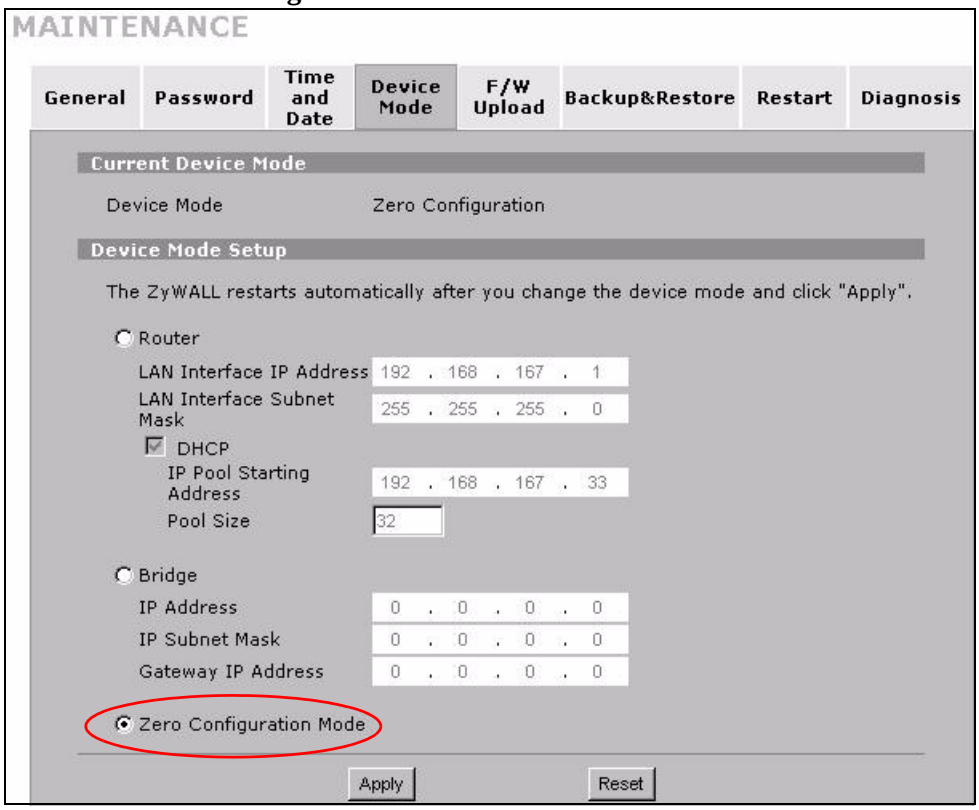

You have configured the company's ZyWALL (A) and the telecommuter's ZyWALL (B).

## 5.1.3 Configure Zero Configuration Mode on ZyWALL B

The ZyWALL P1's zero configuration mode provides a simplified user mode for the web configurator interface. The user uses this interface to configure the ZyWALL's Internet access settings and log into the VPN tunnel (see Section 5.1.4 on page 117). Do the following to have the telecommuter's ZyWALL (B) use zero configuration mode.

1. Log into ZyWALL B's web configurator.
2. Go to **MAINTENANCE** and click the **Device Mode** tab.

3 Select **Zero Configuration Mode**.




4 Click **Apply**. The system reboots automatically and restarts in zero configuration mode.

## 5.1.4 Testing Your VPN Configuration

Test the VPN configuration before giving the ZyWALL P1 to Bob.

1 ZyWALL A should already be connected to the Internet using it's public WAN IP address. Connect ZyWALL B to the Internet. Make sure it gets a public WAN IP. You may have to take ZyWALL B to another location if it cannot get a public IP address at the company.

2 Configure one computer to use IP address 192.168.167.2/24 behind ZyWALL B. Use "ipconfig" in the command mode to ensure the IP address is properly configured.

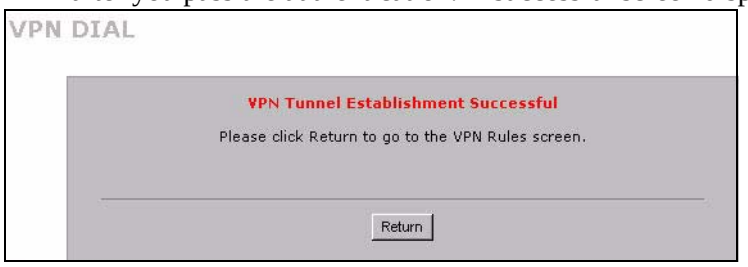
**Figure 50** Check The Telecommuter's Computer IP Address

```
C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.167.2
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.167.1
```

3 Open a web browser (like Internet Explorer) to connect to the ZyWALL P1's LAN IP address (http://192.168.167.1 in this example).

4 The user mode screen for VPN authentication displays. Enter the user name "SalesManager" and password "Manager1234". Click **Activate**.


5 ZyWALL B automatically initiates and negotiates the VPN tunnel with ZyWALL A after you pass the authentication. A successful screen displays. Click **Return**.




6 Send a ping from the telecommuter's computer (IP address 192.168.167.2) to a device on the office network (**X**), for example 10.0.0.2. You should get a response.

To do this in most Windows computers, click **Start** > **Run**, enter `cmd`, and then enter `ping` followed by the IP address of a computer on network **X**. Here is an example.

**Figure 51** Telecommuter Pinging a Network X IP Address Example

```
C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time=3ms TTL=126
Reply from 10.0.0.2: bytes=32 time=2ms TTL=126
Reply from 10.0.0.2: bytes=32 time=2ms TTL=126
Reply from 10.0.0.2: bytes=32 time=2ms TTL=126

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum =  3ms, Average =  2ms
```

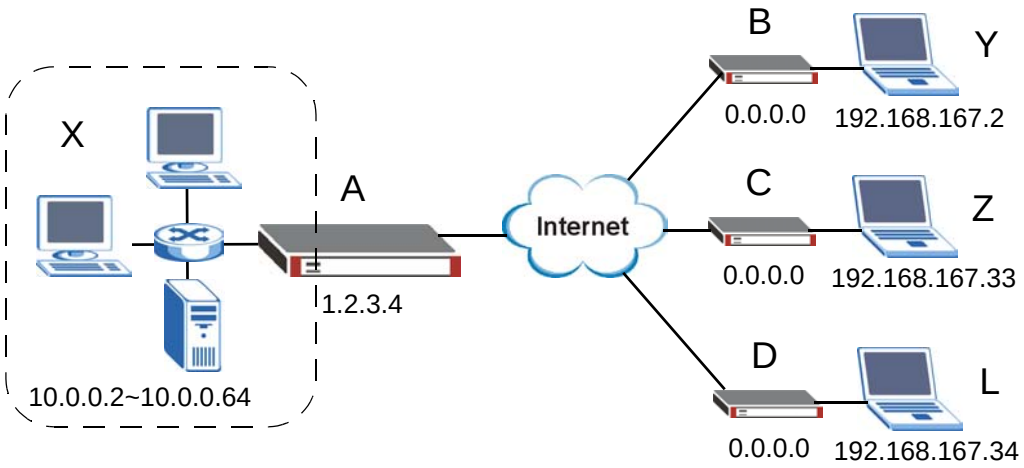
If there is no reply to the ping, the system log can help identify a configuration problem. Click **LOGS** to see the system log. See Section  on page 561 for information on the log messages. You may need to click **LOGS** > **Log Settings** in the advanced web configurator and make sure IKE and IPSec logging is enabled at both ends. You can clear the existing log and re-attempt to build the tunnel (this makes it easier to identify the relevant logs).

When you can ping IP address 10.0.0.2 from the computer with IP address 192.168.167.2 behind ZyWALL B, you know the VPN tunnel works.

### 5.1.5 Using the Dynamic VPN Rule for More VPN Tunnels

Other remote users (like sales people and telecommuters) using IPSec routers with dynamic WAN IP addresses can also use the same gateway and network policy on ZyWALL A. The gateway policies you configure on the remote IPSec routers differ by user name and password. The network policies on the remote IPSec routers differ by the IP address of the computer behind the remote IPSec router. Even though all of the remote IPSec routers use the same gateway policy and network policy on ZyWALL A, ZyWALL A builds a different VPN tunnel for each remote IPSec router. See Section 19.9 on page 379 to display VPN tunnels.

**Figure 52** Additional Dynamic VPN Rules Example




- Create a unique user name and password for each remote IPSec router in ZyWALL A's local user database (or on a RADIUS server that ZyWALL A is configured to use).
- Configure a gateway policy on each remote IPSec router. Use the same **MyZyWALL** and **Primary Remote Gateway** address and **Pre-Shared Key** settings on all of the remote IPSec routers, but a different user name and password for each.
- Configure a different network policy for each remote IPSec router. Make sure the IP addresses of the computers (behind the remote IPSec routers) that can trigger the dynamic rule VPN tunnels do not overlap with each other. For example, computers **Y**, **Z**, and **L** all use different private IP addresses. You can also use virtual address mapping (NAT over IPSec) to avoid an overlap (see Section  on page 393).

## 5.2 Security Settings for VPN Traffic

The ZyWALL can apply the firewall, IDP, anti-virus, anti-spam and content filtering to the traffic going to or from the ZyWALL's VPN tunnels. The ZyWALL applies the security settings to the traffic before encrypting VPN traffic that it sends out or after decrypting received VPN traffic.

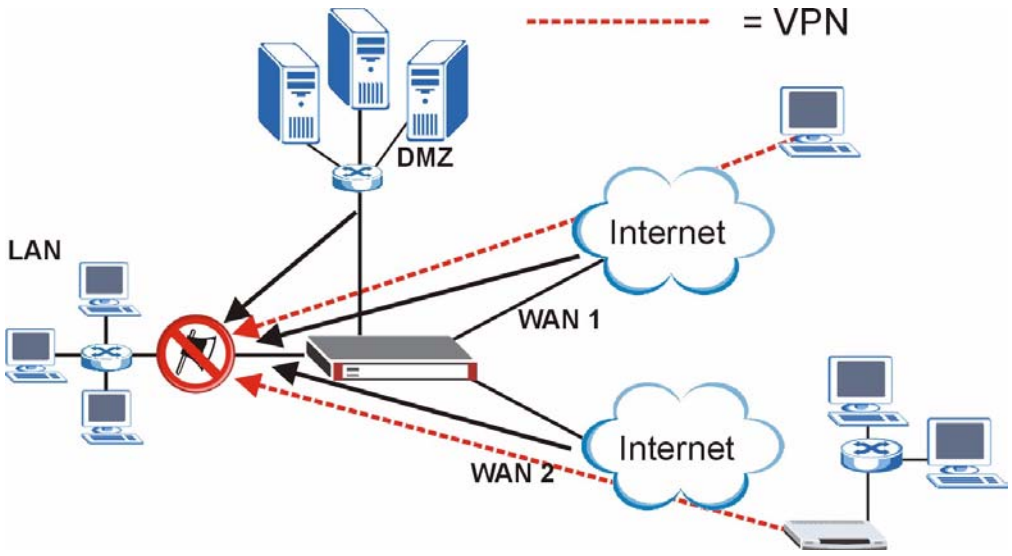
The security settings apply to VPN traffic going to or from the ZyWALL's VPN tunnels. They do not apply to other VPN traffic for which the ZyWALL is not one of the gateways (VPN pass-through traffic).

You can turn on content filtering for all of the ZyWALL's VPN traffic (regardless of its direction of travel). You can apply firewall, IDP, anti-virus and anti-spam security to VPN traffic based on its direction of travel. The following examples show how you do this for IDP and the firewall.

## 5.2.1 IDP for From VPN Traffic Example

You can apply security settings to the **From VPN** packet direction to protect your network from attacks, intrusions, viruses and spam that may come in through a VPN tunnel. For example, you can use IDP to protect your LAN from intrusions that might come in through any of the VPN tunnels or interfaces.

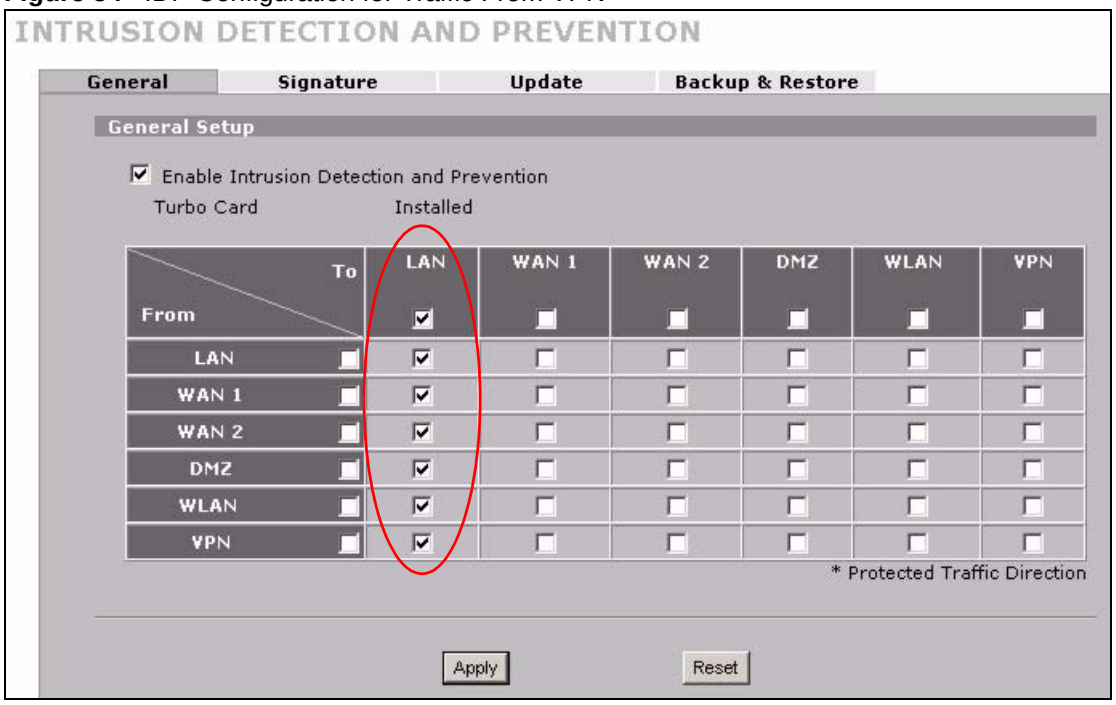
**Figure 53** IDP for From VPN Traffic




Here is how you would configure this example.

1. Click **SECURITY** > **IDP** > **General**.
2. Select the **To LAN** column's first check box (with the interface label) to select all of the **To LAN** packet directions.
3. Click **Apply**.

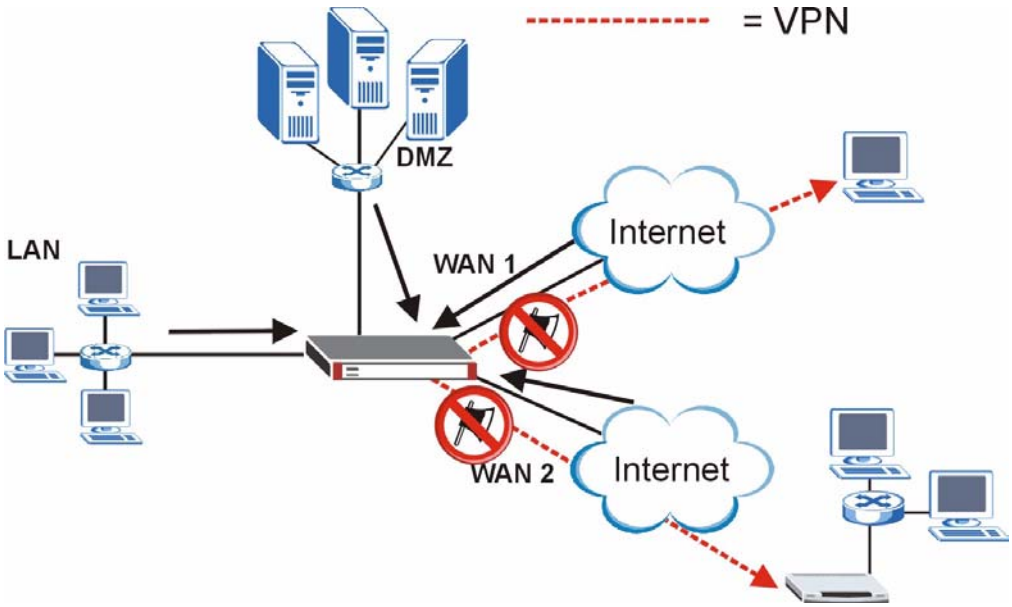
**Figure 54** IDP Configuration for Traffic From VPN




## 5.2.2 IDP for To VPN Traffic Example

You can also apply security settings to the **To VPN** packet direction to protect the remote networks from attacks, intrusions, viruses and spam originating from your own network. For example, you can use IDP to protect the remote networks from intrusions that might come in through your ZyWALL's VPN tunnels.

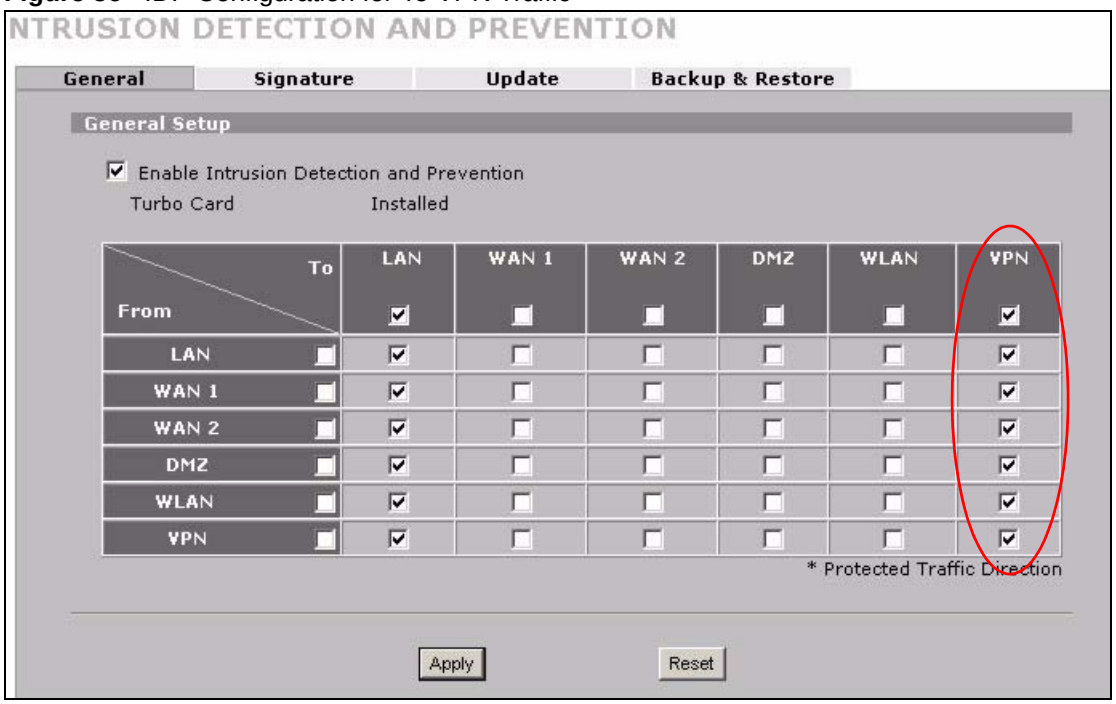
**Figure 55** IDP for To VPN Traffic




Here is how you would configure this example.

1. Click **SECURITY** > **IDP** > **General**.
2. Select the **To VPN** column's first check box (with the interface label) to select all of the **To VPN** packet directions.
3. Click **Apply**.

**Figure 56** IDP Configuration for To VPN Traffic

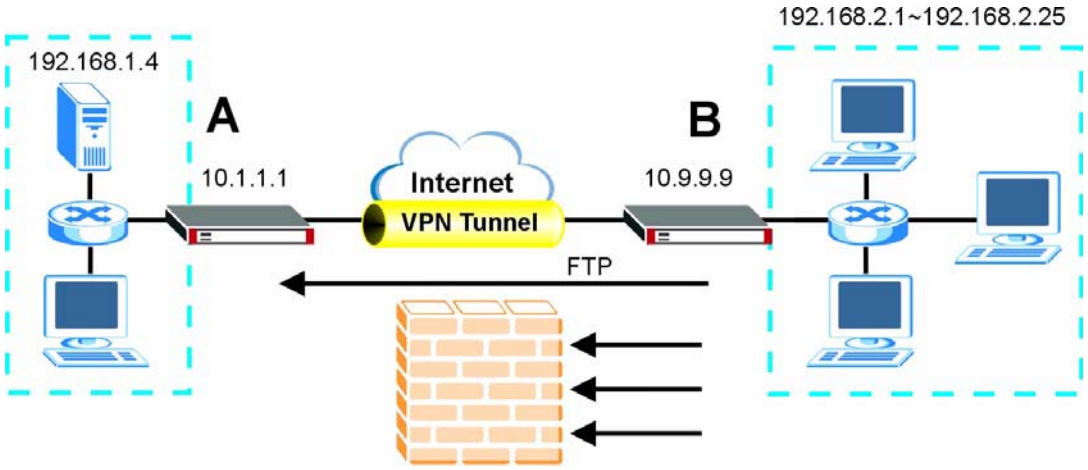



## 5.3 Firewall Rule for VPN Example

The firewall provides even more fine-tuned control for VPN tunnels. You can configure default and custom firewall rules for VPN packets.

Take the following example. You have a LAN FTP server with IP address 192.168.1.4 behind device A. You could configure a VPN rule to allow the network behind device B to access your LAN FTP server through a VPN tunnel. Now, if you don't want other services like chat or e-mail going to the FTP server, you can configure firewall rules that allow only FTP traffic to come from VPN tunnels to the FTP server. Furthermore, you can configure the firewall rule so that only the network behind device B can access the FTP server through a VPN tunnel (not other remote networks that have VPN tunnels with the ZyWALL).

**Figure 57** Firewall Rule for VPN

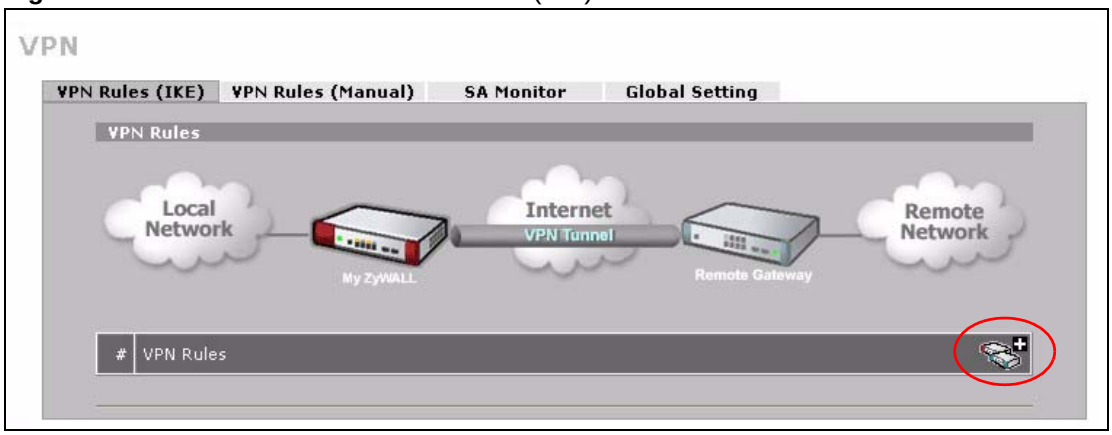



## 5.3.1 Configuring the VPN Rule

This section shows how to configure a VPN rule on device A to let the network behind B access the FTP server. You would also have to configure a corresponding rule on device B.

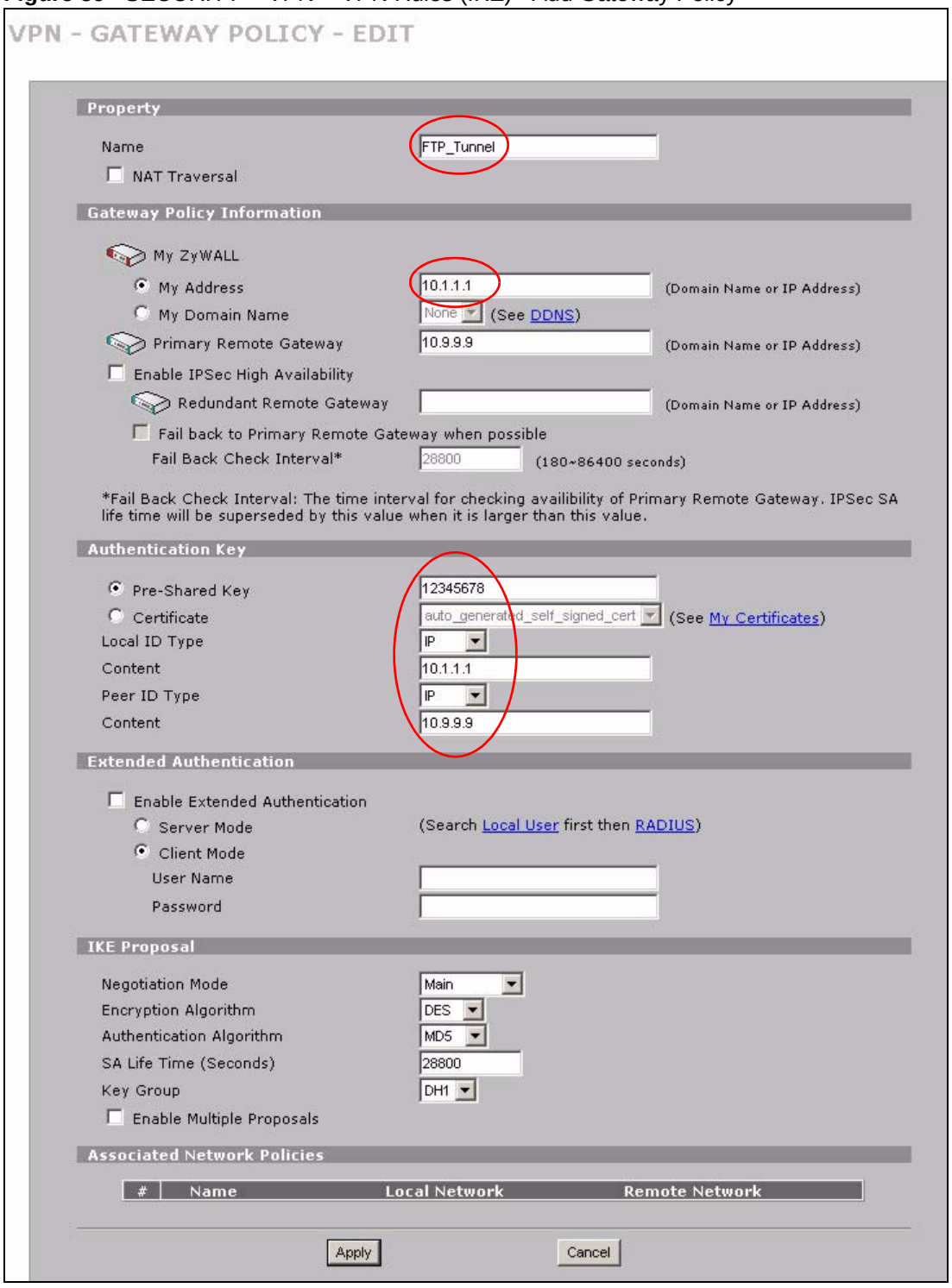
1 Click **Security** > **VPN** to open the following screen. Click the **Add Gateway Policy** icon.

**Figure 58** SECURITY > VPN > VPN Rules (IKE)



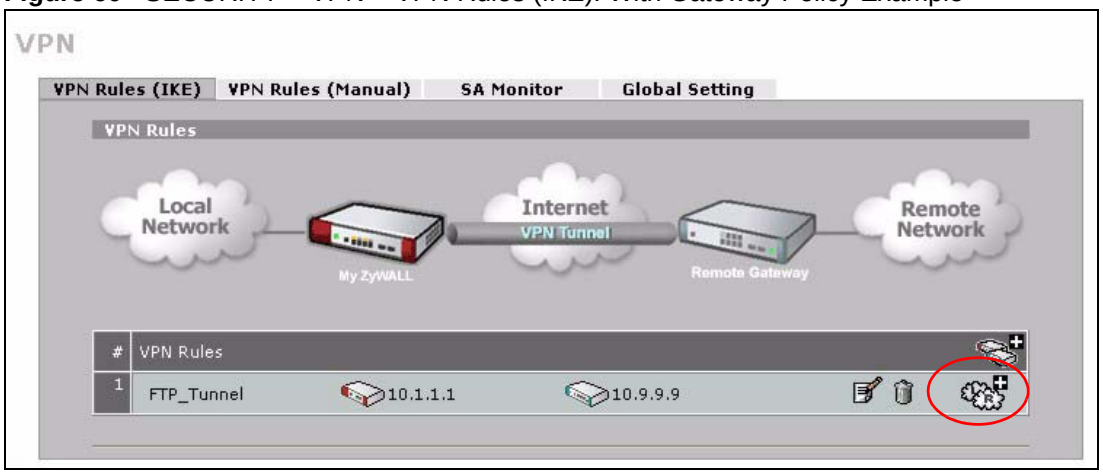

2 Use this screen to set up the connection between the routers. Configure the fields that are circled as follows and click **Apply**.

**Figure 59** SECURITY > VPN > VPN Rules (IKE)> Add Gateway Policy




**3** Click the **Add Network Policy** icon.

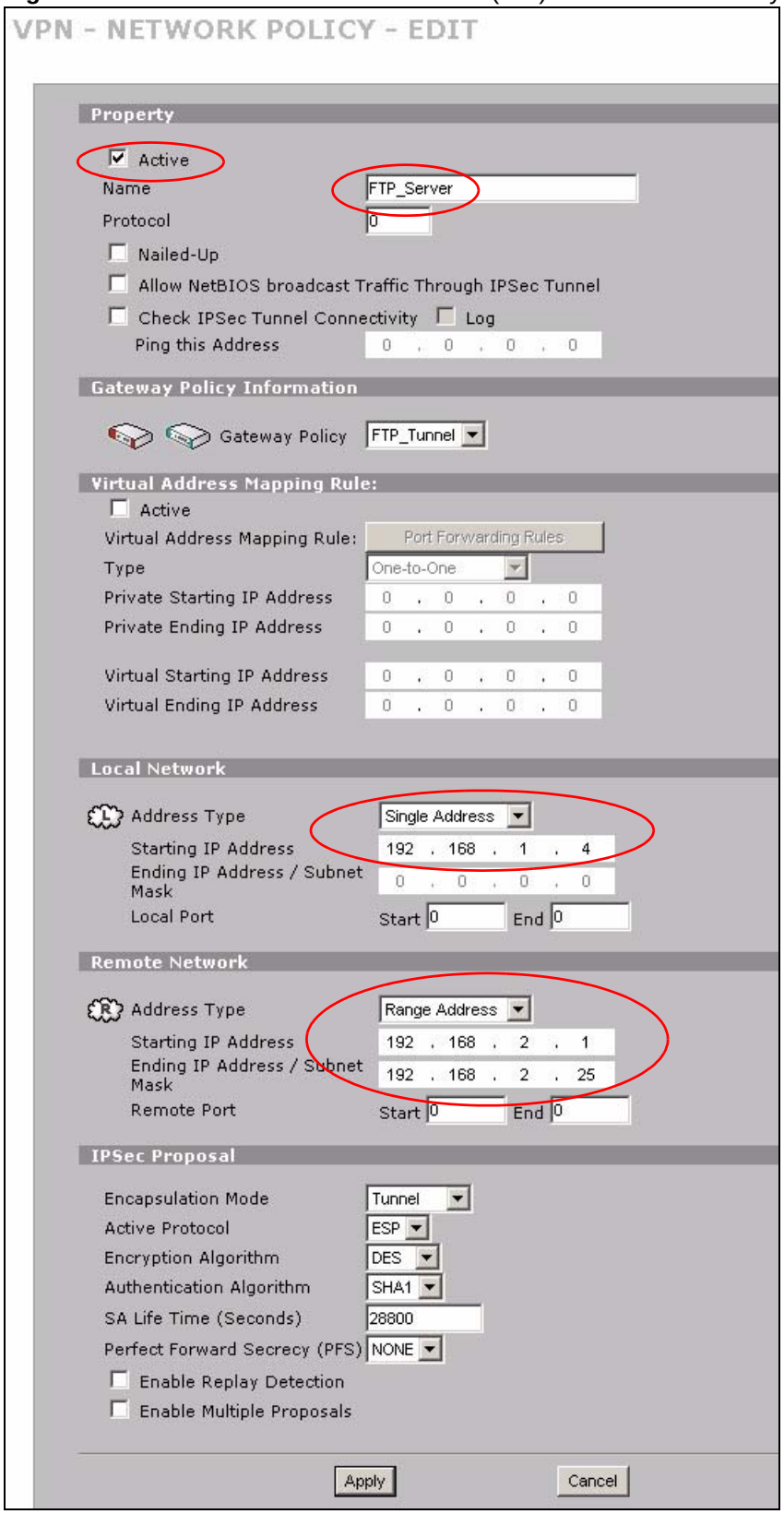
**Figure 60** SECURITY > VPN > VPN Rules (IKE): With Gateway Policy Example




4 Use this screen to specify which computers behind the routers can use the VPN tunnel. Configure the fields that are circled as follows and click **Apply**. You may notice that the example does not specify the port numbers. This is due to the following reasons.

- While FTP uses a control session on port 20, the port for the data session is not fixed. So this example uses the firewall's FTP application layer gateway (ALG) to handle this instead of specifying port numbers in this VPN network policy.
- The firewall provides better security because it operates at layer 4 and checks traffic sessions. The VPN network policy only operates at layer 3 and just checks IP addresses and port numbers.

**Figure 61** SECURITY > VPN > VPN Rules (IKE)> Add Network Policy



## 5.3.2 Configuring the Firewall Rules

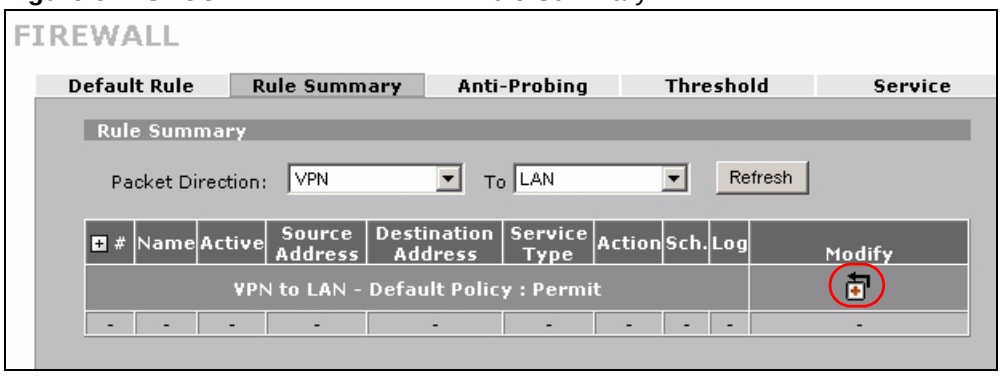
Suppose you have several VPN tunnels but you only want to allow device B's network to access the FTP server. You also only want FTP traffic to go to the FTP server, so you want to block all other traffic types (like chat, e-mail, web and so on). The following sections show how to configure firewall rules to enforce these restrictions.

### 5.3.2.1 Firewall Rule to Allow Access Example

Configure a firewall rule that allows FTP access from the VPN tunnel to the FTP server.

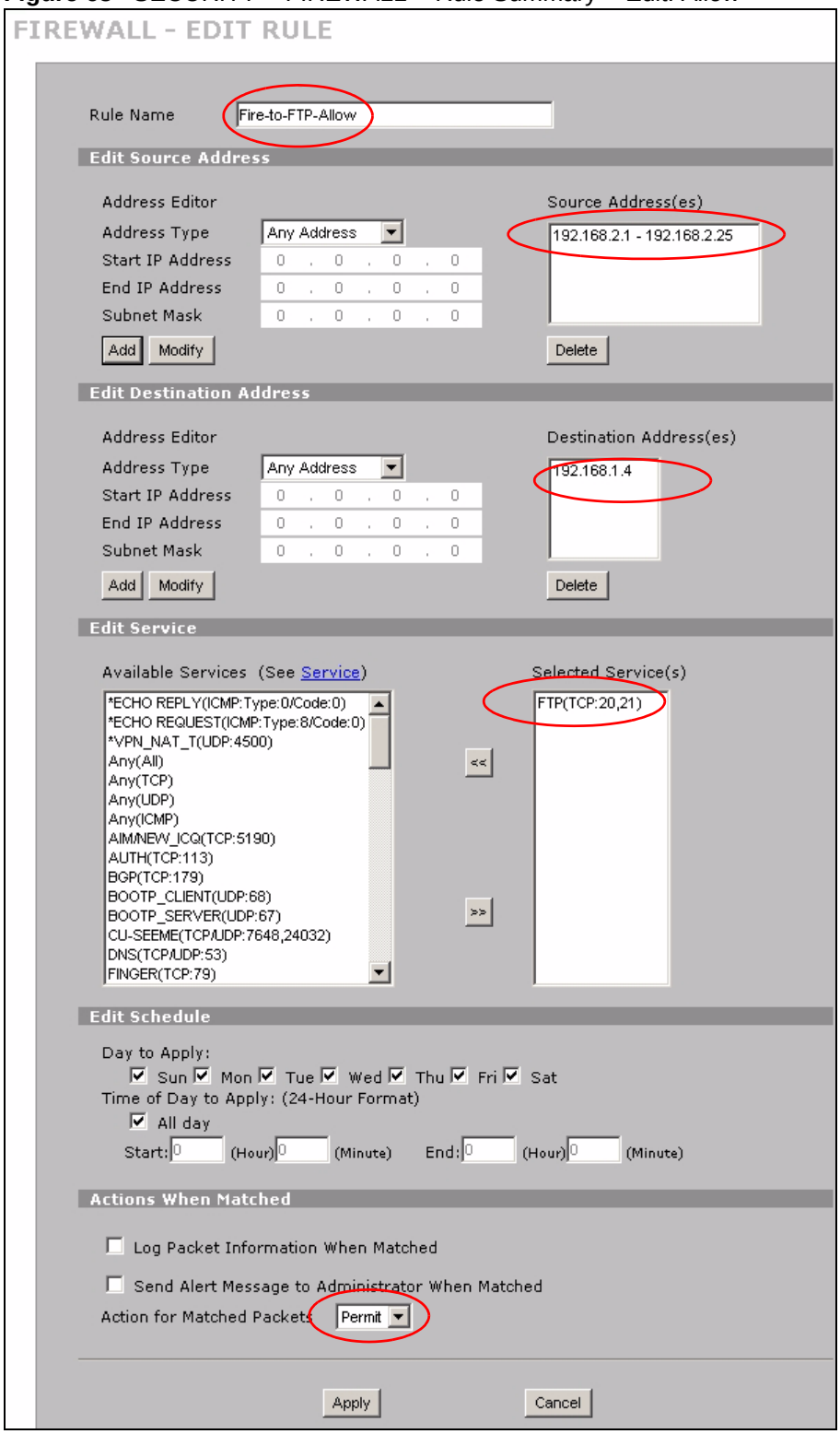
1. Click **Security** > **Firewall** > **Rule Summary**.
2. Select **VPN To LAN** as the packet direction and click **Refresh**.
3. Click the insert icon at the top of the **Modify** column.

**Figure 62** SECURITY > FIREWALL > Rule Summary



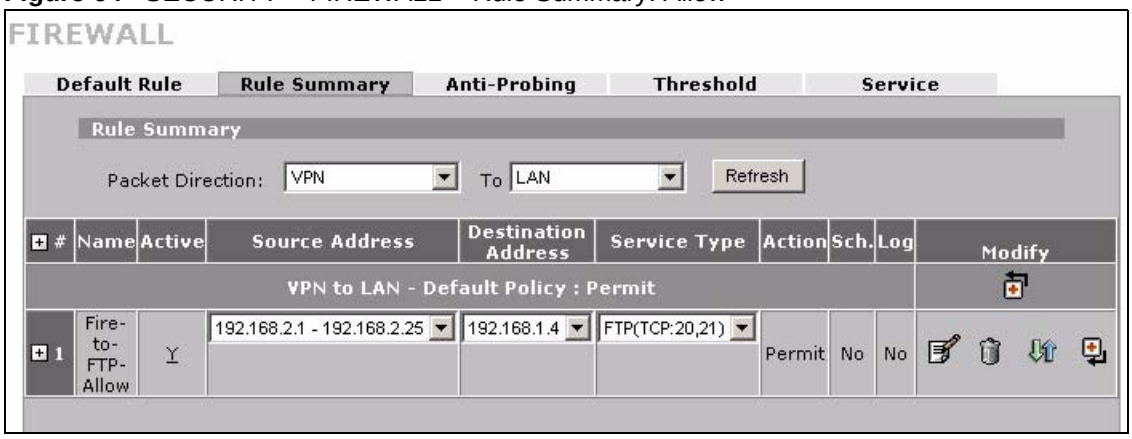

4. Configure the rule as follows and click **Apply**. The source addresses are the VPN rule's remote network and the destination address is the LAN FTP server.

**Figure 63** SECURITY > FIREWALL > Rule Summary > Edit: Allow




**5** The rule displays in the summary list of VPN to LAN firewall rules.

**Figure 64** SECURITY > FIREWALL > Rule Summary: Allow

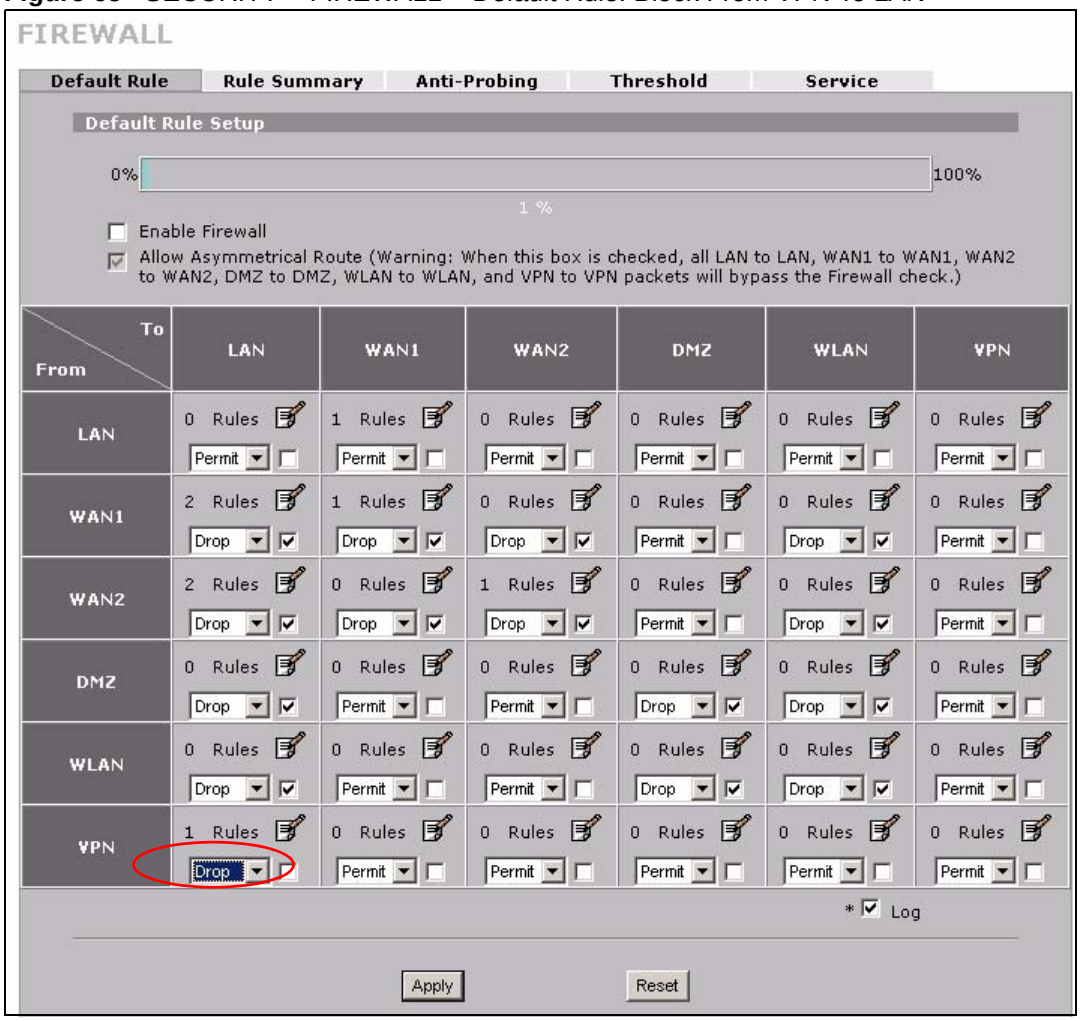



### 5.3.2.2 Default Firewall Rule to Block Other Access Example

Now you configure the default firewall rule to block all VPN to LAN traffic. This blocks any other types of access from VPN tunnels to the LAN FTP server. This means that you need to configure more firewall rules if you want to allow any other VPN tunnels to access the LAN.

1. Click **SECURITY** > **FIREWALL** > **Default Rule**.
2. Configure the screen as follows and click **Apply**.

**Figure 65** SECURITY > FIREWALL > Default Rule: Block From VPN To LAN




## 5.4 How to Set up a 3G WAN Connection

This section shows you how to configure and set up a 3G WAN connection on the ZyWALL. In this example, you have set up WAN 1 and want the ZyWALL to use both of the WAN interfaces (the physical WAN port and 3G card) for Internet access at the same time.

### 5.4.1 Inserting a 3G Card

To enable and use the 3G WAN connection, you need to insert a 3G card into the ZyWALL.

See Table 272 on page 773 for the 3G wireless cards you can use in the ZyWALL 5.

1 Make sure the ZyWALL is off before inserting or removing a card (to avoid damage).

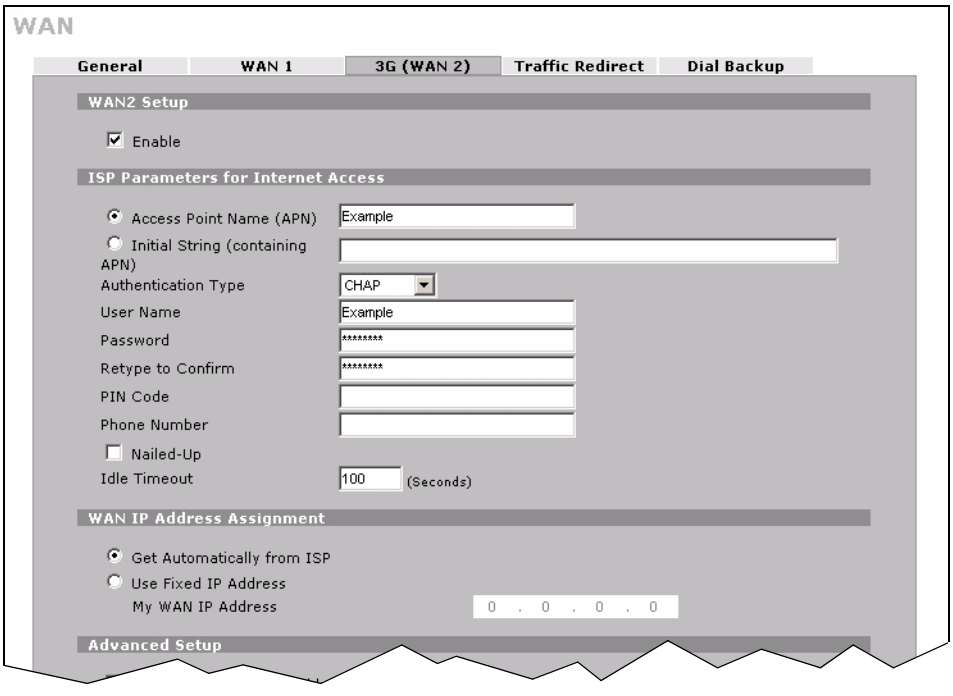
2 If you have a wireless card or Turbo card in the ZyWALL, remove it.
3 Slide the connector end of the 3G card into the slot.
4 Connect the ZyWALL's power.

## 5.4.2 Configuring 3G WAN Settings

You should already have an activated user account and network access information from the service provider.

1 Click **NETWORK > WAN > 3G (WAN 2)** on the ZyWALL.
2 Enable WAN 2.
3 The **Access Point Name (APN)** field displays with a GSM or HSDPA 3G card. Select **Access Point Name (APN)** and enter the APN ("Internet" for example) provided by your service provider.
4 If your service provider gave you a user name and password, select **CHAP/PAP** in the **Authentication Type** field and enter the user name and password in the fields below. If they were not given, set the authentication type to **None**.
5 The **Pin Code** field displays with a GSM or HSDPA 3G card. Enter the PIN code and phone number provided by your service provider. contact your service provider if they did not provide these.
6 If your service provider gave you an IP address for a 3G connection, select **Use Fixed IP Address** and enter it in the **My WAN IP Address** field. Otherwise, select **Get Automatically from ISP**.
7 Click **Apply**.

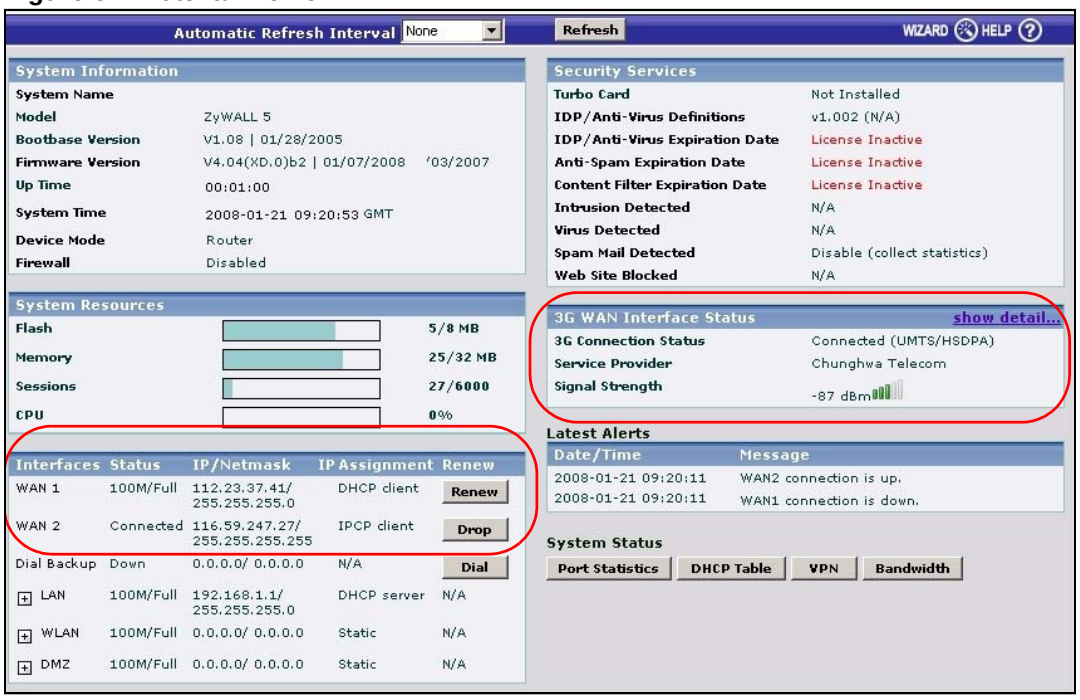
**Figure 66** Tutorial: NETWORK > WAN > 3G (WAN2)



### 5.4.3 Checking WAN Connections

1. Go to the web configurator's **Home** screen.
2. In the network status table, make sure the status for **WAN 1** and **WAN 2** is not **Down** and there is an IP address. If the WAN 2 connection is not up, make sure you have entered the correct information in the **NETWORK > WAN > 3G (WAN 2)** screen and the signal strength to the service provider's base station is not too low and can connect to a network.

**Figure 67** Tutorial: Home

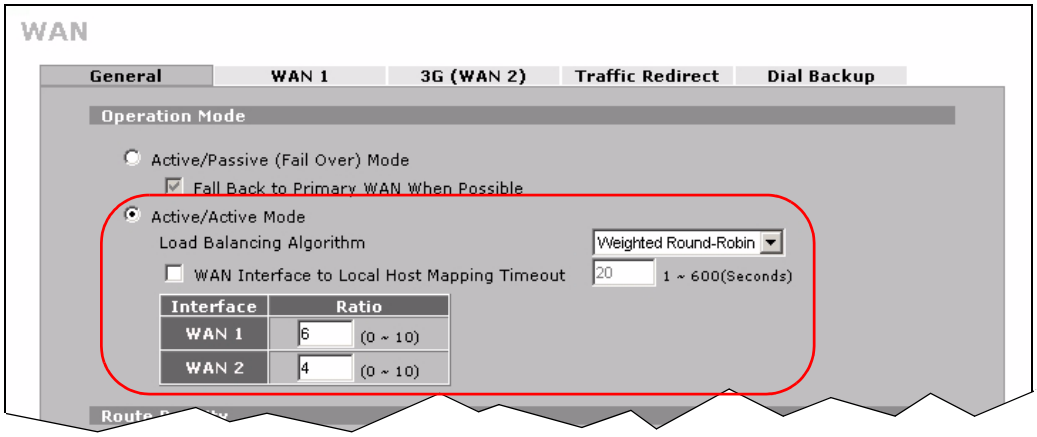



## 5.5 Configuring Load Balancing

In this example, you have set up WAN 1 and WAN 2 and you want the ZyWALL to use both of the WAN interfaces at the same time. You also balance the load between the two WAN interfaces using the weighted round-robin method.

1. Click **NETWORK > WAN > General**.
2. Set the WAN operation mode to active/active and select **Weighted Round-Robin** in the **Load Balancing Algorithm** field.
3. Enter 6 as the weight for WAN 1 and 4 for WAN 2.
4. Click **Apply**.

**Figure 68** Tutorial: NETWORK > WAN > General




## 5.6 Configuring Content Filtering

You can use the ZyWALL's content filtering policies to apply specific content filtering settings to specific users. You can even filter certain things at certain times. For example, you decide to set the default policy to block access to several categories of web content including things like pornography, hacking, nudity, and arts and entertainment, and so on. Now, suppose you want to allow an employee named Bob to access arts and entertainment web pages during lunch. You can create another policy for traffic from Bob's computer.

The ordering of your policies is very important as the ZyWALL applies policies in the order they are listed.

The ZyWALL applies the content filter policies based on the source address and the schedule. So for this example, when the ZyWALL receives a request from the LAN for a web page, it checks the request against the first policy. If the traffic matches (that is if it is from Bob's computer and the time is between 12:00 and 13:00), the ZyWALL applies the first policy. Any traffic that does not match the first policy will match the default policy and the ZyWALL treats it based on the default policy.

### 5.6.1 Enable Content Filtering

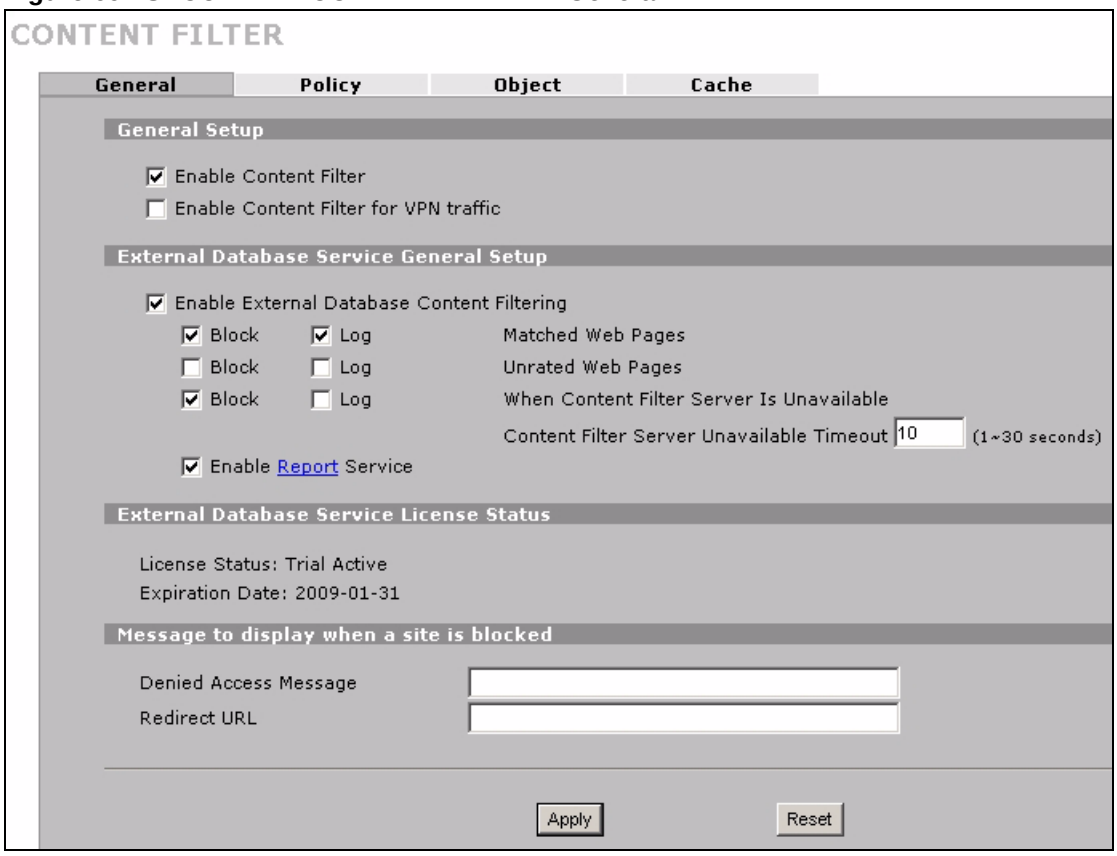
Do the following to turn on content filtering and have the ZyWALL use the external content filtering service.

You must register for external content filtering before you can use it.

Use the **REGISTRATION** screens (see Chapter 6 on page 141) to create a myZyXEL.com account, register your device and activate the external content filtering service.

1. Click **SECURITY** > **CONTENT FILTER**.
2. Enable the content filter and external database content filtering.
3. Click **Apply**.

**Figure 69** SECURITY > CONTENT FILTER > General

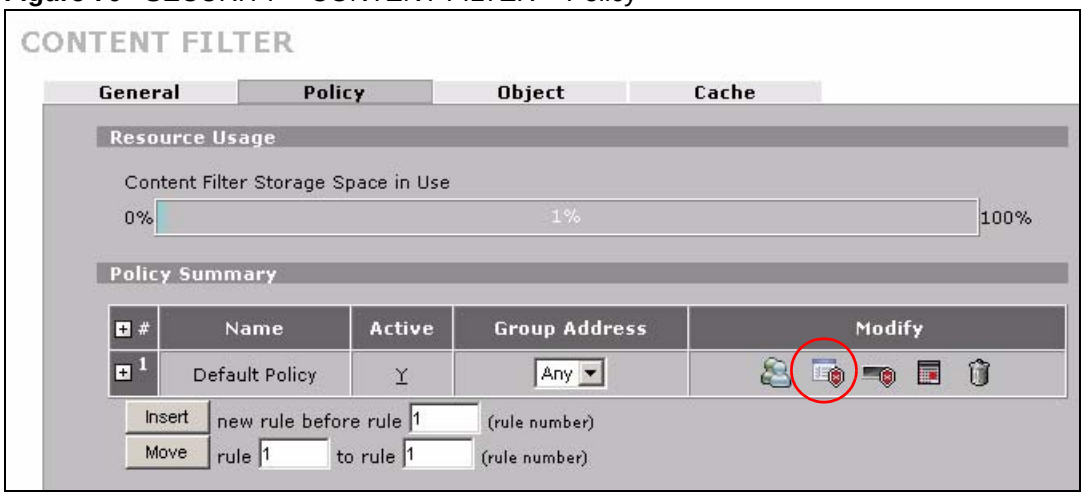



## 5.6.2 Block Categories of Web Content

Here is how to block access to web pages by category of content.

1. Click **SECURITY** > **CONTENT FILTER** > **Policy** and then the external database icon next to the default policy.

**Figure 70** SECURITY > CONTENT FILTER > Policy

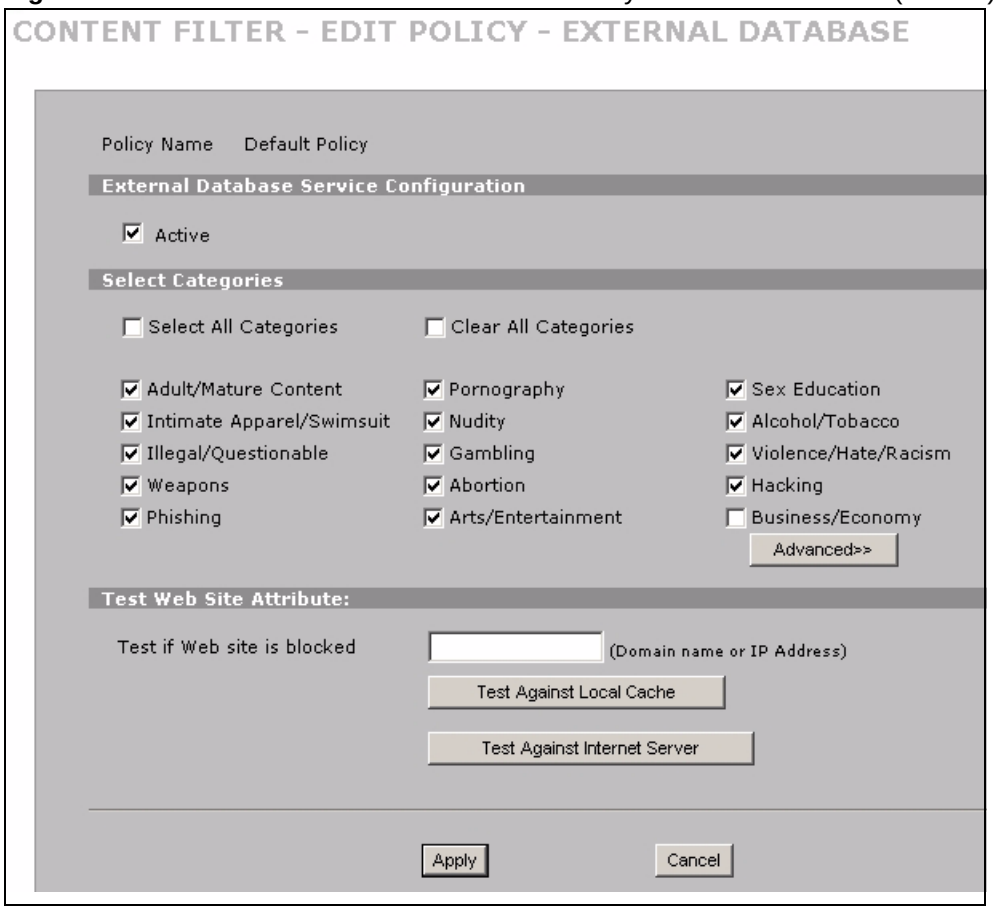



2 Select **Active**.

3 Select the categories to block.

4 Click **Apply**.

**Figure 71** SECURITY > CONTENT FILTER > Policy > External Database (Default)

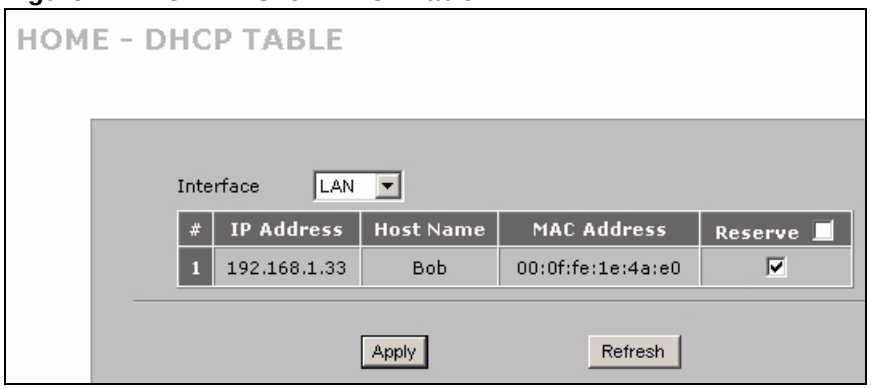


## 5.6.3 Assign Bob's Computer a Specific IP Address

You will configure a content filtering policy for traffic from Bob's computer's IP address. Do the following to have the ZyWALL always give Bob's computer the same IP address (192.168.1.33 in this example).

1. Click **HOME** > **Show DHCP Table**.
2. Find the entry for Bob's computer and select the **Reserve** check box as shown next.
3. Click **Apply**.

**Figure 72** HOME > Show DHCP Table

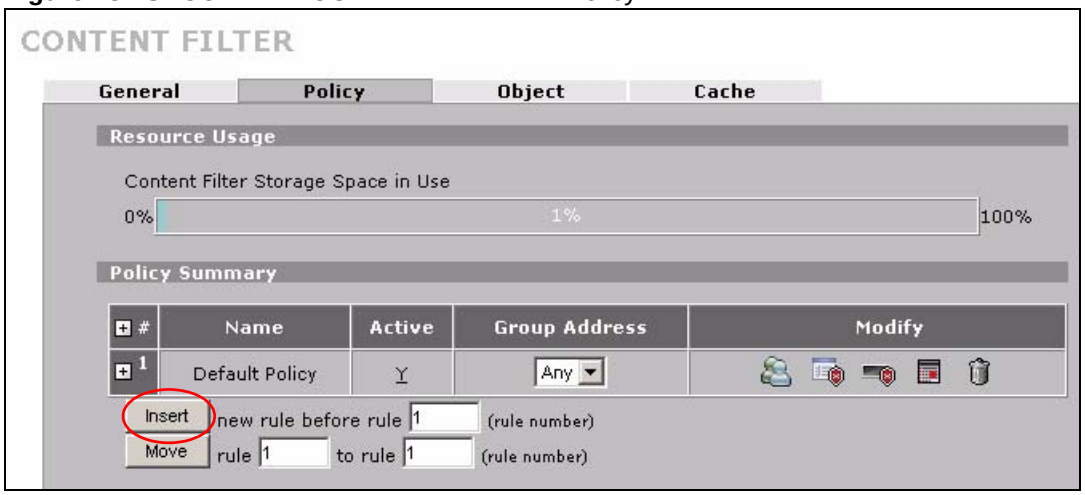



## 5.6.4 Create a Content Filter Policy for Bob

Do the following to create a content filtering policy for traffic from Bob's computer.

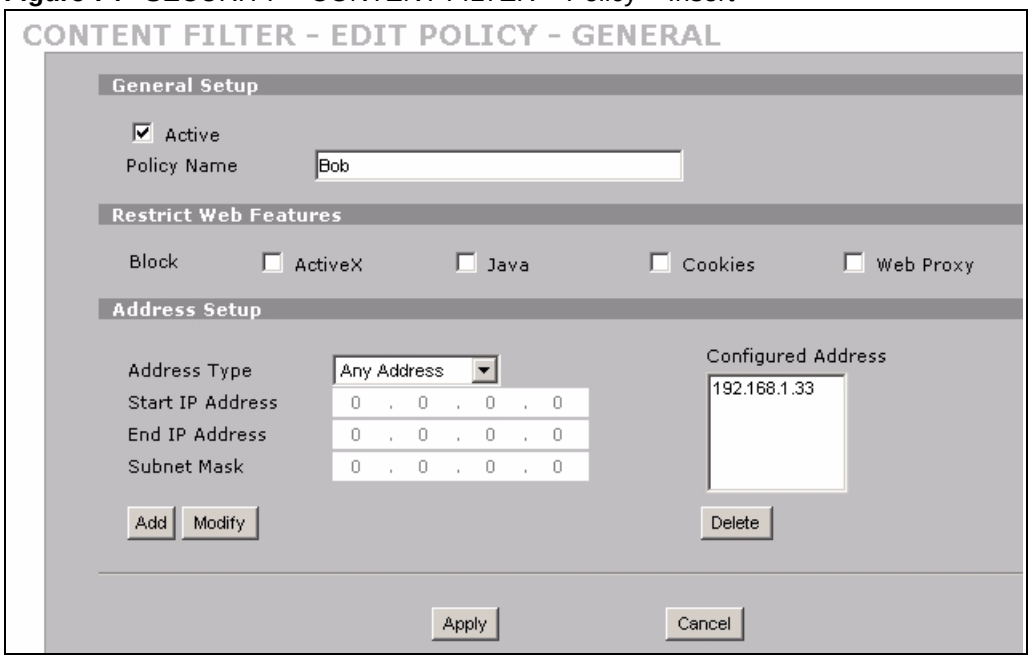
1. Click **SECURITY** > **CONTENT FILTER** > **Policy** and then the **Insert** button. The ZyWALL applies the content filter policies in order, so make sure you add the new policy before the default policy.

**Figure 73** SECURITY > CONTENT FILTER > Policy




2. Select **Active**.
3. Give the policy a name.
4. Configure a single address of 192.168.1.33.
5. Click **Apply**.

**Figure 74** SECURITY > CONTENT FILTER > Policy > Insert

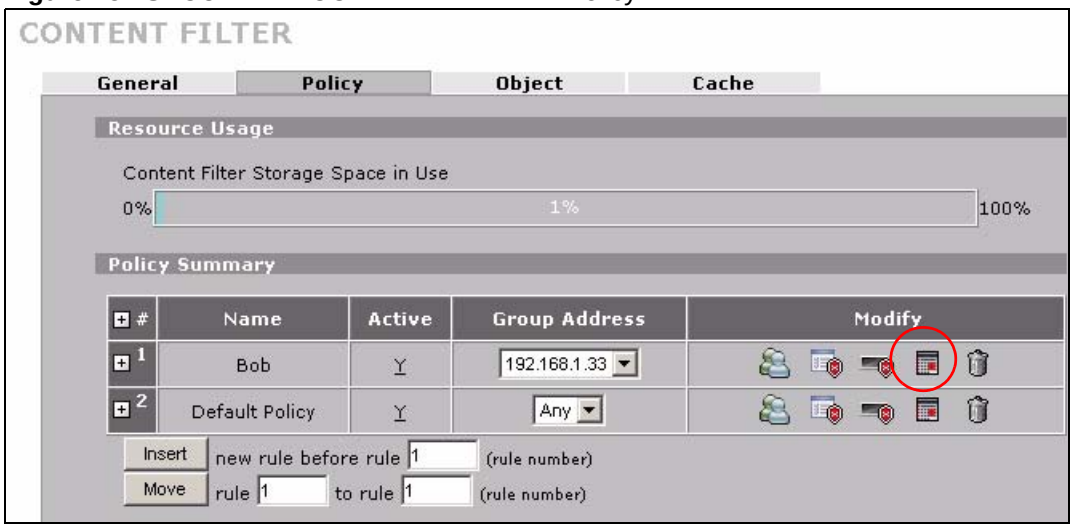



## 5.6.5 Set the Content Filter Schedule

You want to let Bob access arts and entertainment web pages, but only during lunch. So you configure a schedule to only apply the Bob policy from 12:00 to 13:00. For the rest of the time, the ZyWALL applies the default content filter policy (which blocks access to arts and entertainment web pages).

1 Click **SECURITY** > **CONTENT FILTER** > **Policy** and then the Bob policy's schedule icon.

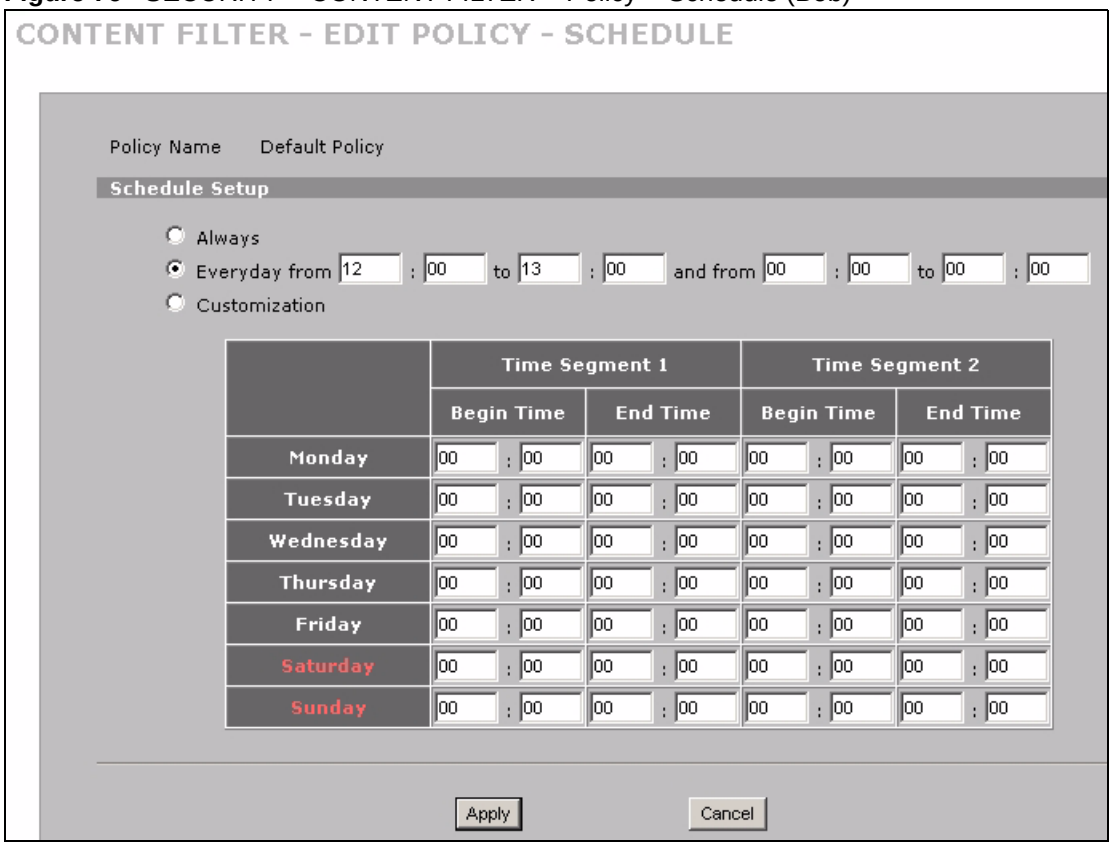
**Figure 75** SECURITY > CONTENT FILTER > Policy




2 Select **Everyday** and enter 12:00 to 13:00.

3 Click **Apply**.

**Figure 76** SECURITY > CONTENT FILTER > Policy > Schedule (Bob)

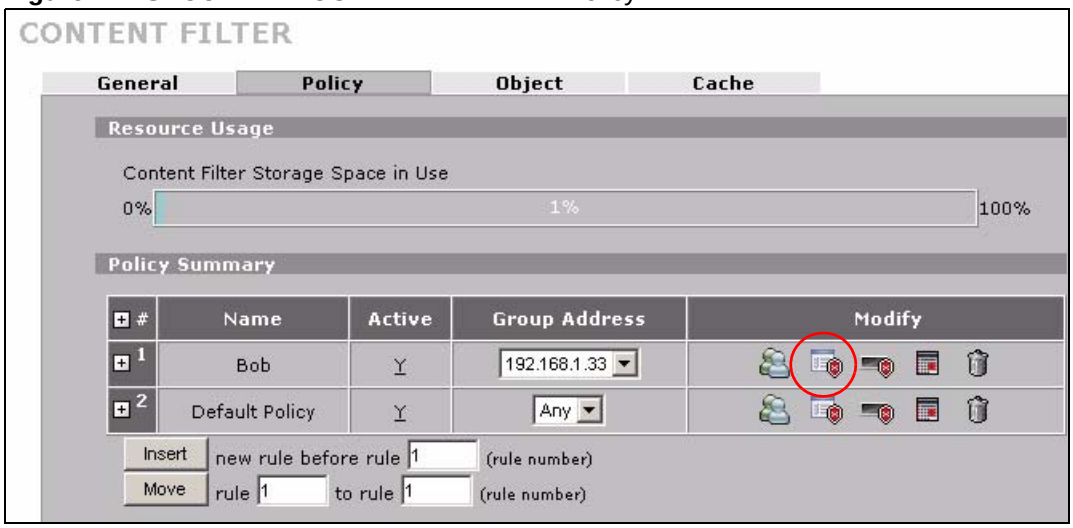



## 5.6.6 Block Categories of Web Content for Bob

Now you select the categories of web pages to block Bob from accessing.

1 Click **SECURITY** > **CONTENT FILTER** > **Policy** and then the Bob policy's external database icon.

**Figure 77** SECURITY > CONTENT FILTER > Policy

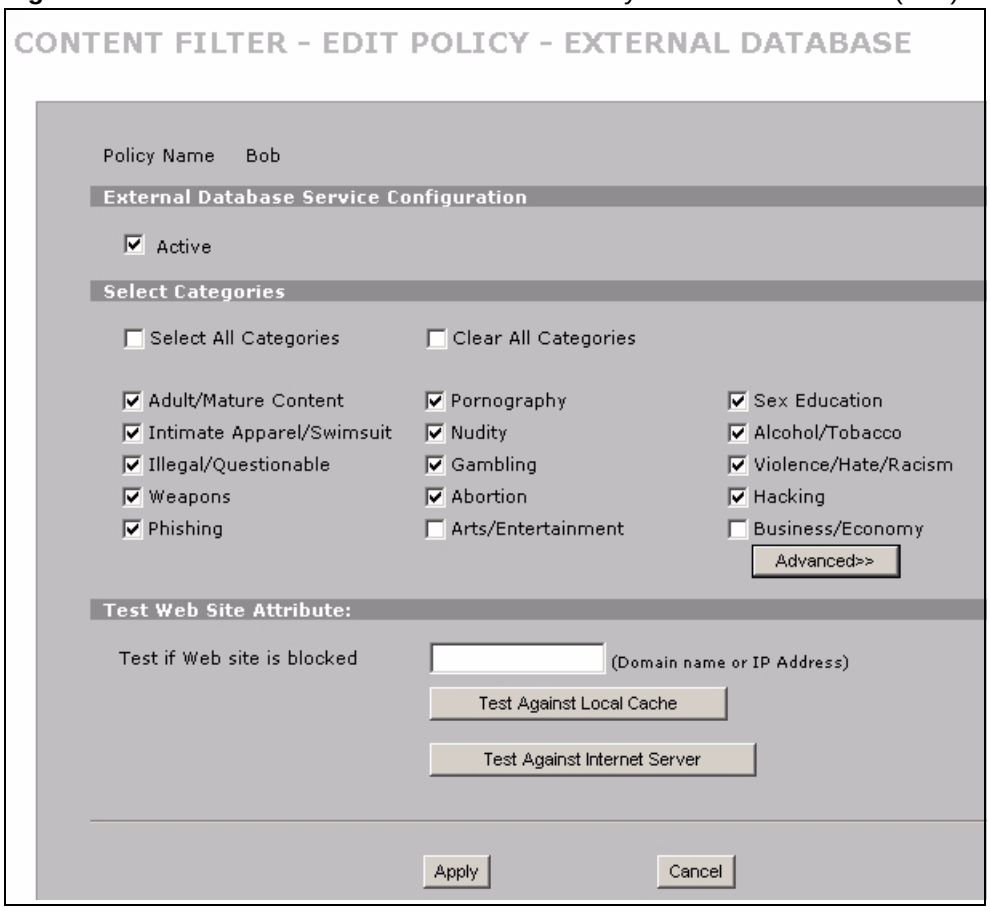



2 Select **Active**.

3 Select the categories to block. This is very similar to Section 5.6.2 on page 134, except you do not select the arts and entertainment category.

4 Click **Apply**.

**Figure 78** SECURITY > CONTENT FILTER > Policy > External Database (Bob)



# 6

# Registration Screens

## 6.1 Overview

The registration screens let you activate and update your account with myZyXEL.com, allowing you access to subscription services required for the ZyWALL's security features.

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

- Use the **Registration** screen (Section 6.2 on page 142) to register with myZyXEL.com and activate a service(s), or view your registration status.
- Use the **Service** screen (Section 6.3 on page 144) to view registration details and enter your iCard's PIN number (license key).

### 6.1.2 What You Need to Know About Registration

#### myZyXEL.com

myZyXEL.com is ZyXEL's online services center where you can register your ZyWALL and manage subscription services available for the ZyWALL.

#### Subscription Services Available on the ZyWALL

At the time of writing, the ZyWALL can use content filtering, anti-spam, anti-virus and IDP (Intrusion Detection and Prevention) subscription services.

#### Content Filtering

Content filtering 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.

#### Anti-spam

Anti-spam identifies and marks or discards spam e-mail. An anti-spam subscription lets the ZyWALL check e-mail with an external anti-spam server.

#### Anti-virus

Anti-virus allows the ZyWALL to scan packets for computer viruses and deletes the infected packets.

### IDP

IDP allows the ZyWALL to detect malicious or suspicious packets and respond immediately.

### Signatures

This is the pattern of code used by a particular virus. The ZyWALL compares files with a database of signatures to identify possible viruses. The ID&P and anti-virus features use the same signature files on the ZyWALL to detect and scan for viruses.

### Signature Updates

After the service is activated, the ZyWALL downloads the up-to-date signature files from the update server (http://myupdate.zywall.zyxel.com). You will get automatic e-mail notification of new signature releases from mySecurityZone after you activate the IDP/Anti-virus service. You can also check for new signature or virus updates at http://mysecurity.zyxel.com.

To update the signature file or use a subscription service, you have to register and activate the corresponding service at myZyXEL.com (through the ZyWALL).

### Finding Out More

See the chapters about content filtering, anti-virus, anti-spam and IDP for more information.

## 6.2 The Registration Screen

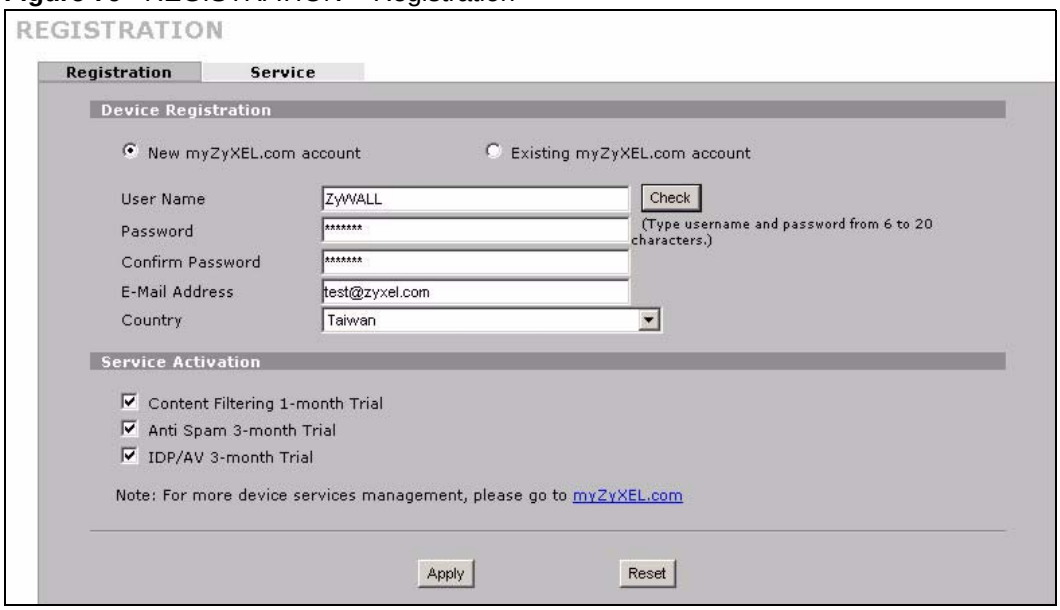
Click **REGISTRATION** in the navigation panel to open the screen as shown next. Use this screen to register your ZyWALL with myZyXEL.com and activate a service, such as content filtering, anti-spam or anti-virus.

Instead of using this screen you can 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.

Please note the following.

- You need to create an account before you can register your device and activate the services at myZyXEL.com.
- To activate a service on a ZyWALL, you need to access myZyXEL.com via that ZyWALL.
- Make sure you have installed the ZyWALL Turbo extension card before you activate the IDP and anti-virus subscription services. Turn the ZyWALL off before you install or remove the ZyWALL Turbo Card. See the ZyWALL Turbo Card guide for more information.

**Figure 79** REGISTRATION > Registration




The following table describes the labels in this screen.

**Table 25** REGISTRATION > Registration

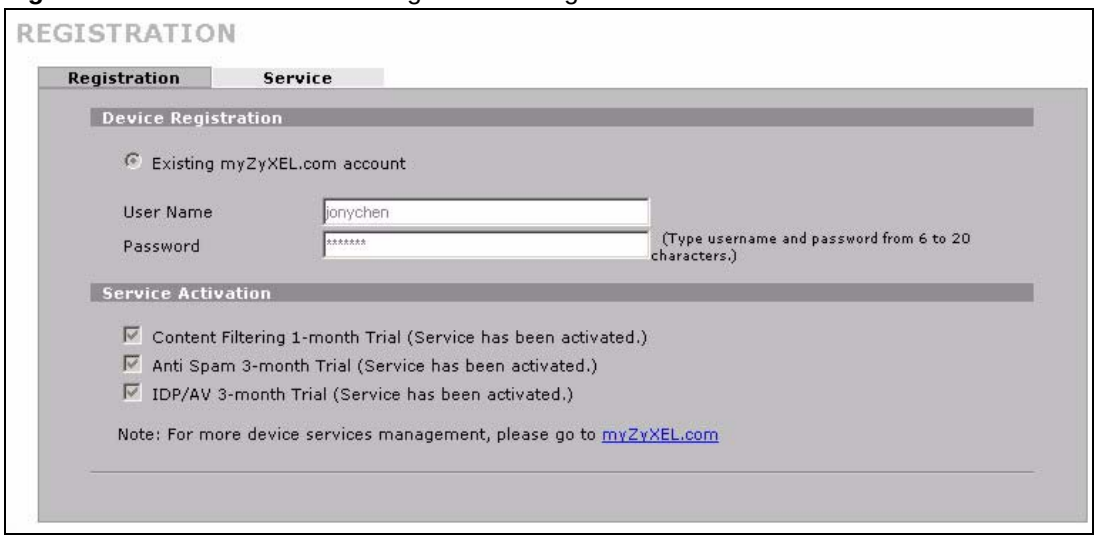
| LABEL | DESCRIPTION |
|---|---|
| Device Registration | If you select **Existing myZyXEL.com account**, only the **User Name** and **Password** fields are available. |
| New myZyXEL.com account | If you haven't created an account at myZyXEL.com, select this option and configure the following fields 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. |
| User Name | 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 | Select your country from the drop-down box list. |
| Service Activation | You can try 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. |
| Content Filtering 1-month Trial | Select the check box to activate a trial. The trial period starts the day you activate the trial. |
| Anti Spam 3-month Trial | Select the check box to activate a trial. The trial period starts the day you activate the trial. |
| IDP/AV 3-month Trial | Select the check box to activate a trial. The trial period starts the day you activate the trial. |

**Table 25** REGISTRATION > Registration

| LABEL | DESCRIPTION |
|---|---|
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

If the ZyWALL is registered already, this screen is read-only and indicates whether trial services are activated. Use the **Service** screen to update your service subscription status.

**Figure 80** REGISTRATION > Registration: Registered Device

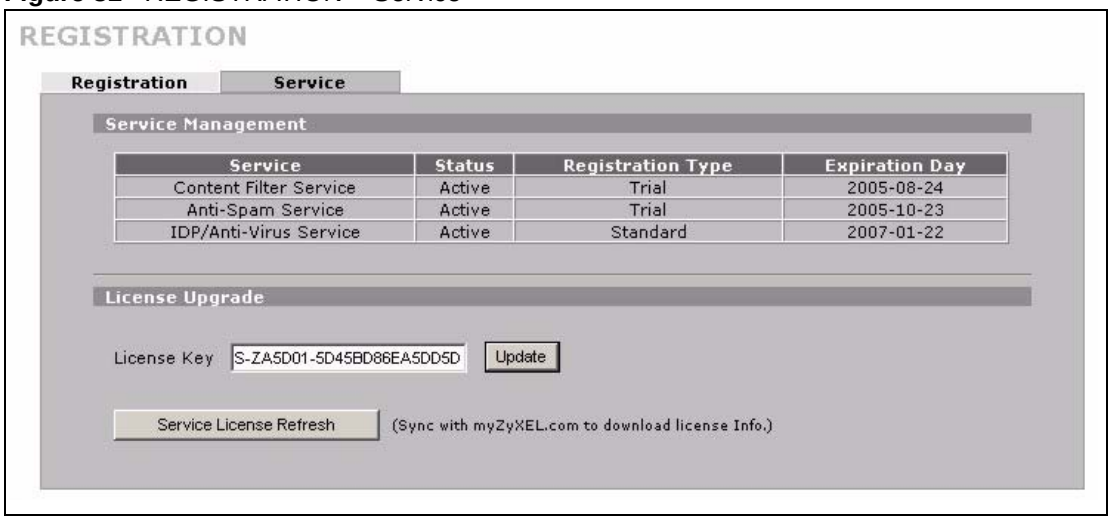



## 6.3 The Service Screen

After you activate a trial, you can also use the **Service** screen to register and enter your iCard's PIN number (license key). Click **REGISTRATION** > **Service** to open the screen as shown next.

If you restore the ZyWALL to the default configuration file or upload a different configuration file after you register, click the **Service License Refresh** button to update license information.

**Figure 81** REGISTRATION > Service




The following table describes the labels in this screen.

**Table 26** REGISTRATION > Service

| LABEL | DESCRIPTION |
|---|---|
| Service Management | |
| Service | This field displays the service name available on the ZyWALL. |
| Status | This field displays whether a service is activated (**Active**) or not (**Inactive**). |
| Registration Type | This field displays whether you applied for a trial application (**Trial**) or registered a service with your iCard's PIN number (**Standard**). |
| Expiration Day | This field displays the date your service expires. |
| License Upgrade | |
| License Key | Enter your iCard's PIN number and click **Update** to activate or extend a standard service subscription.<br>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 license key, registration status and expiration day). |

# PART II
# Network

# 7

# LAN Screens

## 7.1 Overview

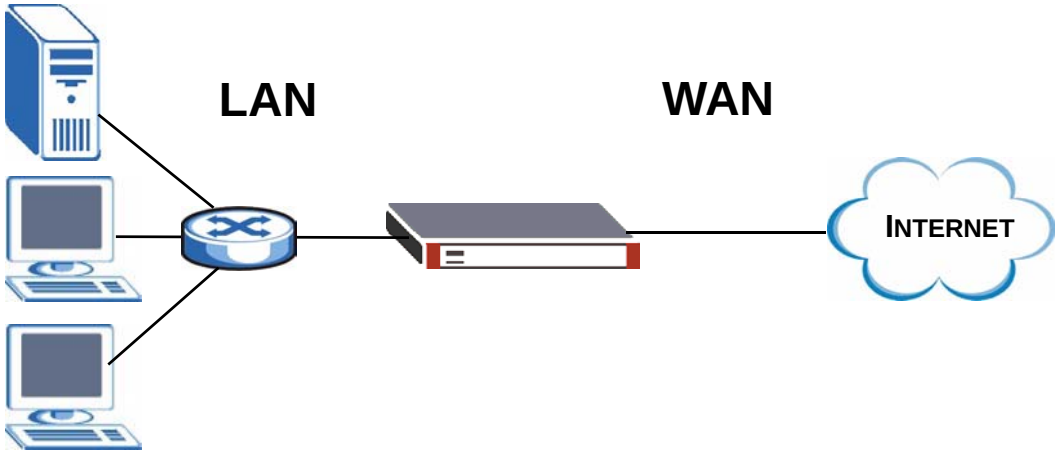
A network is a shared communication system to which many computers are attached.

The Local Area Network (LAN) includes the computers and networking devices in your home or office that you connect to the ZyWALL's LAN ports.

The Wide Area Network (WAN) is another network (most likely the Internet) that you connect to the ZyWALL's WAN port. See Chapter 9 on page 169 for how to use the WAN screens to set up your WAN connection.

The LAN and the WAN are two separate networks. The ZyWALL controls the traffic that goes between them. The following graphic gives an example.

**Figure 82** LAN and WAN




This chapter is only applicable when the ZyWALL is in router mode.

### 7.1.1 What You Can Do in The LAN Screens

- Use the **LAN** screen (Section 7.2 on page 152) to configure TCP/IP, DHCP, IP/MAC binding and NetBIOS settings on the LAN.
- Use the **Static DHCP** screen (Section 7.3 on page 155) to configure the IP addresses assigned to devices in the LAN by DHCP.

- Use the **IP Alias** screen (Section 7.4 on page 156) to configure IP alias settings on the ZyWALL's LAN ports.
- Use the **Port Roles** screen (Section 7.5 on page 158) to configure LAN ports on the ZyWALL. The **Port Roles** screen is available on the ZyWALL 5 and ZyWALL 35.

## 7.1.2 What You Need to Know About LAN

### IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number.

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the Network Address Translation (NAT) feature of the ZyWALL. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. If you select 192.168.1.0 as the network number; it covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your ZyWALL, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your ZyWALL will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the ZyWALL unless you are instructed to do otherwise.

### Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet, for example, only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, *Address Allocation for Private Internets* and RFC 1466, *Guidelines for Management of IP Address Space.*

### MAC Address

Every Ethernet 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.

### DHCP

The ZyWALL can use DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) to automatically assign IP addresses subnet masks, gateways, and some network information like the IP addresses of DNS servers to the computers on your LAN. You can alternatively have the ZyWALL relay DHCP information from another DHCP server. If you disable the ZyWALL's DHCP service, you must have another DHCP server on your LAN, or else the computers must be manually configured.

### IP Pool Setup

The ZyWALL is pre-configured with a pool of IP addresses for the computers on your LAN. See Table 269 on page 770 for the default IP pool range. Do not assign your LAN computers static IP addresses that are in the DHCP pool.

### RIP Setup

RIP (Routing Information Protocol, RFC 1058 and RFC 1389) allows a router to exchange routing information with other routers. **RIP Direction** controls the sending and receiving of RIP packets. When set to **Both** or **Out Only**, the ZyWALL will broadcast its routing table periodically. When set to **Both** or **In Only**, it will incorporate the RIP information that it receives; when set to **None**, it will not send any RIP packets and will ignore any RIP packets received.

**RIP Version** controls the format and the broadcasting method of the RIP packets that the ZyWALL sends (it recognizes both formats when receiving). **RIP-1** is universally supported; but **RIP-2** carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology.

Both **RIP-2B** and **RIP-2M** send routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also.

By default, **RIP Direction** is set to **Both** and **RIP Version** to **RIP-1**.

### Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

IGMP (Internet Group Management Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

The ZyWALL supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**). At start up, the ZyWALL queries all directly connected networks to gather group membership. After that, the ZyWALL periodically updates this information. IP multicasting can be enabled/disabled on the ZyWALL LAN and/or WAN interfaces in the web configurator (**LAN**; **WAN**). Select **None** to disable IP multicasting on these interfaces.

### 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.

### IP Alias

IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The LAN, DMZ or WLAN may all be partitioned in this way.

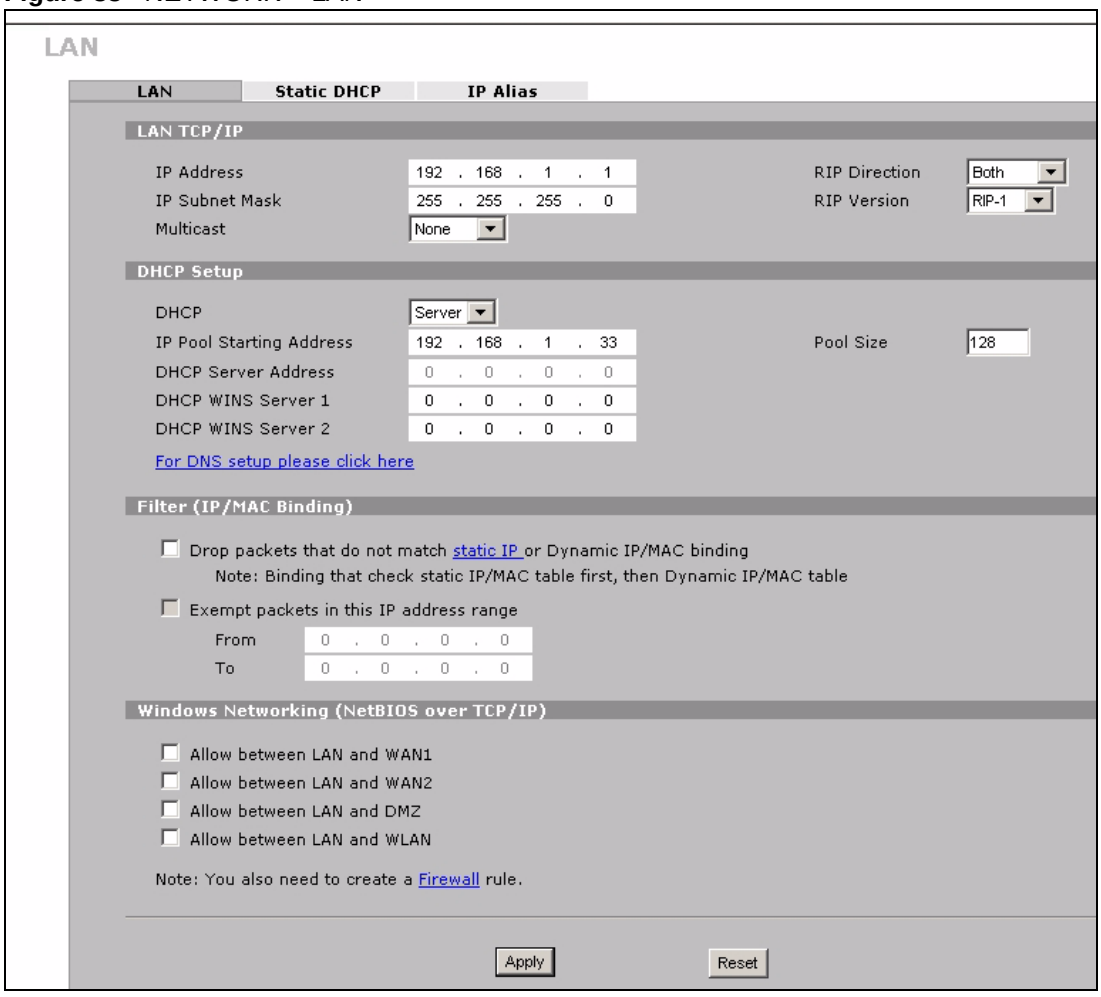
### Port Roles

Port Roles allows you to set ports as part of the LAN, DMZ and/or WLAN interface.

## 7.2 The LAN Screen

Click **NETWORK** > **LAN** to open the **LAN** screen. Use this screen to configure the ZyWALL's IP address and other LAN TCP/IP settings as well as the built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

**Figure 83** NETWORK > LAN




The following table describes the labels in this screen.

**Table 27** NETWORK > LAN

| LABEL | DESCRIPTION |
|---|---|
| LAN TCP/IP | |
| IP Address | Type the IP address of your ZyWALL in dotted decimal notation. 192.168.1.1 is the factory default. Alternatively, click the right mouse button to copy and/or paste the IP address. |
| IP Subnet Mask | The subnet mask specifies the network number portion of an IP address. Your ZyWALL automatically calculates the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyWALL. |
| RIP Direction | RIP (Routing Information Protocol, RFC1058 and RFC 1389) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Select the RIP direction from **Both**/**In Only**/**Out Only**/**None**. When set to **Both** or **Out Only**, the ZyWALL will broadcast its routing table periodically. When set to **Both** or **In Only**, it will incorporate the RIP information that it receives; when set to **None**, it will not send any RIP packets and will ignore any RIP packets received. **Both** is the default. |

**Table 27** NETWORK > LAN (continued)

| LABEL | DESCRIPTION |
|---|---|
| RIP Version | The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyWALL sends (it recognizes both formats when receiving). **RIP-1** is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to **Both** and the Version set to **RIP-1**. |
| Multicast | Select **IGMP V-1** or **IGMP V-2** or **None**. IGMP (Internet Group Management Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see *sections 4 and 5 of RFC 2236*. |
| DHCP Setup | |
| DHCP | DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (workstations) to obtain TCP/IP configuration at startup from a server. Unless you are instructed by your ISP, leave this field set to **Server**. When configured as a server, the ZyWALL provides TCP/IP configuration for the clients. When set as a server, fill in the **IP Pool Starting Address** and **Pool Size** fields.<br>Select **Relay** to have the ZyWALL forward DHCP requests to another DHCP server. When set to **Relay**, fill in the **DHCP Server Address** field.<br>Select **None** to stop the ZyWALL from acting as a DHCP server. When you select **None**, you must have another DHCP server on your LAN, or else the computers must be manually configured. |
| IP Pool Starting Address | This field specifies the first of the contiguous addresses in the IP address pool. |
| Pool Size | This field specifies the size, or count of the IP address pool. |
| DHCP Server Address | Type the IP address of the DHCP server to which you want the ZyWALL to relay DHCP requests. Use dotted decimal notation. Alternatively, click the right mouse button to copy and/or paste the IP address. |
| DHCP WINS Server 1, 2 | 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. |
| Filter (IP/MAC Binding | |
| Drop packets that do not match static IP or Dynamic IP/MAC binding | Select this to allow traffic only from devices on the LAN which have received an IP address from the ZyWALL. This is done by allowing traffic only from devices on the LAN with specific combinations of IP and MAC addresses. These IP addresses are dynamically assigned by the ZyWALL or manually set using static DHCP.<br>See the **Static DHCP** screen for a list of static IP/MAC address combinations. See the **DHCP Table** available from the **Home** screen for a list of dynamically assigned IP (and their corresponding MAC addresses). |
| Exempt packets in this IP address range. | Set the ZyWALL to allow packets from the LAN with source IP addresses within a specified range. This allows packets even when their IP and MAC addresses do not match those specified in the **Static DHCP** screen or **DHCP Table**.<br>Type this range of IP addresses in the **From** and **To** fields. |

**Table 27** NETWORK > LAN (continued)

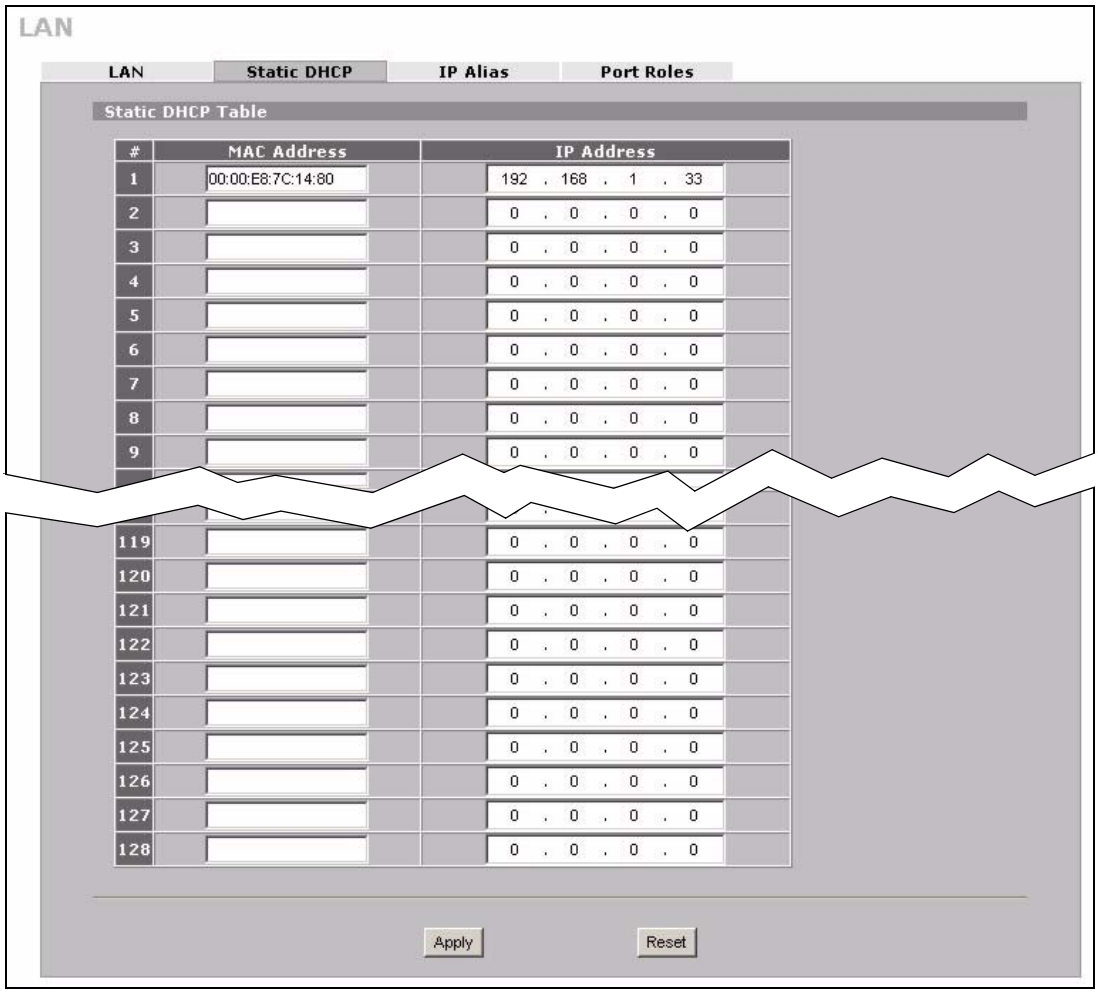
| LABEL | DESCRIPTION |
|---|---|
| Windows Networking (NetBIOS over TCP/IP) | NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls. However it may sometimes be necessary to allow NetBIOS packets to pass through to the WAN in order to find a computer on the WAN. |
| Allow between LAN and WAN1 | Select this check box to forward NetBIOS packets from the LAN to WAN 1and from WAN 1 to the LAN. If your firewall is enabled with the default policy set to block WAN 1 to LAN traffic, you also need to enable the default WAN 1 to LAN firewall rule that forwards NetBIOS traffic.<br>Clear this check box to block all NetBIOS packets going from the LAN to WAN 1 and from WAN 1 to the LAN. |
| Allow between LAN and WAN2 | Select this check box to forward NetBIOS packets from the LAN to WAN 2 and from WAN 2 to the LAN. If your firewall is enabled with the default policy set to block WAN 2 to LAN traffic, you also need to enable the default WAN 2 to LAN firewall rule that forwards NetBIOS traffic.<br>Clear this check box to block all NetBIOS packets going from the LAN to WAN 2 and from WAN 2 to the LAN. |
| Allow between LAN and DMZ | Select this check box to forward NetBIOS packets from the LAN to the DMZ and from the DMZ to the LAN. If your firewall is enabled with the default policy set to block DMZ to LAN traffic, you also need to enable the default DMZ to LAN firewall rule that forwards NetBIOS traffic.<br>Clear this check box to block all NetBIOS packets going from the LAN to the DMZ and from the DMZ to the LAN. |
| Allow between LAN and WLAN | Select this check box to forward NetBIOS packets from the LAN to the WLAN and from the WLAN to the LAN.<br>Clear this check box to block all NetBIOS packets going from the LAN to the WLAN and from the WLAN to the LAN. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 7.3 The LAN Static DHCP Screen

This table allows you to assign IP addresses on the LAN to specific individual computers based on their MAC addresses.

To change your ZyWALL's static DHCP settings, click **NETWORK** > **LAN** > **Static DHCP**. The screen appears as shown.

**Figure 84** NETWORK > LAN > Static DHCP




The following table describes the labels in this screen.

**Table 28** NETWORK > LAN > Static DHCP

| LABEL | DESCRIPTION |
|---|---|
| # | This is the index number of the static IP table entry (row). |
| MAC Address | Type the MAC address of a computer on your LAN. |
| IP Address | Type the IP address that you want to assign to the computer on your LAN. Alternatively, click the right mouse button to copy and/or paste the IP address. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 7.4 The LAN IP Alias Screen

IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface.

The ZyWALL has a single LAN interface. Even though more than one of ports 1~4 may be in the LAN port role, they are all still part of a single physical Ethernet interface and all use the same IP address.

The ZyWALL supports three logical LAN interfaces via its single physical LAN Ethernet interface. The ZyWALL itself is the gateway for each of the logical LAN networks.

When you use IP alias, you can also configure firewall rules to control access between the LAN's logical networks (subnets).

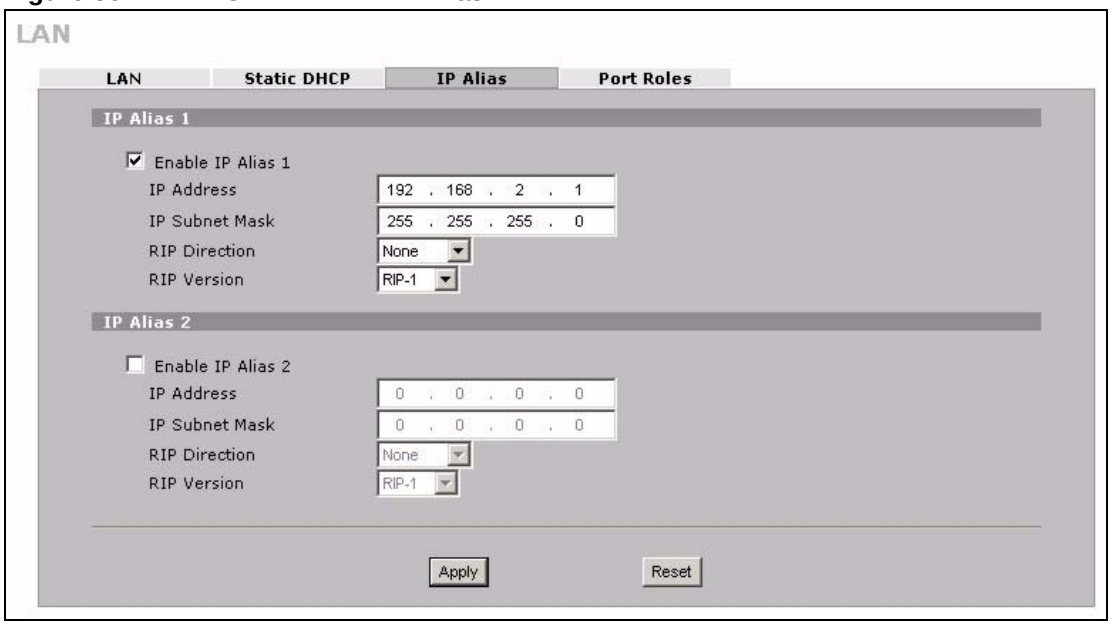
Make sure that the subnets of the logical networks do not overlap.

The following figure shows a LAN divided into subnets A, B, and C.

**Figure 85** Physical Network & Partitioned Logical Networks


To change your ZyWALL's IP alias settings, click **NETWORK** > **LAN** > **IP Alias**. The screen appears as shown.

**Figure 86** NETWORK > LAN > IP Alias



The following table describes the labels in this screen.

**Table 29** NETWORK > LAN > IP Alias

| LABEL | DESCRIPTION |
|---|---|
| Enable IP Alias 1, 2 | Select the check box to configure another LAN network for the ZyWALL. |
| IP Address | Enter the IP address of your ZyWALL in dotted decimal notation.<br>Alternatively, click the right mouse button to copy and/or paste the IP address. |
| IP Subnet Mask | Your ZyWALL will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyWALL. |
| RIP Direction | RIP (Routing Information Protocol, RFC 1058 and RFC 1389) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Select the RIP direction from **Both**/**In Only**/**Out Only**/**None**. When set to **Both** or **Out Only**, the ZyWALL will broadcast its routing table periodically. When set to **Both** or **In Only**, it will incorporate the RIP information that it receives; when set to **None**, it will not send any RIP packets and will ignore any RIP packets received. |
| RIP Version | The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyWALL sends (it recognizes both formats when receiving). **RIP-1** is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting.<br>Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to **Both** and the Version set to **RIP-1**. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 7.5 The LAN Port Roles Screen

Use the **Port Roles** screen to set ports as part of the LAN, DMZ and/or WLAN interface.

Ports 1~4 on the ZyWALL 5 and ZyWALL 35 ports can be part of the LAN, DMZ or WLAN interface. The ZyWALL 70 has a separate (dedicated) LAN port, so ports 1~4 can be set as part of the DMZ and/or WLAN interface.

Do the following if you are configuring from a computer connected to a LAN, DMZ or WLAN port and changing the port's role:

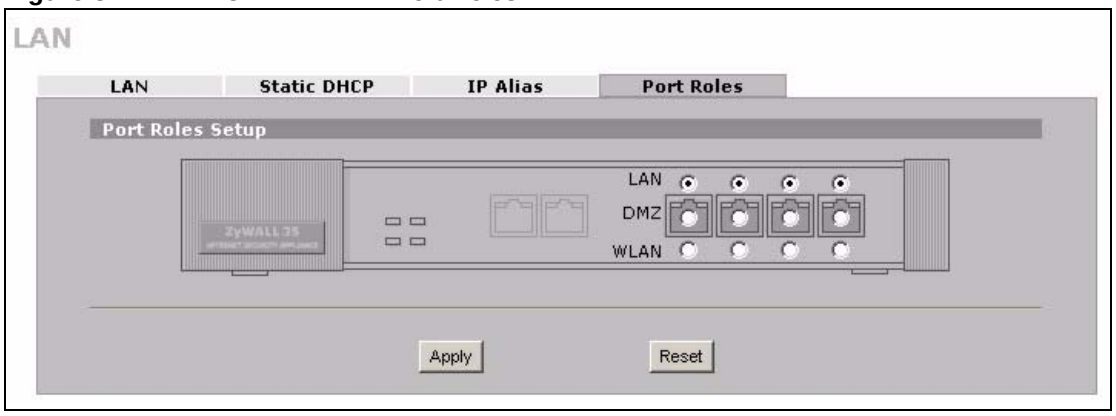
1. A port's IP address varies as its role changes, make sure your computer's IP address is in the same subnet as the ZyWALL's LAN, DMZ or WLAN IP address.
2. Use the appropriate LAN, DMZ or WLAN IP address to access the ZyWALL.

To change your ZyWALL's port role settings, click **NETWORK** > **LAN** > **Port Roles**. The screen appears as shown.

The radio buttons correspond to Ethernet ports on the front panel of the ZyWALL. On the ZyWALL 70, ports 1 to 4 are all DMZ ports by default. On the ZyWALL 5 or ZyWALL 35, ports 1 to 4 are all LAN ports by default.

Your changes are also reflected in the **DMZ Port Roles** and **WLAN Port Roles** screens.

**Figure 87** NETWORK > LAN > Port Roles




The following table describes the labels in this screen.

**Table 30** NETWORK > LAN > Port Roles

| LABEL | DESCRIPTION |
|---|---|
| LAN | Select a port's LAN radio button to use the port as part of the LAN. The port will use the ZyWALL's LAN IP address and MAC address. |
| DMZ | Select a port's DMZ radio button to use the port as part of the DMZ. The port will use the ZyWALL's DMZ IP address and MAC address. |
| WLAN | Select a port's WLAN radio button to use the port as part of the WLAN. The port will use the ZyWALL's WLAN IP address and MAC address. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

After you change the LAN/DMZ/WLAN port roles and click **Apply**, please wait for few seconds until the following screen appears. Click **Return** to go back to the **Port Roles** screen.

**Figure 88** Port Roles Change Complete

# 8

# Bridge Screens

## 8.1 Overview

The ZyWALL can act as a bridge between a switch and a wired LAN or between two routers. This chapter describes how to configure bridge settings. This chapter is only applicable when the ZyWALL is in bridge mode.

In bridge mode, the ZyWALL functions as a transparent firewall (also known as a bridge firewall). The ZyWALL bridges traffic traveling between the ZyWALL's interfaces and still filters and inspects packets. You do not need to change the configuration of your existing network.

In the first figure below the ZyWALL is in bridge mode and is bridging traffic on the WAN. The router device has a public WAN IP address and the ZyWALL is transparent. In the second figure the ZyWALL is in router mode and has a public WAN IP address and routes traffic between the LAN and WAN.

**Figure 89** Bridge Mode

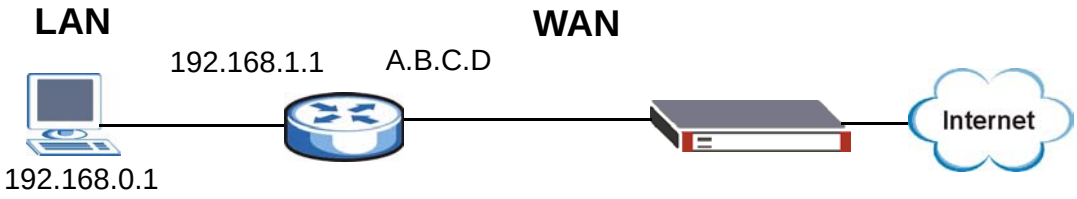
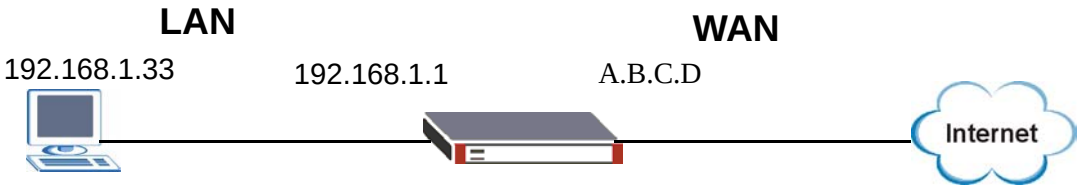



**Figure 90** Router Mode




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

- Use the **Bridge** screen (Section 8.2 on page 163) to configure bridge and RSTP (Rapid Spanning Tree Protocol) settings.
- Use the **Port Roles** screen (Section 8.3 on page 164) to set ports as part of the LAN, DMZ and/or WLAN interface.

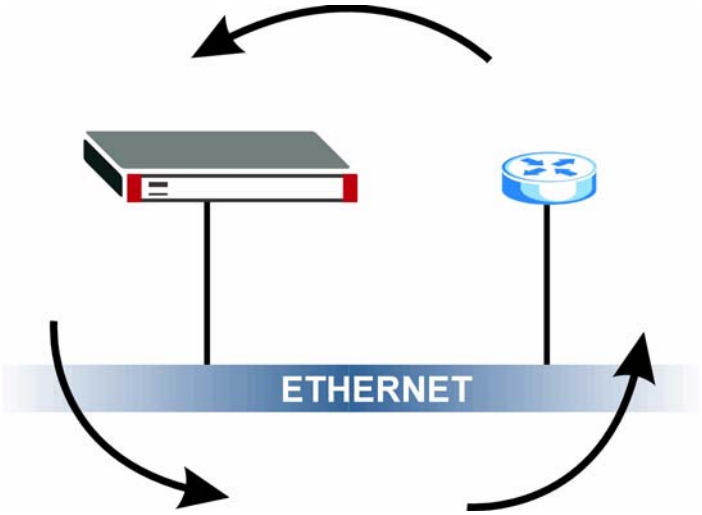
## 8.1.2 What You Need To Know About Bridging

### Bridge Loop

Be careful to avoid bridge loops when you enable bridging in the ZyWALL. Bridge loops cause broadcast traffic to circle the network endlessly, resulting in possible throughput degradation and disruption of communications. The following example shows the network topology that can lead to this problem:

- If your ZyWALL (in bridge mode) is connected to a wired LAN while communicating with another bridge or a switch that is also connected to the same wired LAN as shown next.

**Figure 91** Bridge Loop: Bridge Connected to Wired LAN




To prevent bridge loops, ensure that your ZyWALL is not set to bridge mode while connected to two wired segments of the same LAN or you enable RSTP in the **Bridge** screen.

### Spanning Tree Protocol (STP)

STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a bridge to interact with other STP-compliant bridges in your network to ensure that only one route exists between any two stations on the network.

### Rapid STP

The ZyWALL uses IEEE 802.1w RSTP (Rapid Spanning Tree Protocol) that allow faster convergence of the spanning tree (while also being backwards compatible with STP-only aware bridges). Using RSTP, topology change information does not have to propagate to the root bridge and unwanted learned addresses are flushed from the filtering database. In RSTP, the port states are Discarding, Learning, and Forwarding.

### Finding Out More

To see more information on bridging refer to Section 33.5 on page 591.

To see more advanced information on bridging refer to Section 8.4 on page 166.

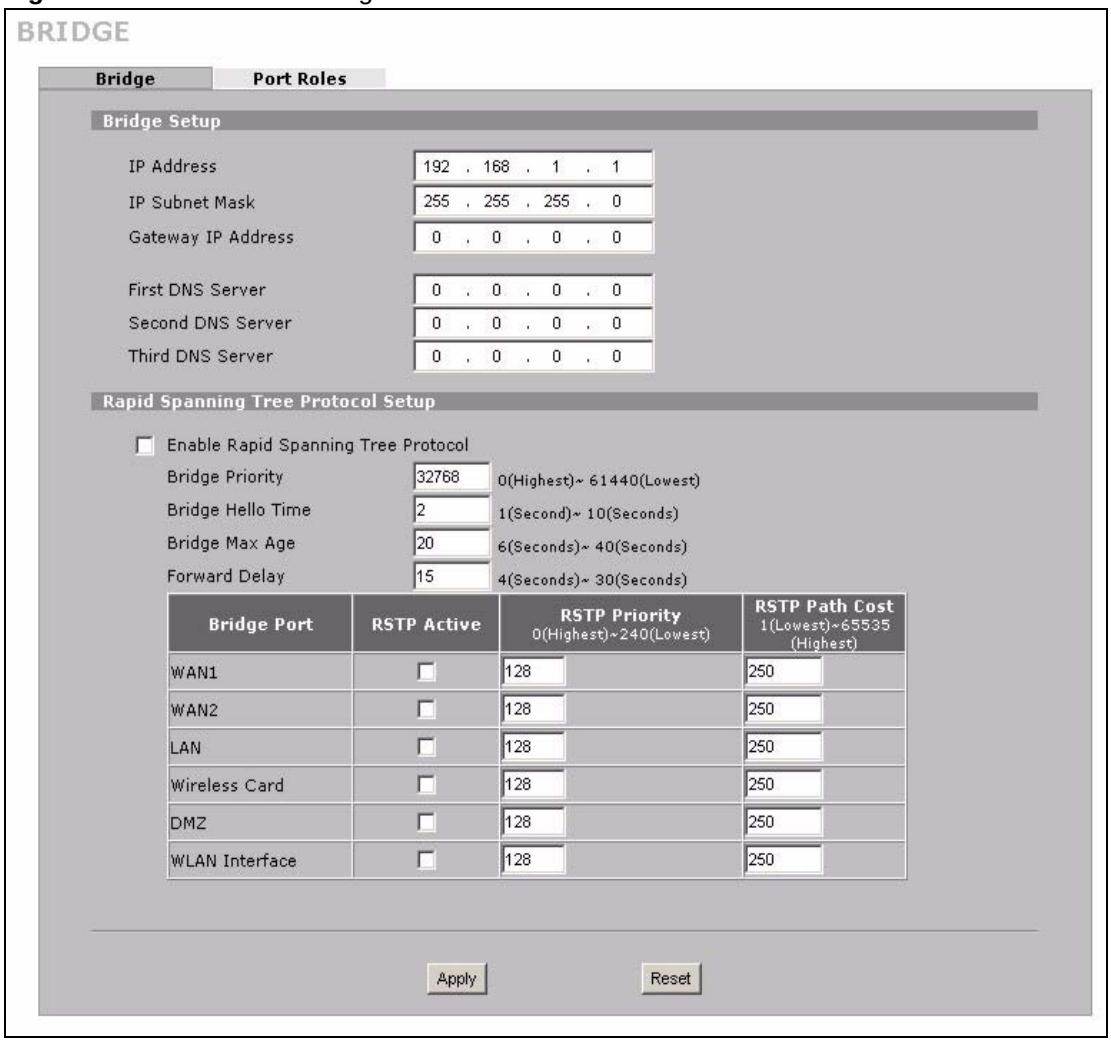
## 8.2 The Bridge Screen

Select **Bridge** and click **Apply** in the **MAINTENANCE > Device Mode** screen to have the ZyWALL function as a bridge.

You can use the firewall and VPN in bridge mode. See the user's guide for a list of other features that are available in bridge mode.

Click **NETWORK** > **BRIDGE** to display the screen shown next. Use this screen to configure bridge and RSTP (Rapid Spanning Tree Protocol) settings.

**Figure 92** NETWORK > Bridge




The following table describes the labels in this screen.

**Table 31** NETWORK > Bridge

| LABEL | DESCRIPTION |
|---|---|
| Bridge IP Address Setup | |
| IP Address | Type the IP address of your ZyWALL in dotted decimal notation. |
| IP Subnet Mask | The subnet mask specifies the network number portion of an IP address. |
| Gateway IP Address | Enter the gateway IP address. |

**Table 31** NETWORK > Bridge (continued)

| LABEL | DESCRIPTION |
|---|---|
| First/Second/Third 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 machine before you can access it. The ZyWALL uses a system DNS server (in the order you specify here) to resolve domain names for content filtering, the time server, etc.<br>If you have the IP address(es) of the DNS server(s), enter the DNS server's IP address(es) in the field(s) to the right. |
| Rapid Spanning Tree Protocol Setup | |
| Enable Rapid Spanning Tree Protocol | Select the check box to activate RSTP on the ZyWALL. |
| Bridge Priority | Enter a number between 0 and 61440 as bridge priority of the ZyWALL.<br>Bridge priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the root. If multiple devices have the lowest priority, the device with the lowest MAC address becomes the root.<br>The lower the numeric value you assign, the higher the priority for this bridge.<br>Bridge Priority determines the root bridge, which in turn determines Hello Time, Max Age and Forward Delay. |
| Bridge Hello Time | Enter an interval (between 1 and 10) in seconds that the root bridge waits before sending a hello packet. |
| Bridge Max Age | Enter an interval (between 6 and 40) in seconds that a bridge waits to get a Hello BPDU from the root bridge. |
| Forward Delay | Enter the length of time (between 4 and 30) in seconds that a bridge remains in the listening and learning port states. The default is 15 seconds. |
| Bridge Port | This is the bridge port type. |
| RSTP Active | Select the check box to enable RSTP on the corresponding port. |
| RSTP Priority 0(Highest)~240(Lowest) | Enter a number between 0 and 240 as RSTP priority for the corresponding port. 0 is the highest. |
| RSTP Path Cost 1(Lowest)~65535(Highest) | Enter a number between 1 and 65535 as RSTP path cost for the corresponding port. 65535 is the highest. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 8.3 The Bridge Port Roles Screen

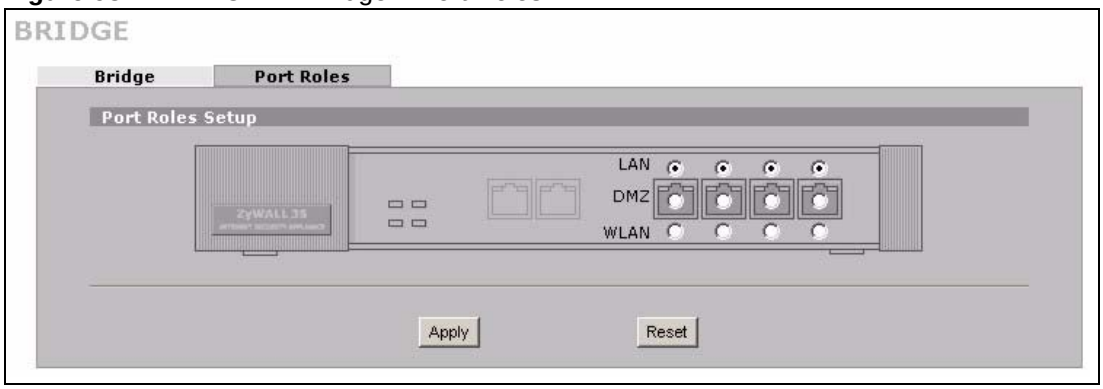
Use the **Port Roles** screen to set ports as part of the LAN, DMZ and/or WLAN interface.

Ports 1~4 on the ZyWALL 5 and ZyWALL 35 ports can be part of the LAN, DMZ or WLAN interface. The ZyWALL 70 has a separate (dedicated) LAN port, so ports 1~4 can be set as part of the DMZ and/or WLAN interface.

To change your ZyWALL's port role settings, click **NETWORK** > **BRIDGE** > **Port Roles**. The screen appears as shown.

The radio buttons correspond to Ethernet ports on the front panel of the ZyWALL. On the ZyWALL 70, ports 1 to 4 are all DMZ ports by default. On the ZyWALL 5 or ZyWALL 35, ports 1 to 4 are all LAN ports by default.

**Figure 93** NETWORK > Bridge > Port Roles




The following table describes the labels in this screen.

**Table 32** NETWORK > Bridge > Port Roles

| LABEL | DESCRIPTION |
|---|---|
| LAN | Select a port's LAN radio button to use the port as part of the LAN. |
| DMZ | Select a port's DMZ radio button to use the port as part of the DMZ. |
| WLAN | Select a port's WLAN radio button to use the port as part of the WLAN. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

After you change the LAN/DMZ/WLAN port roles and click **Apply**, please wait for few seconds until the following screen appears. Click **Return** to go back to the **Port Roles** screen.

**Figure 94** Port Roles Change Complete

# 8.4 Bridge Technical Reference

## STP Terminology

The root bridge is the base of the spanning tree. Path cost is the cost of transmitting a frame from the root bridge to that port. It is assigned according to the speed of the link to which a port is attached. The slower the media, the higher the cost - see the next table.

**Table 33** STP Path Costs

| | LINK SPEED | RECOMMENDED VALUE | RECOMMENDED RANGE | ALLOWED RANGE |
|---|---|---|---|---|
| Path Cost | 4Mbps | 250 | 100 to 1000 | 1 to 65535 |
| Path Cost | 10Mbps | 100 | 50 to 600 | 1 to 65535 |
| Path Cost | 16Mbps | 62 | 40 to 400 | 1 to 65535 |
| Path Cost | 100Mbps | 19 | 10 to 60 | 1 to 65535 |
| Path Cost | 1Gbps | 4 | 3 to 10 | 1 to 65535 |
| Path Cost | 10Gbps | 2 | 1 to 5 | 1 to 65535 |

On each bridge, the root port is the port through which this bridge communicates with the root. It is the port on this switch with the lowest path cost to the root (the root path cost). If there is no root port, then this bridge has been accepted as the root bridge of the spanning tree network.

For each LAN segment, a designated bridge is selected. This bridge has the lowest cost to the root among the bridges connected to the LAN.

## How STP Works

After a bridge determines the lowest cost-spanning tree with STP, it enables the root port and the ports that are the designated ports for connected LANs, and disables all other ports that participate in STP. Network packets are therefore only forwarded between enabled ports, eliminating any possible network loops.

STP-aware bridges exchange Bridge Protocol Data Units (BPDUs) periodically. When the bridged LAN topology changes, a new spanning tree is constructed.

Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a Hello BPDU after a predefined interval (Max Age), the bridge assumes that the link to the root bridge is down. This bridge then initiates negotiations with other bridges to reconfigure the network to re-establish a valid network topology.

# STP Port States

STP assigns five port states (see next table) to eliminate packet looping. A bridge port is not allowed to go directly from blocking state to forwarding state so as to eliminate transient loops.

**Table 34** STP Port States

| PORT STATE | DESCRIPTION |
|---|---|
| Disabled | STP is disabled (default). |
| Blocking | Only configuration and management BPDUs are received and processed. |
| Listening | All BPDUs are received and processed. |
| Learning | All BPDUs are received and processed. Information frames are submitted to the learning process but not forwarded. |
| Forwarding | All BPDUs are received and processed. All information frames are received and forwarded. |

# 9

# WAN Screens

## 9.1 Overview

This chapter discusses the ZyWALL's **WAN** screens. Use these screens to configure your ZyWALL for Internet access.

A WAN (Wide Area Network) connection is an outside connection to another network or the Internet. It connects your private networks (such as a LAN (Local Area Network) and other networks, so that a computer in one location can communicate with computers in other locations.

The ZyWALL has a multiple WAN feature which enables you to connect up to two ISPs (or networks). The ZyWALL 5 also supports a 3G WAN connection. You can configure the distribution of traffic on the WAN connections using the load balancing settings.

You can have either a wired WAN connection with a 3G (WAN) connection or two wired WAN connections as shown in the following figures.

**Figure 95** LAN and WAN (Multiple)

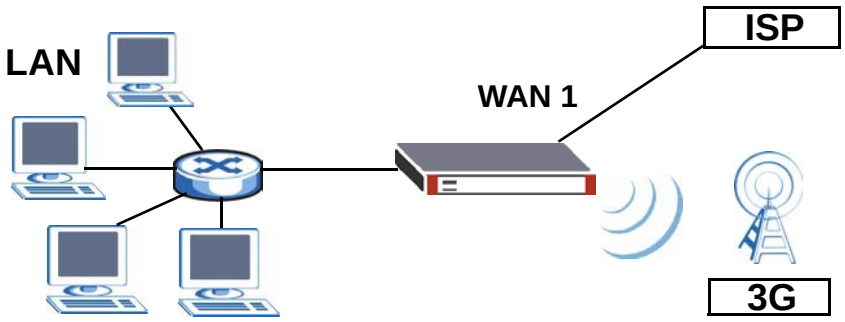
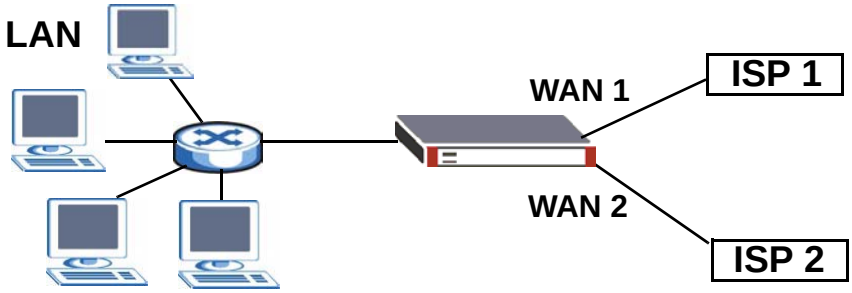



**Figure 96** LAN and WAN (Multiple)



## 9.1.1 What You Can Do in the WAN Screens

- Use the **General** screen (Section 9.2 on page 172) to configure load balancing, route priority, and connection test settings for the ZyWALL.
- Use the **WAN 1 and 2** screens (Section 9.3 on page 182) to configure the WAN1 and WAN2 interfaces for Internet access on the ZyWALL.
- Use the **3G (WAN2)** screen (Section 9.4 on page 192 for 3G) to configure the WAN2 interface for Internet access on the ZyWALL.
- Use the **Traffic Redirect** screen (Section 9.5 on page 197) to configure an alternative gateway.
- Use the **Dial Backup** screen (Section 9.7 on page 199) to configure the backup WAN dial-up connection.

## 9.1.2 What You Need to Know About WAN

### Encapsulation Method

Encapsulation is used to include data from an upper layer protocol into a lower layer protocol. To set up a WAN connection to the Internet, you need to use the same encapsulation method used by your ISP (Internet Service Provider). If your ISP offers a dial-up Internet connection using PPPoE (PPP over Ethernet) or PPPoA, they should also provide a username and password (and service name) for user authentication.

### WAN IP Address

The WAN IP address is an IP address for the ZyWALL, which makes it accessible from an outside network. It is used by the ZyWALL to communicate with other devices in other networks. It can be static (fixed) or dynamically assigned by the ISP each time the ZyWALL tries to access the Internet.

If your ISP assigns you a static WAN IP address, they should also assign you the subnet mask and DNS server IP address(es) (and a gateway IP address if you use the Ethernet or ENET ENCAP encapsulation method).

### 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.

### Multiple WAN Features

You can use a second connection for load sharing to increase overall network throughput or as a backup to enhance network reliability.

The ZyWALL 70 or ZyWALL 35 has two WAN ports. You can connect one port to one ISP (or network) and connect the other to a second ISP (or network). When the ZyWALL 5 is in router mode, you can optionally insert a 3G card to add a second WAN interface.

The ZyWALL can balance the load between the two WAN interfaces (see Section 9.2.2 on page 177).

You can use policy routing to specify the WAN interface that specific services go through. An ISP may give traffic from certain (more expensive) connections priority over the traffic from other accounts. You could route delay intolerant traffic (like voice over IP calls) through this kind of connection. Other traffic could be routed through a cheaper broadband Internet connection that does not provide priority service. If one WAN interface's connection goes down, the ZyWALL can automatically send its traffic through the other WAN interface. See Chapter 24 on page 457 for details.

The ZyWALL's NAT feature allows you to configure sets of rules for one WAN interface and separate sets of rules for the other WAN interface. Refer to Chapter 22 on page 435 for details.

You can select through which WAN interface you want to send out traffic from UPnP-enabled applications (see Chapter 28 on page 519).

The ZyWALL's DDNS lets you select which WAN interface you want to use for each individual domain name. The DDNS high availability feature lets you have the ZyWALL use the other WAN interface for a domain name if the configured WAN interface's connection goes down. See Section 26.1.2 on page 479 for details.

When configuring a VPN rule, you have the option of selecting one of the ZyWALL's domain names in the **My Address** field.

### Load Balancing

On the ZyWALL, load balancing is the process of dividing traffic loads between the two WAN interfaces (or ports). This allows you to improve quality of services and maximize bandwidth utilization.

See also policy routing to provide quality of service by dedicating a route for a specific traffic type and bandwidth management to specify a set amount of bandwidth for a specific traffic type on an interface.

The ZyWALL uses three load balancing methods (least load first, weighted round robin and spillover) to decide which WAN interface the traffic for a session[1] (from the LAN) uses.

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.

### TCP/IP Priority (Metric)

The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".

1. The metric sets the priority for the ZyWALL's routes to the Internet. Each route must have a unique metric.
2. The priorities of the WAN interface routes must always be higher than the dial-backup and traffic redirect route priorities.

1. In the load balancing section, a session may refer to normal connection-oriented, UDP and SNMP2 traffic.

Lets say that you have the WAN operation mode set to active/passive, meaning the ZyWALL uses the second highest priority WAN interface as a back up. The WAN 1 route has a metric of "2", the WAN 2 route has a metric of "3", the traffic-redirect route has a metric of "14" and the dial-backup route has a metric of "15". In this case, the WAN 1 route acts as the primary default route. If the WAN 1 route fails to connect to the Internet, the ZyWALL tries the WAN 2 route next. If the WAN 2 route fails, the ZyWALL tries the traffic-redirect route. In the same manner, the ZyWALL uses the dial-backup route if the traffic-redirect route also fails.

The dial-backup or traffic redirect routes cannot take priority over the WAN 1 and WAN 2 routes.

#### Finding Out More

Refer to Section 7.1.2 on page 150 for information on IP addresses, LAN and more.

### 9.1.3 Before You Begin

You need to know your Internet access settings such as encapsulation and WAN IP address. Get this information from your ISP.

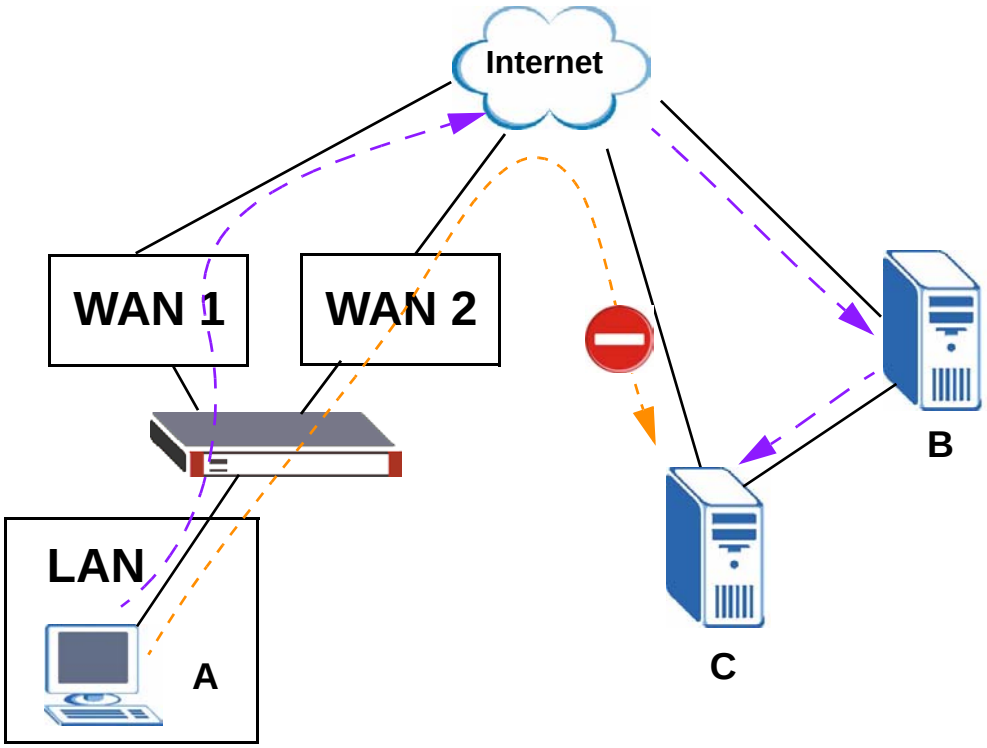
## 9.2 The General Screen

Use this screen to configure load balancing, route priority, and connection test properties.

#### Mapping a WAN Interface to a Local Host

You can set the ZyWALL to send all of a local computer's traffic through the same WAN interface. 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 97** Incorrect WAN IP




1. LAN user **A** wants to download a file from a remote server on the Internet. The ZyWALL is using active/active load balancing and sends the request to an update server (**B**) through WAN 1.
2. Update server **B** sends a file list to LAN user **A**. The download address of the desired file is a file server (**C**). At the same time, update server **B** informs file server **C** that a computer located at the WAN 1's IP address will download a file.
3. When LAN user **A** tries to retrieve the file from file server **C**, the request goes through WAN 2.

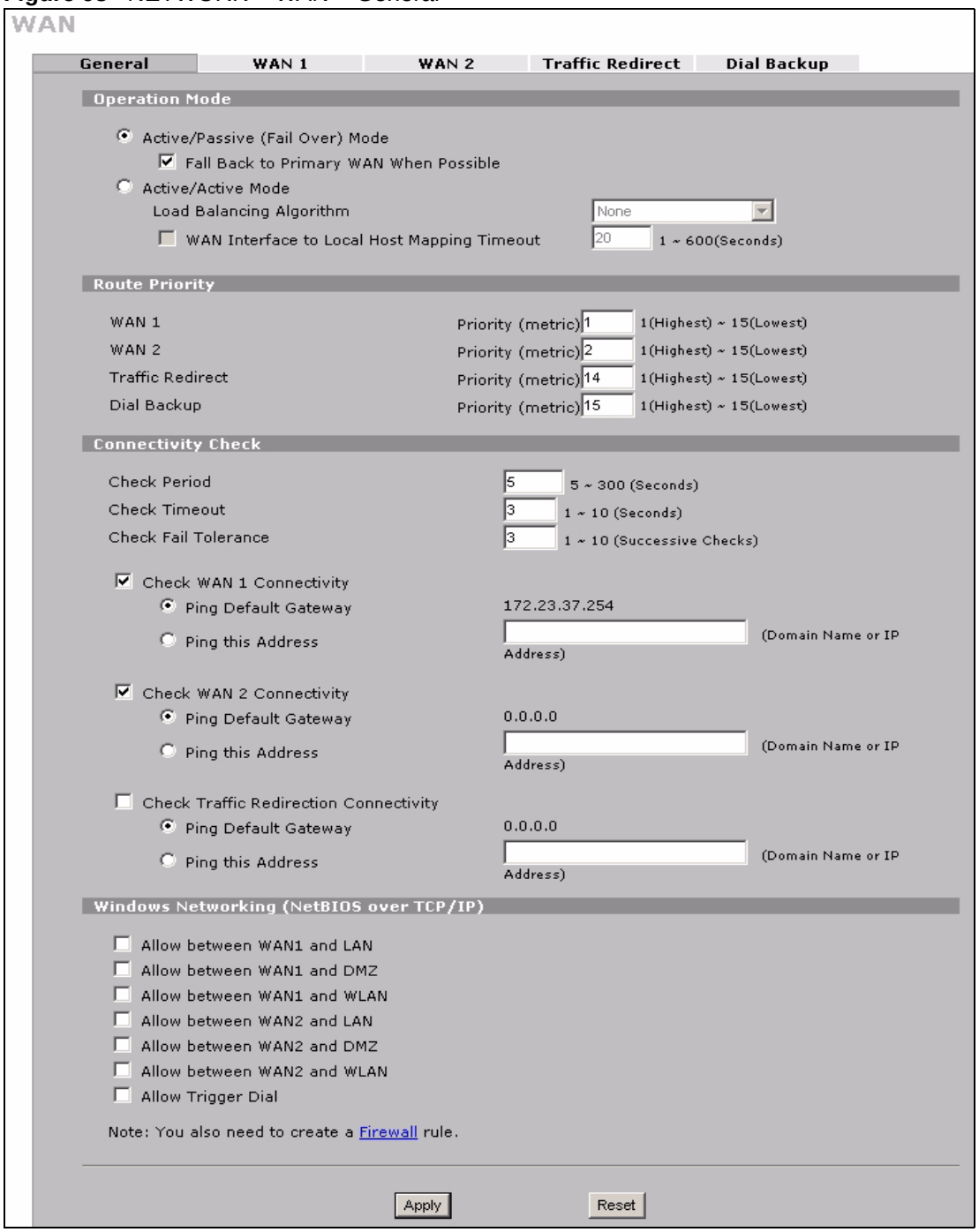
File server **C** finds that the request comes from WAN 2's IP address instead of WAN 1's IP address and rejects the request.

## 9.2.1 Configuring the General Screen

To configure your WAN General settings click **NETWORK** > **WAN** to open the **General** screen.

WAN 2 refers to either the physical WAN 2 port on a ZyWALL with multiple WAN ports or the 3G card on a single WAN ZyWALL in router mode.

**Figure 98** NETWORK > WAN > General



The following table describes the labels in this screen.

**Table 35** NETWORK > WAN > General

| LABEL | DESCRIPTION |
|---|---|
| Active/Passive (Fail Over) Mode | Select the Active/Passive (fail over) operation mode to have the ZyWALL use the second highest priority WAN interface as a back up. This means that the ZyWALL will normally use the highest priority (primary) WAN interface (depending on the priorities you configure in the **Route Priority** fields). The ZyWALL will switch to the secondary (second highest priority) WAN interface when the primary WAN interface's connection fails. |
| Fall Back to Primary WAN When Possible | This field determines the action the ZyWALL takes after the primary WAN interface fails and the ZyWALL starts using the secondary WAN interface.<br>Select this check box to have the ZyWALL change back to using the primary WAN interface when the ZyWALL can connect through the primary WAN interface again.<br>Clear this check box to have the ZyWALL continue using the secondary WAN interface, even after the ZyWALL can connect through the primary WAN interface again. The ZyWALL continues to use the secondary WAN interface until it's connection fails (at which time it will change back to using the primary WAN interface if its connection is up. |
| Active/Active Mode | Select **Active/Active Mode** to have the ZyWALL use both of the WAN interfaces at the same time and allow you to enable load balancing. |
| Load Balancing Algorithm | Select **Least Load First**, **Weighted Round Robin** or **Spillover** to activate load balancing and set the related fields. Otherwise, select **None**.<br>Refer to Section 9.2.2 on page 177 for load balancing configuration. |
| WAN Interface to Local Host Mapping Timeout | Select this option to have the ZyWALL send all of a local computer's traffic through the same WAN interface for the period of time that you specify (1 to 600 seconds).<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.<br>This field is configurable only when you select **Active/Active Mode** and enable load balancing. |
| Route Priority | |
| WAN1<br>WAN2<br>Traffic Redirect<br>Dial Backup | The default WAN connection is "1' as your broadband connection via the WAN interface should always be your preferred method of accessing the WAN. The ZyWALL switches from WAN interface 1 to WAN interface 2 if WAN interface 1's connection fails and then back to WAN interface 1 when WAN interface 1's connection comes back up. The default priority of the routes is **WAN 1**, **WAN 2**, **Traffic Redirect** and then **Dial Backup**:<br>You have three choices for an auxiliary connection (**WAN 2**, **Traffic Redirect** and **Dial Backup**) in the event that your regular WAN connection goes down. If **Dial Backup** is preferred to **Traffic Redirect**, then type "14" in the **Dial Backup Priority (metric)** field (and leave the **Traffic Redirect Priority (metric)** at the default of "15").<br>The **Dial Backup** field is available only when you enable the corresponding dial backup feature in the **Dial Backup** screen. |
| Connectivity Check | |
| Check Period | The ZyWALL tests a WAN connection by periodically sending a ping to either the default gateway or the address in the **Ping this Address** field.<br>Type a number of seconds (5 to 300) to set the time interval between checks. Allow more time if your destination IP address handles lots of traffic. |
| Check Timeout | Type the number of seconds (1 to 10) for your ZyWALL to wait for a response to the ping before considering the check to have failed. This setting must be less than the **Check Period**. Use a higher value in this field if your network is busy or congested. |

**Table 35** NETWORK > WAN > General (continued)

| LABEL | DESCRIPTION |
|---|---|
| Check Fail Tolerance | Type how many WAN connection checks can fail (1-10) before the connection is considered "down" (not connected). The ZyWALL still checks a "down" connection to detect if it reconnects. |
| Check WAN1/2 Connectivity | Select the check box to have the ZyWALL periodically test the respective WAN interface's connection.<br>Select **Ping Default Gateway** to have the ZyWALL ping the WAN interface's default gateway IP address.<br>Select **Ping this Address** and enter a domain name or IP address of a reliable nearby computer (for example, your ISP's DNS server address) to have the ZyWALL ping that address. For a domain name, use up to 63 alphanumeric characters (hyphens, periods and the underscore are also allowed) without spaces. |
| Check Traffic Redirection Connectivity | Select the check box to have the ZyWALL periodically test the traffic redirect connection.<br>Select **Ping Default Gateway** to have the ZyWALL ping the backup gateway's IP address.<br>Select **Ping this Address** and enter a domain name or IP address of a reliable nearby computer (for example, your ISP's DNS server address) to have the ZyWALL ping that address. For a domain name, use up to 63 alphanumeric characters (hyphens, periods and the underscore are also allowed) without spaces. |
| Windows Networking (NetBIOS over TCP/IP): | NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls. |
| Allow between WAN1 and LAN | Select this check box to forward NetBIOS packets from WAN 1 to the LAN port and from the LAN port to WAN1. If your firewall is enabled with the default policy set to block WAN 1 to LAN traffic, you also need to enable the default WAN1 to LAN firewall rule that forwards NetBIOS traffic.<br>Clear this check box to block all NetBIOS packets going from WAN 1 to the LAN port and from LAN port to WAN1. |
| Allow between WAN1 and DMZ | Select this check box to forward NetBIOS packets from WAN 1 to the DMZ port and from the DMZ port to WAN1.<br>Clear this check box to block all NetBIOS packets going from WAN 1 to the DMZ port and from DMZ port to WAN1. |
| Allow between WAN1 and WLAN | Select this check box to forward NetBIOS packets from WAN 1 to the WLAN port and from the WLAN port to WAN 1.<br>Clear this check box to block all NetBIOS packets going from WAN 1to the WLAN port and from WLAN port to WAN1. |
| Allow between WAN2 and LAN | Select this check box to forward NetBIOS packets from WAN 2 to the LAN port and from the LAN port to WAN2. If your firewall is enabled with the default policy set to block WAN 2 to LAN traffic, you also need to enable the default WAN2 to LAN firewall rule that forwards NetBIOS traffic.<br>Clear this check box to block all NetBIOS packets going from WAN 2 to the LAN port and from LAN port to WAN2. |
| Allow between WAN2 and DMZ | Select this check box to forward NetBIOS packets from WAN 2 to the DMZ port and from the DMZ port to WAN2.<br>Clear this check box to block all NetBIOS packets going from WAN 2 to the DMZ port and from DMZ port to WAN2. |
| Allow between WAN1 and WLAN | Select this check box to forward NetBIOS packets from WAN 2 to the WLAN port and from the WLAN port to WAN 2.<br>Clear this check box to block all NetBIOS packets going from WAN 2 to the WLAN port and from WLAN port to WAN 2. |

**Table 35** NETWORK > WAN > General (continued)

| LABEL | DESCRIPTION |
|---|---|
| Allow Trigger Dial | Select this option to allow NetBIOS packets to initiate calls. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 9.2.2 Configuring Load Balancing

To configure load balancing on the ZyWALL, click **NETWORK** > **WAN** in the navigation panel. The **WAN General** screen displays by default. Select **Active/Active Mode** under **Operation Mode** to enable load balancing on the ZyWALL.

The **WAN General** screen varies depending on what you select in the **Load Balancing Algorithm** field.

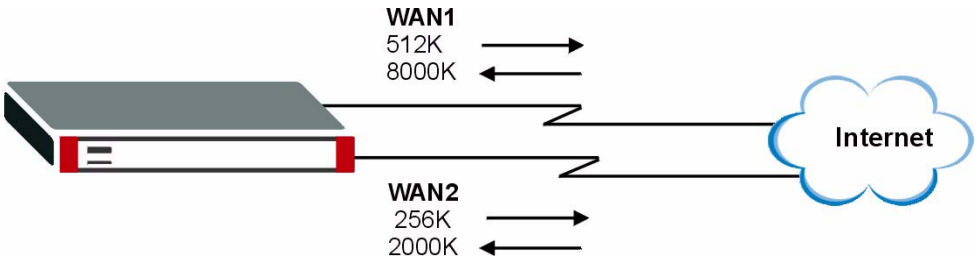
## 9.2.3 Least Load First

The least load first algorithm uses the current (or recent) outbound and/or inbound bandwidth utilization of each WAN interface as the load balancing criteria for making decisions on how how to route traffic. The outbound bandwidth utilization is defined as the measured outbound throughput over the available outbound bandwidth. The inbound bandwidth utilization is defined as the measured inbound throughput over the available inbound bandwidth. The two ratios are indexes used to calculate which WAN interface is less utilized at the time. A new LAN-originated session is distributed to the less utilized WAN interface.

**Example 1**

The following figure depicts an example where both the WAN interfaces on the ZyWALL are connected to the Internet. The configured available outbound bandwidths for WAN 1 and WAN 2 are 512K and 256K respectively.

**Figure 99** Least Load First Example




If the outbound bandwidth utilization is used as the load balancing index and the measured outbound throughput of WAN 1 is 412K and 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 36** Least Load First: Example 1

| 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 |

**Example 2**

This example uses the same network scenario as in Figure 99 on page 177, but uses both the outbound and inbound bandwidth utilization in calculating the load balancing index. If the measured inbound stream throughput for both WAN 1 and WAN 2 is 1600K, the ZyWALL calculates the average load balancing indices as shown in the table below.

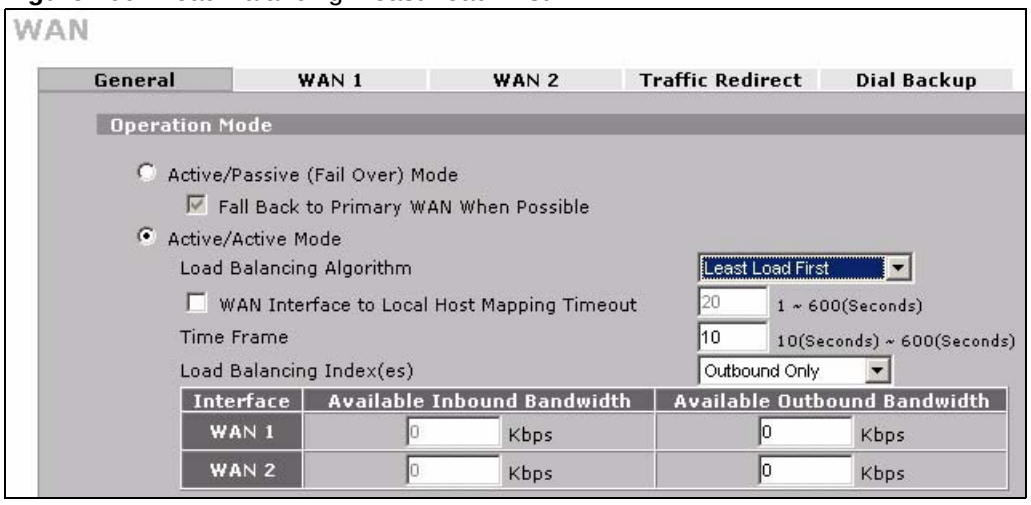
Since WAN 1 has a smaller load balancing index (meaning that it is less utilized than WAN 2), the ZyWALL will send the next new session traffic through WAN 1.

**Table 37** Least Load First: Example 2

| INTERFACE | OUTBOUND | | INBOUND | | AVERAGE LOAD BALANCING INDEX (OM / OA + IM / IA) / 2 |
|---|---|---|---|---|---|
| | AVAILABLE (OA) | MEASURED (OM) | AVAILABLE (IA) | MEASURED (IM) | |
| WAN 1 | 512 K | 412 K | 8000 K | 1600 K | ( 0.8 + 0.2) / 2 = 0.5 |
| WAN 2 | 256 K | 198 K | 2000 K | 1600 K | ( 0.77 + 0.8 ) / 2 = 0.79 |

To configure **Least Load First**, select **Least Load First** in the **Load Balancing Algorithm** field.

**Figure 100** Load Balancing: Least Load First



The following table describes the related fields in this screen.

**Table 38** Load Balancing: Least Load First

| LABEL | DESCRIPTION |
|---|---|
| Active/Active Mode | Select **Active/Active Mode** and set the related fields to enable load balancing on the ZyWALL. |
| Load Balancing Algorithm | Set the load balancing method to **Least Load First**. |
| WAN Interface to Local Host Mapping Timeout | Select this option to have the ZyWALL send all of a local computer's traffic through the same WAN interface for the period of time that you specify (1 to 600 seconds).<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. |
| Time Frame | You can set the ZyWALL to get the measured bandwidth using the average bandwidth in the specified time interval.<br>Enter the time interval between 10 and 600 seconds. |
| Load Balancing Index(es) | Specify the direction of the traffic utilization you want the ZyWALL to use in calculating the load balancing index.<br>Select **Outbound Only**, **Inbound Only** or **Outbound + Inbound**. |
| Interface | This field displays the name of the WAN interface (**WAN 1** and **WAN 2**). |
| Available Inbound Bandwidth | This field is applicable when you select **Outbound + Inbound** or **Inbound Only** in the **Load Balancing Index(es)** field.<br>Specify the inbound (or downstream) bandwidth (in kilo bites per second) for the interface. This should be the actual downstream bandwidth that your ISP provides. |
| Available Outbound Bandwidth | This field is applicable when you select **Outbound + Inbound** or **Outbound Only** in the **Load Balancing Index(es)** field.<br>Specify the outbound (or upstream) bandwidth (in kilo bites per second) for the interface. This should be the actual upstream bandwidth that your ISP provides. |

## 9.2.4 Weighted Round Robin

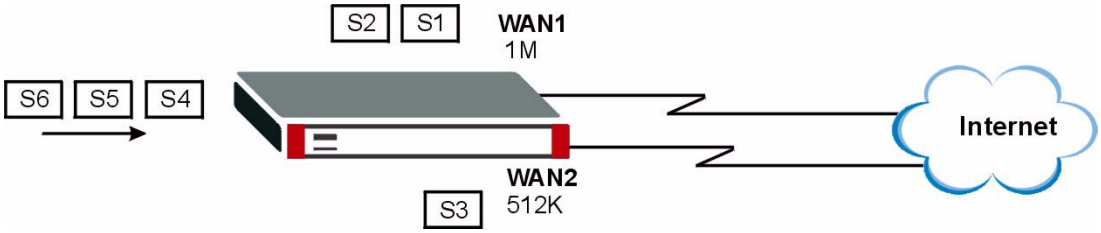
Round Robin routes traffic on a rotating basis and is activated only when a WAN interface has more traffic than the configured available bandwidth. On the ZyWALL with two WAN interfaces, an amount of traffic is sent through the first interface. The second interface is also given an equal amount of traffic, and then the same amount of traffic is sent through the first interface again; and so on. This works in a looping fashion until there is no outgoing traffic.

Similar to the Round Robin (RR) algorithm, 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.

This algorithm is best suited for situations when the bandwidths set for the two WAN interfaces are different.

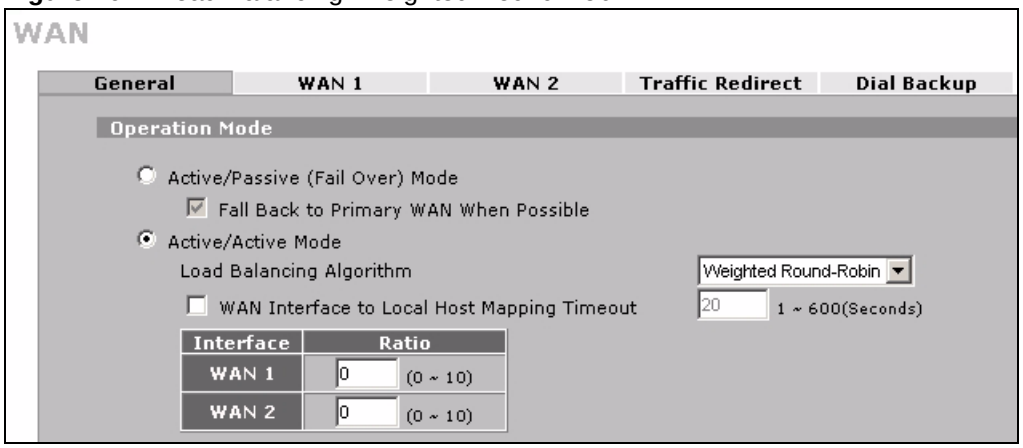
For example, in the figure below, the configured available bandwidth of WAN1 is 1M and WAN2 is 512K. You can set the ZyWALL to distribute the network traffic between the two interfaces by setting the weight of WAN1 and WAN2 to 2 and 1 respectively. The ZyWALL assigns the traffic of two sessions to WAN1 for every one session's traffic assigned to WAN2.

**Figure 101** Weighted Round Robin Algorithm Example




To load balance using the weighted round robin method, select **Weighted Round Robin** in the **Load Balancing Algorithm** field.

**Figure 102** Load Balancing: Weighted Round Robin




The following table describes the related fields in this screen.

**Table 39** Load Balancing: Weighted Round Robin

| LABEL | DESCRIPTION |
|---|---|
| Active/Active Mode | Select **Active/Active Mode** and set the related fields to enable load balancing on the ZyWALL. |
| Load Balancing Algorithm | Set the load balancing method to **Weighted Round Robin**. |
| WAN Interface to Local Host Mapping Timeout | Select this option to have the ZyWALL send all of a local computer's traffic through the same WAN interface for the period of time that you specify (1 to 600 seconds). 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. |
| Interface | This field displays the name of the WAN interface (**WAN 1** and **WAN 2**). |
| Ratio | Specify the weight for the interface. Enter 0 to set the ZyWALL not to send traffic load to the interface. The higher the number, the bigger the weight (the more traffic sent). |

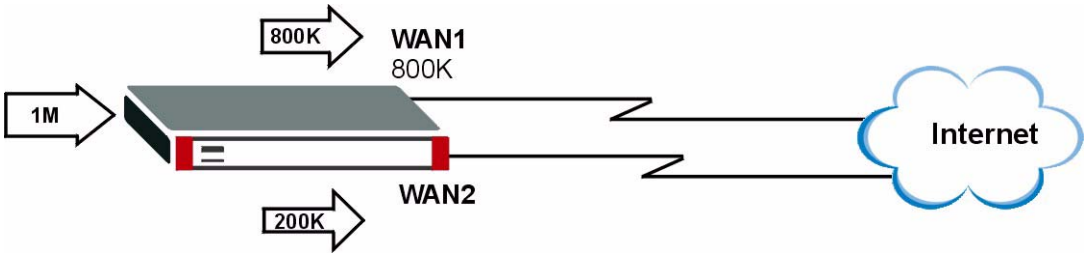
## 9.2.5 Spillover

With the spillover load balancing algorithm, the ZyWALL sends network traffic to the primary interface until the maximum allowable load is reached, then the ZyWALL sends the excess network traffic of new sessions to the secondary WAN interface. Configure the **Route Priority** metrics in the **WAN General** screen to determine the primary and secondary WANs.

In cases where the primary WAN interface uses an unlimited access Internet connection and the secondary WAN uses a per-use timed access plan, the ZyWALL will only use the secondary WAN interface when the traffic load reaches the upper threshold on the primary WAN interface. This allows you to fully utilize the bandwidth of the primary WAN interface while avoiding overloading it and reducing Internet connection fees at the same time.

In the following example figure, the upper threshold of the primary WAN interface is set to 800K. The ZyWALL sends network traffic of a new session that exceeds this limit to the secondary WAN interface.

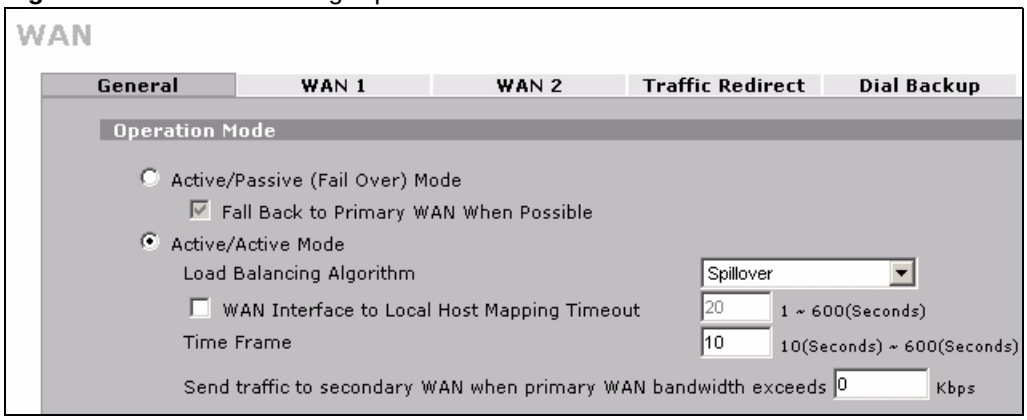
**Figure 103** Spillover Algorithm Example




To load balance using the spillover method, select **Spillover** in the **Load Balancing Algorithm** field.

Configure the **Route Priority** metrics in the **WAN General** screen to determine the primary and secondary WANs. By default, WAN 1 is the primary WAN and WAN 2 is the secondary WAN.

**Figure 104** Load Balancing: Spillover




The following table describes the related fields in this screen.

**Table 40** Load Balancing: Spillover

| LABEL | DESCRIPTION |
|---|---|
| Active/Active Mode | Select **Active/Active Mode** and set the related fields to enable load balancing on the ZyWALL. |
| Load Balancing Algorithm | Set the load balancing method to **Spillover**. |

**Table 40** Load Balancing: Spillover (continued)

| LABEL | DESCRIPTION |
|---|---|
| WAN Interface to Local Host Mapping Timeout | Select this option to have the ZyWALL send all of a local computer's traffic through the same WAN interface for the period of time that you specify (1 to 600 seconds).<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. |
| Time Frame | You can set the ZyWALL to get the measured bandwidth using the average bandwidth in the specified time interval.<br>Enter the time interval between 10 and 600 seconds. |
| Send traffic to secondary WAN when primary WAN bandwidth exceeds | Specify the maximum allowable bandwidth on the primary WAN. Once this maximum bandwidth is reached, the ZyWALL sends the new session traffic that exceeds this limit to the secondary WAN. The ZyWALL continues to send traffic of existing sessions to the primary WAN. |

## 9.3 The WAN1 and WAN2 Screen

To change your ZyWALL's WAN ISP, IP and MAC settings, click **NETWORK** > **WAN** and then the **WAN** > **WAN 1** or **WAN 2** (on a ZyWALL with two WAN Ethernet interfaces). The screen differs by the encapsulation.

The WAN 1 and WAN 2 IP addresses of a ZyWALL with multiple WAN interfaces must be on different subnets.

### WAN IP Address Assignment

Every computer on the Internet must have a unique IP address. If your networks are isolated from the Internet, for instance, only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks.

**Table 41** Private IP Address Ranges

| | | |
|---|---|---|
| 10.0.0.0 | - | 10.255.255.255 |
| 172.16.0.0 | - | 172.31.255.255 |
| 192.168.0.0 | - | 192.168.255.255 |

You can obtain your IP address from the IANA, from an ISP or have it assigned by a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, Address Allocation for Private Internets and RFC 1466, Guidelines for Management of IP Address Space.

#### DNS Server Address Assignment

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa, for instance, the IP address of www.zyxel.com is 204.217.0.2. 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 can get the DNS server addresses in the following ways.

1. 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.
2. 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.
3. You can manually enter the IP addresses of other DNS servers. These servers can be public or private. A DNS server could even be behind a remote IPSec router (see Section on page 480).

#### WAN MAC Address

Every Ethernet 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.

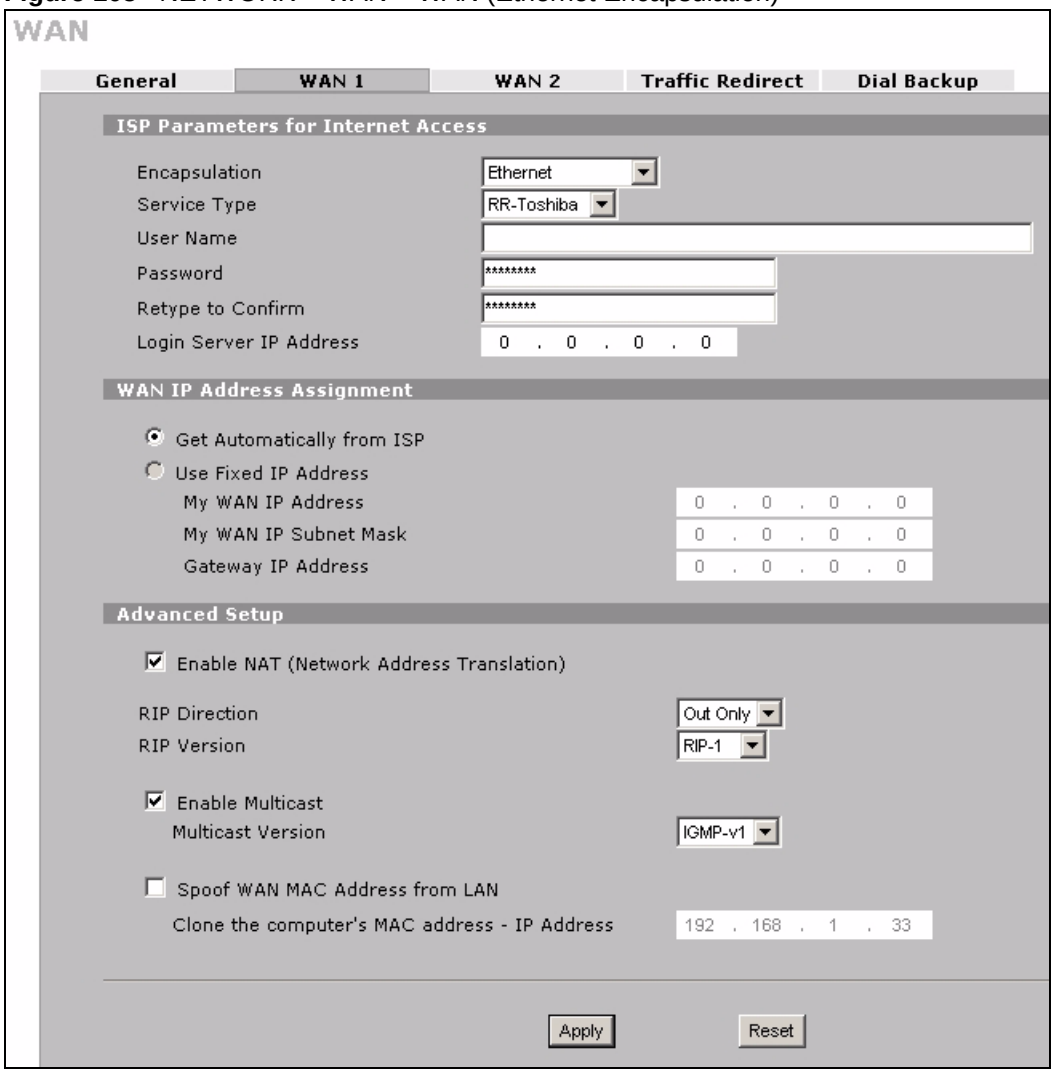
You can configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a computer on your LAN. Once it is successfully configured, the address will be copied to the "rom" file (ZyNOS configuration file). It will not change unless you change the setting or upload a different "rom" file.

### 9.3.1 WAN Ethernet Encapsulation

For ISPs (such as Telstra) that send UDP heartbeat packets to verify that the customer is still online, please create a **WAN-to-WAN/ZyWALL** firewall rule for those packets. Contact your ISP to find the correct port number.

The screen shown next is for **Ethernet** encapsulation.

**Figure 105** NETWORK > WAN > WAN (Ethernet Encapsulation)




The following table describes the labels in this screen.

**Table 42** NETWORK > WAN > WAN (Ethernet Encapsulation)

| LABEL | DESCRIPTION |
|---|---|
| ISP Parameters for Internet Access | |
| Encapsulation | You must choose the **Ethernet** option when the WAN port is used as a regular Ethernet. |
| Service Type | Choose from **Standard**, **Telstra** (RoadRunner Telstra authentication method), **RR-Manager** (Roadrunner Manager authentication method), **RR-Toshiba** (Roadrunner Toshiba authentication method) or **Telia Login**.<br>The following fields do not appear with the **Standard** service type. |
| User Name | Type the user name given to you by your ISP. |
| Password | Type the password associated with the user name above. |
| Retype to Confirm | Type your password again to make sure that you have entered is correctly. |

**Table 42** NETWORK > WAN > WAN (Ethernet Encapsulation) (continued)

| LABEL | DESCRIPTION |
|---|---|
| Login Server IP Address | Type the authentication server IP address here if your ISP gave you one.<br>This field is not available for Telia Login. |
| Login Server (Telia Login only) | Type the domain name of the Telia login server, for example login1.telia.com. |
| Relogin Every(min) (Telia Login only) | The Telia server logs the ZyWALL out if the ZyWALL does not log in periodically. Type the number of minutes from 1 to 59 (30 default) for the ZyWALL to wait between logins. |
| WAN IP Address Assignment | |
| Get automatically from ISP | 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. |
| My WAN IP Address | Enter your WAN IP address in this field if you selected **Use Fixed IP Address**. |
| My WAN IP Subnet Mask | Enter the IP subnet mask (if your ISP gave you one) in this field if you selected **Use Fixed IP Address**. |
| Gateway IP Address | Enter the gateway IP address (if your ISP gave you one) in this field if you selected **Use Fixed IP Address**. |
| Advanced Setup | |
| Enable NAT (Network Address Translation) | Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet).<br>Select this check box to enable NAT. |
| RIP Direction | RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets.<br>Choose **Both**, **None**, **In Only** or **Out Only**.<br>When set to **Both** or **Out Only**, the ZyWALL will broadcast its routing table periodically.<br>When set to **Both** or **In Only**, the ZyWALL will incorporate RIP information that it receives.<br>When set to **None**, the ZyWALL will not send any RIP packets and will ignore any RIP packets received.<br>By default, **RIP Direction** is set to **Both**. |
| RIP Version | The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyWALL sends (it recognizes both formats when receiving).<br>Choose **RIP-1**, **RIP-2B** or **RIP-2M**.<br>**RIP-1** is universally supported; but **RIP-2** carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, the **RIP Version** field is set to **RIP-1**. |
| Enable Multicast | Select this check box to turn on IGMP (Internet Group Management Protocol). IGMP is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. |

**Table 42** NETWORK > WAN > WAN (Ethernet Encapsulation) (continued)

| LABEL | DESCRIPTION |
|---|---|
| Multicast Version | Choose **None** (default), **IGMP-V1** or **IGMP-V2**. IGMP (Internet Group Management Protocol) is a session-layer protocol used to establish membership in a Multicast group – it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about inter-operability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. |
| Spoof WAN MAC Address from LAN | You can configure the WAN port's MAC address by either using the factory assigned default MAC Address or cloning the MAC address of a computer on your LAN. By default, the ZyWALL uses the factory assigned MAC Address to identify itself on the WAN.<br>Otherwise, select this option and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different ROM file. |
| Clone the computer's MAC address – IP Address | Enter the IP address of the computer on the LAN whose MAC you are cloning.<br>If you clone the MAC address of a computer on your LAN, it is recommended that you clone the MAC address prior to hooking up the WAN port. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 9.3.2 PPPoE Encapsulation

The ZyWALL supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection. The **PPPoE** option is for a dial-up connection using PPPoE.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example RADIUS).

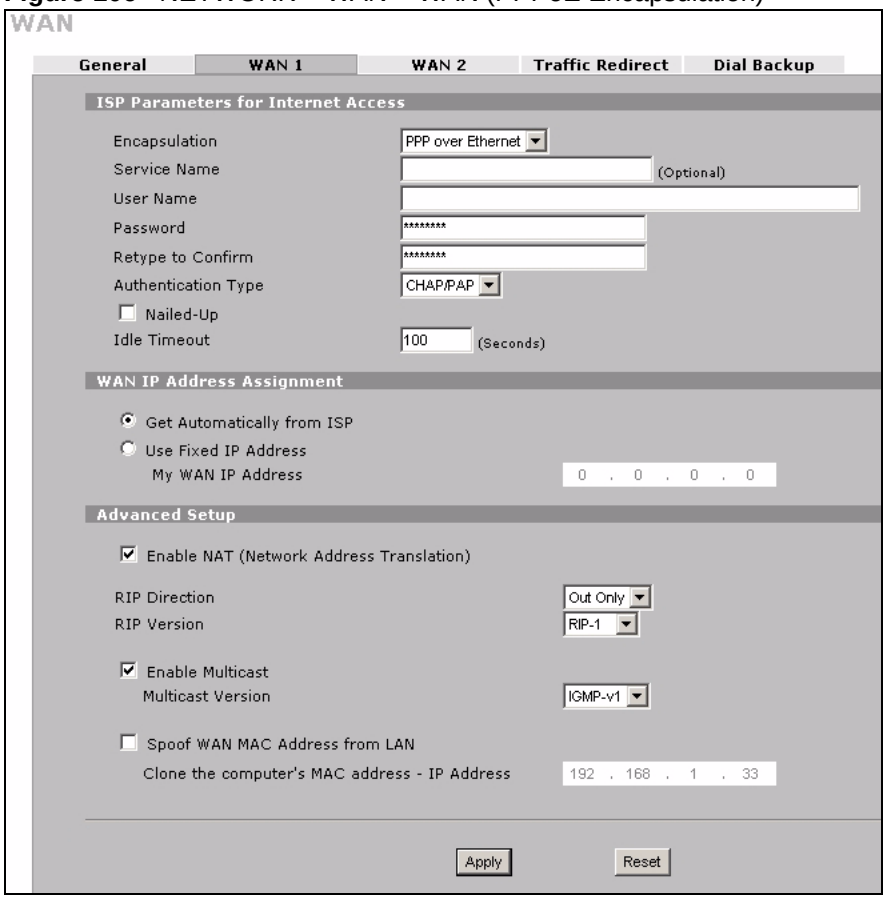
One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the ZyWALL (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the ZyWALL does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

The screen shown next is for **PPPoE** encapsulation.

**Figure 106** NETWORK > WAN > WAN (PPPoE Encapsulation)




The following table describes the labels in this screen.

**Table 43** NETWORK > WAN > WAN (PPPoE Encapsulation)

| LABEL | DESCRIPTION |
|---|---|
| ISP Parameters for Internet Access | |
| Encapsulation | Select **PPPoE** for a dial-up connection using PPPoE. |
| Service Name | Type the PPPoE service name provided to you by your ISP. PPPoE uses a service name to identify and reach the PPPoE server. |
| User Name | Type the user name given to you by your ISP. |
| Password | Type the password associated with the user name above. |
| Retype to Confirm | Type your password again to make sure that you have entered is correctly. |
| 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>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. |

**Table 43** NETWORK > WAN > WAN (PPPoE Encapsulation) (continued)

| LABEL | DESCRIPTION |
|---|---|
| Nailed-Up | Select **Nailed-Up** if you do not want the connection to time out. |
| Idle Timeout | This value specifies the time in seconds that elapses before the ZyWALL automatically disconnects from the PPPoE server. |
| WAN IP Address Assignment | |
| Get automatically from ISP | 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. |
| My WAN IP Address | Enter your WAN IP address in this field if you selected **Use Fixed IP Address.** |
| Advanced Setup | |
| Enable NAT (Network Address Translation) | Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet).<br>Select this checkbox to enable NAT.<br>For more information about NAT see Chapter 22 on page 435. |
| RIP Direction | RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets.<br>Choose **Both**, **None**, **In Only** or **Out Only**.<br>When set to **Both** or **Out Only**, the ZyWALL will broadcast its routing table periodically.<br>When set to **Both** or **In Only**, the ZyWALL will incorporate RIP information that it receives.<br>When set to **None**, the ZyWALL will not send any RIP packets and will ignore any RIP packets received.<br>By default, **RIP Direction** is set to **Both**. |
| RIP Version | The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyWALL sends (it recognizes both formats when receiving).<br>Choose **RIP-1**, **RIP-2B** or **RIP-2M**.<br>**RIP-1** is universally supported; but **RIP-2** carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, the **RIP Version** field is set to **RIP-1**. |
| Enable Multicast | Select this check box to turn on IGMP (Internet Group Management Protocol). IGMP is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. |
| Multicast Version | Choose **None** (default), **IGMP-V1** or **IGMP-V2**. IGMP (Internet Group Management Protocol) is a session-layer protocol used to establish membership in a Multicast group – it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about inter-operability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. |

**Table 43** NETWORK > WAN > WAN (PPPoE Encapsulation) (continued)

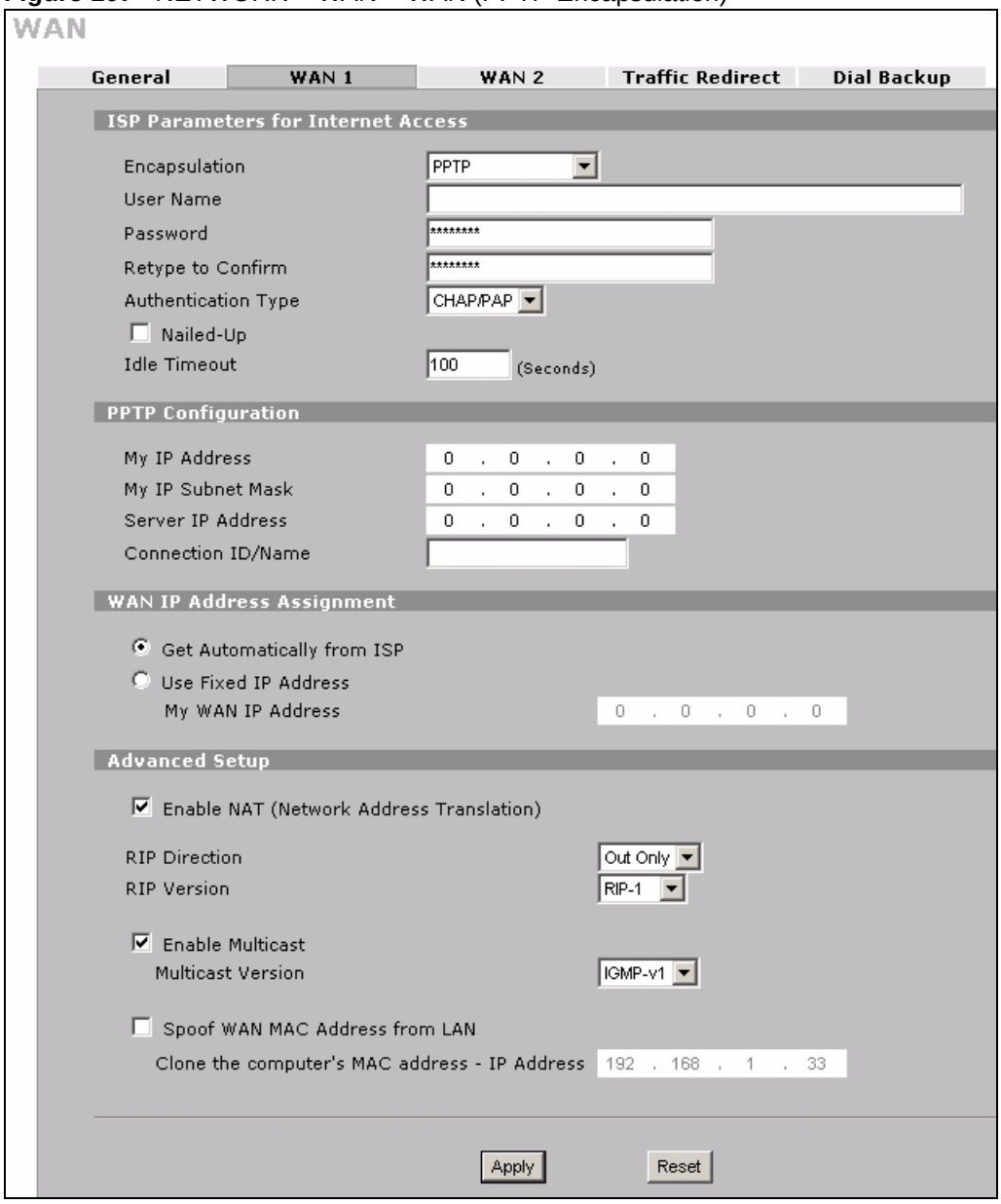
| LABEL | DESCRIPTION |
|---|---|
| Spoof WAN MAC Address from LAN | You can configure the WAN port's MAC address by either using the factory assigned default MAC Address or cloning the MAC address of a computer on your LAN. By default, the ZyWALL uses the factory assigned MAC Address to identify itself on the WAN.<br>Otherwise, select this option and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different ROM file. |
| Clone the computer's MAC address – IP Address | Enter the IP address of the computer on the LAN whose MAC you are cloning.<br>If you clone the MAC address of a computer on your LAN, it is recommended that you clone the MAC address prior to hooking up the WAN port. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 9.3.3 PPTP Encapsulation

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks.

PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet. The screen shown next is for **PPTP** encapsulation.

**Figure 107** NETWORK > WAN > WAN (PPTP Encapsulation)




The following table describes the labels in this screen.

**Table 44** NETWORK > WAN > WAN (PPTP Encapsulation)

| LABEL | DESCRIPTION |
|---|---|
| ISP Parameters for Internet Access | |
| Encapsulation | Set the encapsulation method to **PPTP**. The ZyWALL supports only one PPTP server connection at any given time. To configure a PPTP client, you must configure the **User Name** and **Password** fields for a PPP connection and the PPTP parameters for a PPTP connection. |
| User Name | Type the user name given to you by your ISP. |
| Password | Type the password associated with the user name above. |
| Retype to Confirm | Type your password again to make sure that you have entered it correctly. |

**Table 44** NETWORK > WAN > WAN (PPTP Encapsulation) (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>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. |
| Nailed-up | Select **Nailed-Up** if you do not want the connection to time out. |
| Idle Timeout | This value specifies the time in seconds that elapses before the ZyWALL automatically disconnects from the PPTP server. |
| PPTP Configuration | |
| My IP Address | Type the (static) IP address assigned to you by your ISP. |
| My IP Subnet Mask | Your ZyWALL will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyWALL. |
| Server IP Address | Type the IP address of the PPTP server. |
| Connection ID/ Name | Type your identification name for the PPTP server. |
| WAN IP Address Assignment | |
| Get automatically from ISP | 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. |
| My WAN IP Address | Enter your WAN IP address in this field if you selected **Use Fixed IP Address**. |
| Advanced Setup | |
| Enable NAT (Network Address Translation) | Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet).<br>Select this checkbox to enable NAT.<br>For more information about NAT see Chapter 22 on page 435. |
| RIP Direction | RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets.<br>Choose **Both**, **None**, **In Only** or **Out Only**.<br>When set to **Both** or **Out Only**, the ZyWALL will broadcast its routing table periodically.<br>When set to **Both** or **In Only**, the ZyWALL will incorporate RIP information that it receives.<br>When set to **None**, the ZyWALL will not send any RIP packets and will ignore any RIP packets received.<br>By default, **RIP Direction** is set to **Both**. |

**Table 44** NETWORK > WAN > WAN (PPTP Encapsulation) (continued)

| LABEL | DESCRIPTION |
|---|---|
| RIP Version | The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyWALL sends (it recognizes both formats when receiving).<br><br>Choose **RIP-1**, **RIP-2B** or **RIP-2M**.<br><br>**RIP-1** is universally supported; but **RIP-2** carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, the **RIP Version** field is set to **RIP-1**. |
| Enable Multicast | Select this check box to turn on IGMP (Internet Group Management Protocol). IGMP is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. |
| Multicast Version | Choose **None** (default), **IGMP-V1** or **IGMP-V2**. IGMP (Internet Group Management Protocol) is a session-layer protocol used to establish membership in a Multicast group – it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about inter-operability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. |
| Spoof WAN MAC Address from LAN | You can configure the WAN port's MAC address by either using the factory assigned default MAC Address or cloning the MAC address of a computer on your LAN. By default, the ZyWALL uses the factory assigned MAC Address to identify itself on the WAN.<br>Otherwise, select this option and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different ROM file. |
| Clone the computer's MAC address – IP Address | Enter the IP address of the computer on the LAN whose MAC you are cloning.<br>If you clone the MAC address of a computer on your LAN, it is recommended that you clone the MAC address prior to hooking up the WAN port. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 9.4 The 3G (WAN2) Screen

Use this screen to configure your 3G (WAN2) settings.

After you insert a 3G card in the ZyWALL 5, the 3G connection becomes WAN 2. Refer to Section 55.1 on page 773 for the type of 3G cards that you can use in the ZyWALL along with the corresponding supported features.

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

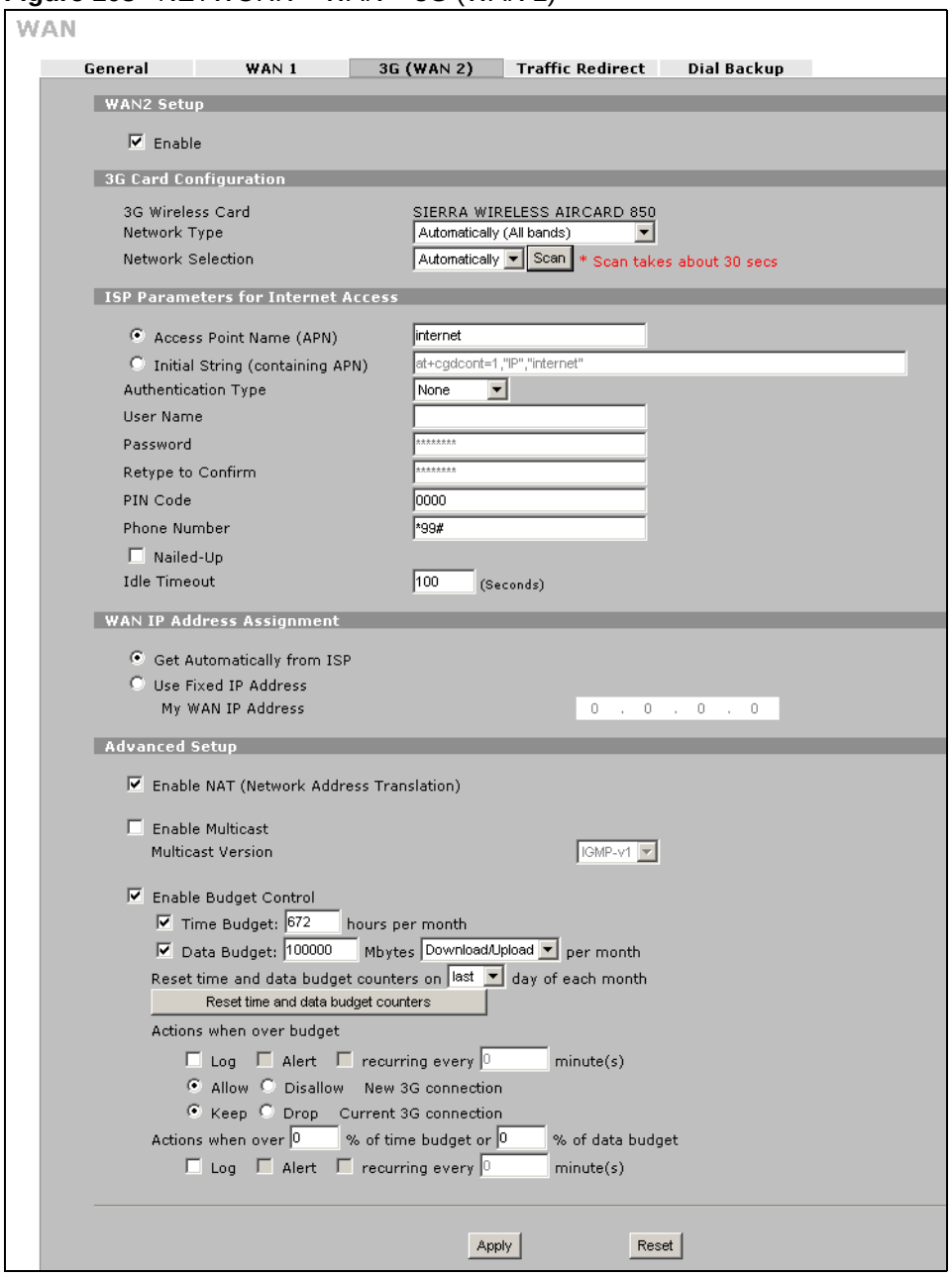
If the signal strength of a 3G network is too low, the 3G card may switch to an available 2.5G or 2.75G network. Refer to Section 9.8 on page 204 for a comparison between 2G, 2.5G, 2.75G and 3G wireless technologies.

Turn the ZyWALL off before you install or remove the 3G card.

The WAN 1 and WAN 2 IP addresses of a ZyWALL with multiple WAN interfaces must be on different subnets.

To change your ZyWALL 5's 3G WAN settings, click **NETWORK** > **WAN** > **3G (WAN 2)** or **NETWORK** > **WIRELESS** > **3G (WAN2)**.

**Figure 108** NETWORK > WAN > 3G (WAN 2)




The following table describes the labels in this screen.

**Table 45** NETWORK > WAN > 3G (WAN 2)

| LABEL | DESCRIPTION |
|---|---|
| Enable | Select this option to enable WAN 2. |
| 3G Card Configuration | The fields below display only when you enable WAN 2. |
| 3G Wireless Card | This displays the manufacturer and model name of your 3G card if you inserted one in the ZyWALL. Otherwise, it displays **Not Installed**. |

**Table 45** NETWORK > WAN > 3G (WAN 2) (continued)

| LABEL | DESCRIPTION |
|---|---|
| Network Type | Select the type of the network (**UMTS/HSDPA only**, **GPRS/EDGE only**, **GSM all** or **WCDMA all**) to which you want the card to connect. See Table 49 on page 204 for more information. Otherwise, select **Automatically** to have the card connect to an available network using the default settings on the 3G card.<br>The types of the network vary depending on the 3G card you inserted.<br>This setting is saved to the flash of your 3G card. |
| Network Selection | Select a service provider to which you want the card to connect. Otherwise, select **Automatically** to have the ZyWALL use the default settings on the 3G card and connect to your service provider's base station.<br>This shows **Automatically** only by default. Click **Scan** to have the ZyWALL search for and display the available service providers.<br>This field resets to the default setting (**Automatically**) if the ZyWALL restarts. |
| ISP Parameters for Internet Access | |
| Access Point Name (APN) | This field displays with a GSM or HSDPA 3G card. Enter the APN (Access Point Name) provided by 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>You can enter up to 31 ASCII printable characters. Spaces are allowed. |
| Initial String (containing APN) | Select this option and enter the initial string and APN if you know how to configure it or your ISP provides a string, which would include the APN, to initialize the 3G card.<br>You can enter up to 72 ASCII printable characters. Spaces are allowed.<br>This field is available only when you insert a GSM 3G card. |
| 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>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. |
| User Name | Type the user name (of up to 31 ASCII printable characters) given to you by your service provider. |
| Password | Type the password (of up to 31 ASCII printable characters) associated with the user name above. |
| Retype to Confirm | Type your password again to make sure that you have entered is correctly. |
| 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>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>If your ISP disabled PIN code authentication, enter an arbitrary number. |
| Phone Number | Enter the phone number (dial string) used to dial up a connection to your service provider's base station. Your ISP should provide the phone number.<br>For example, *99# is the dial string to establish a GPRS or 3G connection in Taiwan. |
| Nailed-Up | Select **Nailed-Up** if you do not want the connection to time out. |

**Table 45** NETWORK > WAN > 3G (WAN 2) (continued)

| LABEL | DESCRIPTION |
|---|---|
| Idle Timeout | This value specifies the time in seconds that elapses before the ZyWALL automatically disconnects from the ISP. |
| WAN IP Address Assignment | |
| Get automatically from ISP | 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. |
| My WAN IP Address | Enter your WAN IP address in this field if you selected **Use Fixed IP Address**. |
| Advanced Setup | |
| Enable NAT (Network Address Translation) | Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet).<br>Select this checkbox to enable NAT.<br>For more information about NAT see Chapter 22 on page 435. |
| Enable Multicast | Select this check box to turn on IGMP (Internet Group Management Protocol). IGMP is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. |
| Multicast Version | Choose **None** (default), **IGMP-V1** or **IGMP-V2**. IGMP (Internet Group Management Protocol) is a session-layer protocol used to establish membership in a Multicast group – it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about inter-operability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. |
| Enable Budget Control | Select this check box to set a monthly limit for the user account of the installed 3G card. You must insert a 3G card before you enable budget control on the ZyWALL.<br>You can set a limit on the total traffic and/or call time. The ZyWALL takes the actions you specified when a limit is exceeded during the month. |
| Time Budget | Select this check box and specify the amount of time (in hours) that the 3G connection can be used within one month.<br>If you change the value after you configure and enable budget control, the ZyWALL resets the statistics. |
| Data Budget | Select this check box and specify how much downstream and/or upstream data (in Mega bytes) can be transmitted via the 3G connection within one month.<br>Select **Download** to set a limit on the downstream traffic (from the ISP to the ZyWALL).<br>Select **Upload** to set a limit on the upstream traffic (from the ZyWALL to the ISP).<br>Select **Download/Upload** to set a limit on the total traffic in both directions.<br>If you change the value after you configure and enable budget control, the ZyWALL resets the statistics. |
| Reset time and data budget counters on | Select the date on which the ZyWALL resets the budget every month. If the date you selected is not available in a month, such as 30th or 31th, the ZyWALL resets the budget on the last day of the month. |
| Reset time and data budget counters | This button is available only when you enable budget control in this screen.<br>Click this button to reset the time and data budgets immediately. The count starts over with the 3G connection's full configured monthly time and data budgets. This does not affect the normal monthly budget restart. |

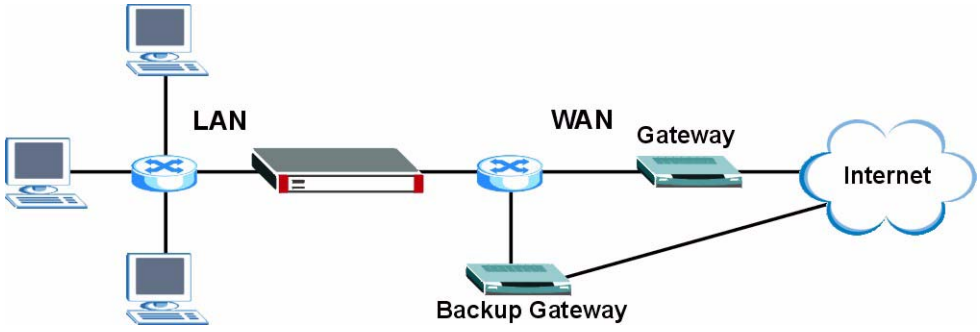
**Table 45** NETWORK > WAN > 3G (WAN 2) (continued)

| LABEL | DESCRIPTION |
|---|---|
| Actions when over budget | Specify the actions the ZyWALL takes when the time or data limit is exceeded.<br>Select **Log** to create a log.<br>Select **Alert** to create an alert. This option is available only when you select **Log**.<br>If you select **Log**, you can also select **recurring every** to have the ZyWALL send a log (and alert if selected) for this event periodically. Specify how often (from 1 to 65535 minutes) to send the log (and alert if selected).<br>Select **Allow** to permit new 3G connections or **Disallow** to drop/block new 3G connections.<br>Select **Keep** to maintain the existing 3G connection or **Drop** to disconnect it.<br>You cannot select **Allow** and **Drop** at the same time.<br>If you select **Disallow** and **Keep**, the ZyWALL allows you to transmit data using the current connection, but you cannot build a new connection if the existing connection is disconnected. |
| Actions when over % of time budget or % of data budget | Specify the actions the ZyWALL takes when the specified percentage of time budget or data limit is exceeded. Enter a number from 1 to 99 in the percentage fields. If you change the value after you configure and enable budget control, the ZyWALL resets the statistics.<br>Select **Log** to create a log.<br>Select **Alert** to create an alert. This option is available only when you select **Log**.<br>If you select **Log**, you can also select **recurring every** to have the ZyWALL send a log (and alert if selected) for this event periodically. Specify how often (from 1 to 65535 minutes) to send the log (and alert if selected). |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 9.5 The Traffic Redirect Screen

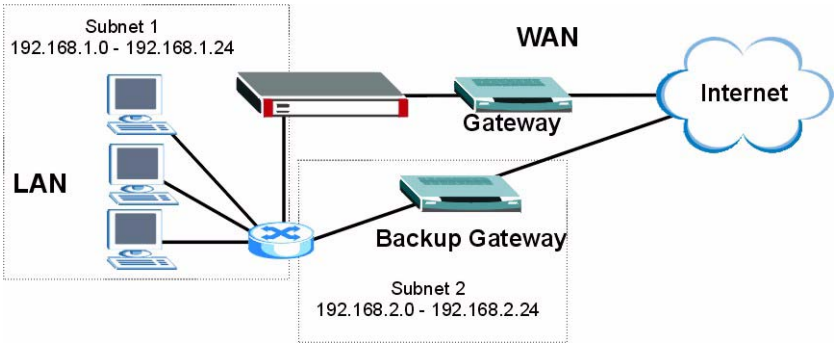
Traffic redirect forwards WAN traffic to a backup gateway when the ZyWALL cannot connect to the Internet through its normal gateway. Connect the backup gateway on the WAN so that the ZyWALL still provides firewall protection for the LAN.

**Figure 109** Traffic Redirect WAN Setup




IP alias allows you to avoid triangle route security issues when the backup gateway is connected to the LAN or DMZ. Use IP alias to configure the LAN into two or three logical networks with the ZyWALL itself as the gateway for each LAN network. Put the protected LAN in one subnet (Subnet 1 in the following figure) and the backup gateway in another subnet (Subnet 2). Configure a LAN to LAN/ZyWALL firewall rule that forwards packets from the protected LAN (Subnet 1) to the backup gateway (Subnet 2).

**Figure 110** Traffic Redirect LAN Setup

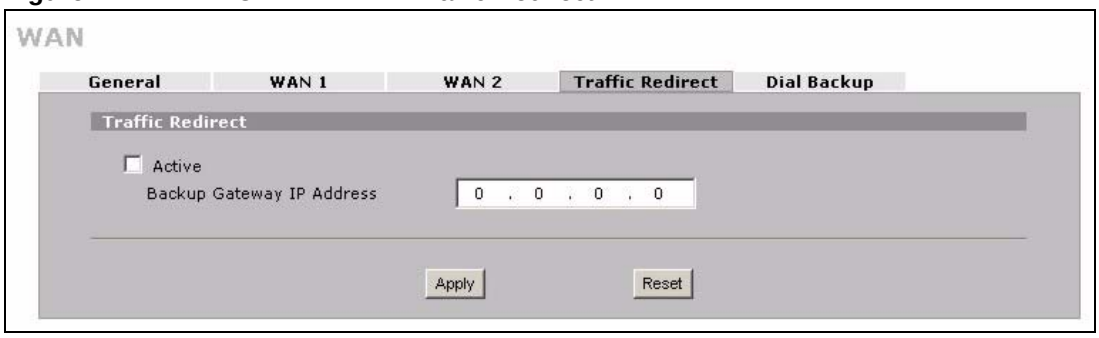



## 9.6 Configuring the Traffic Redirect Screen

To change your ZyWALL's traffic redirect settings, click **NETWORK** > **WAN** > **Traffic Redirect**. The screen appears as shown.

For the ZyWALL 5, if the traffic redirect feature does not work after you configure the ZyWALL's traffic redirect settings in the **Traffic Redirect** screen, you may need to turn on the WAN ping check by entering `sys rn pingDrop` in the command interpreter. See the CLI Reference Guide.

**Figure 111** NETWORK > WAN > Traffic Redirect




The following table describes the labels in this screen.

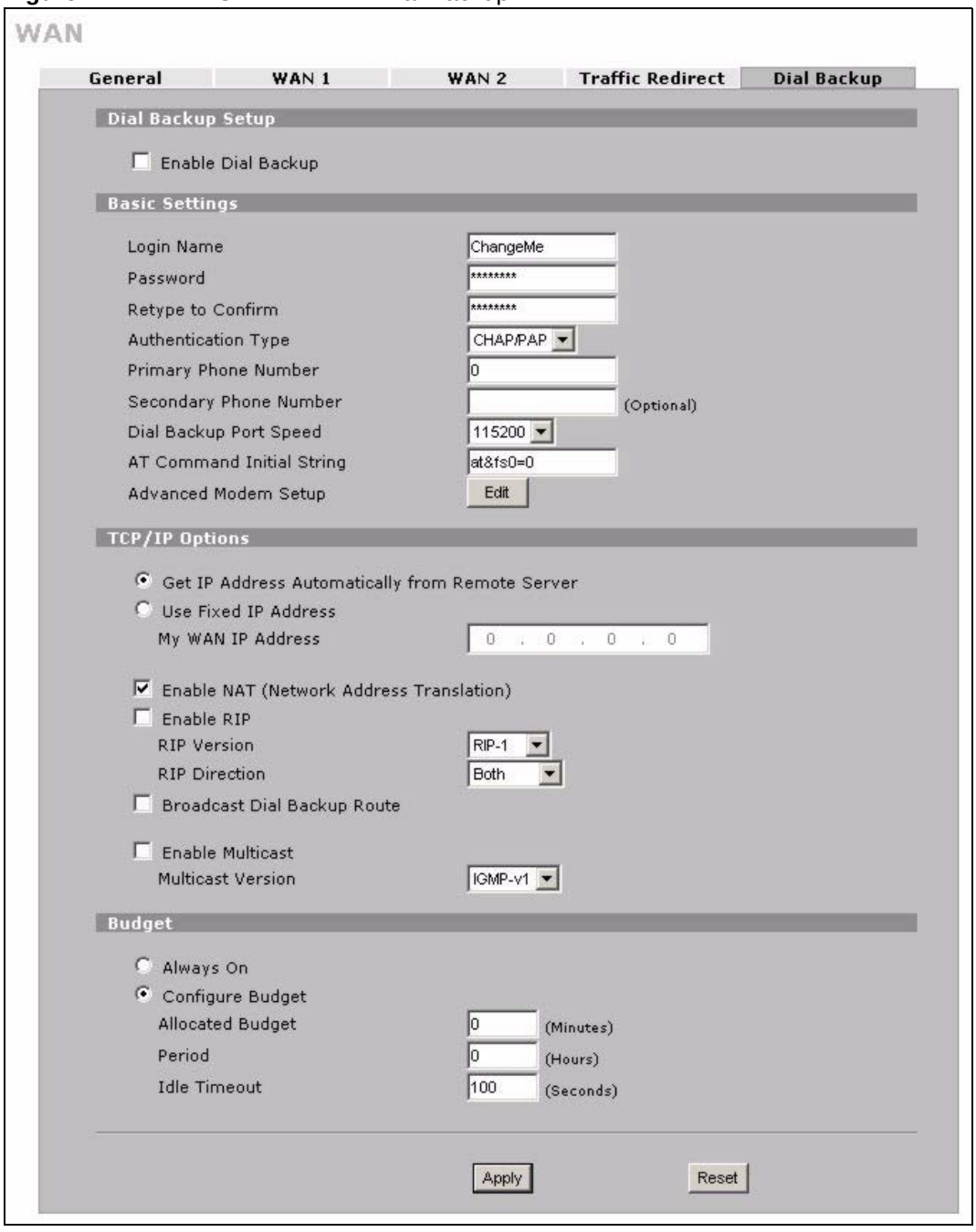
**Table 46** NETWORK > WAN > Traffic Redirect

| LABEL | DESCRIPTION |
|---|---|
| Active | Select this check box to have the ZyWALL use traffic redirect if the normal WAN connection goes down. |
| Backup Gateway IP Address | Type the IP address of your backup gateway in dotted decimal notation. The ZyWALL automatically forwards traffic to this IP address if the ZyWALL's Internet connection terminates. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# 9.7 The Dial Backup Screen

Click **NETWORK** > **WAN** > **Dial Backup** to display the **Dial Backup** screen. Use this screen to configure the backup WAN dial-up connection. Not all fields are available on all models.

**Figure 112** NETWORK > WAN > Dial Backup



The following table describes the labels in this screen.

**Table 47** NETWORK > WAN > Dial Backup

| LABEL | DESCRIPTION |
|---|---|
| Dial Backup Setup | |
| Enable Dial Backup | Select this check box to turn on dial backup. |
| Basic Settings | |
| Login Name | Type the login name assigned by your ISP. |
| Password | Type the password assigned by your ISP. |
| Retype to Confirm | Type your password again to make sure that you have entered is correctly. |
| 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. |
| Primary/ Secondary Phone Number | Type the first (primary) phone number from the ISP for this remote node. If the Primary Phone number is busy or does not answer, your ZyWALL dials the Secondary Phone number if available. Some areas require dialing the pound sign # before the phone number for local calls. Include a # symbol at the beginning of the phone numbers as required. |
| Dial Backup Port Speed | Use the drop-down list box to select the speed of the connection between the Dial Backup port and the external device. Available speeds are: **9600**, **19200**, **38400**, **57600**, **115200** or **230400** bps. |
| AT Command Initial String | Type the AT command string to initialize the WAN device. Consult the manual of your WAN device connected to your Dial Backup port for specific AT commands. |
| Advanced Modem Setup | Click **Edit** to display the **Advanced Setup** screen and edit the details of your dial backup setup. |
| TCP/IP Options | |
| Get IP Address Automatically from Remote Server | Type the login name assigned by your ISP for this remote node. |
| Used Fixed IP Address | Select this check box if your ISP assigned you a fixed IP address, then enter the IP address in the following field. |
| My WAN IP Address | Leave the field set to 0.0.0.0 (default) to have the ISP or other remote router dynamically (automatically) assign your WAN IP address if you do not know it. Type your WAN IP address here if you know it (static). This is the address assigned to your local ZyWALL, not the remote router. |
| Enable NAT (Network Address Translation) | Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network to a different IP address known within another network.<br>Select the check box to enable NAT. Clear the check box to disable NAT so the ZyWALL does not perform any NAT mapping for the dial backup connection. |
| Enable RIP | Select this check box to turn on RIP (Routing Information Protocol), which allows a router to exchange routing information with other routers. |

**Table 47** NETWORK > WAN > Dial Backup (continued)

| LABEL | DESCRIPTION |
|---|---|
| RIP Version | The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyWALL sends (it recognizes both formats when receiving).<br>Choose **RIP-1**, **RIP-2B** or **RIP-2M**.<br>**RIP-1** is universally supported; but **RIP-2** carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. |
| RIP Direction | RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets.<br>Choose **Both**, **In Only** or **Out Only**.<br>When set to **Both** or **Out Only**, the ZyWALL will broadcast its routing table periodically.<br>When set to **Both** or **In Only**, the ZyWALL will incorporate RIP information that it receives. |
| Broadcast Dial Backup Route | Select this check box to forward the backup route broadcasts to the WAN. |
| Enable Multicast | Select this check box to turn on IGMP (Internet Group Management Protocol). IGMP is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. |
| Multicast Version | Select **IGMP-v1** or **IGMP-v2**. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see *sections 4* and *5* of *RFC 2236*. |
| Budget | |
| Always On | Select this check box to have the dial backup connection on all of the time. |
| Configure Budget | Select this check box to have the dial backup connection on during the time that you select. |
| Allocated Budget | Type the amount of time (in minutes) that the dial backup connection can be used during the time configured in the **Period** field. Set an amount that is less than the time period configured in the **Period** field. |
| Period | Type the time period (in hours) for how often the budget should be reset. For example, to allow calls to this remote node for a maximum of 10 minutes every hour, set the **Allocated Budget** to 10 (minutes) and the **Period** to 1 (hour). |
| Idle Timeout | Type the number of seconds of idle time (when there is no traffic from the ZyWALL to the remote node) for the ZyWALL to wait before it automatically disconnects the dial backup connection. This option applies only when the ZyWALL initiates the call. The dial backup connection never times out if you set this field to "0" (it is the same as selecting **Always On**). |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 9.7.1 The Advanced Modem Setup Screen

Click the **Edit** button in the **Dial Backup** screen to display the **Advanced Setup** screen. Use this screen to configure your advanced modem setup settings for the Dial Backup screen.

### 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.

For ISDN lines, there are many more protocols and operational modes. Please consult the documentation of your TA. You may need additional commands in both Dial and Init strings.

### 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

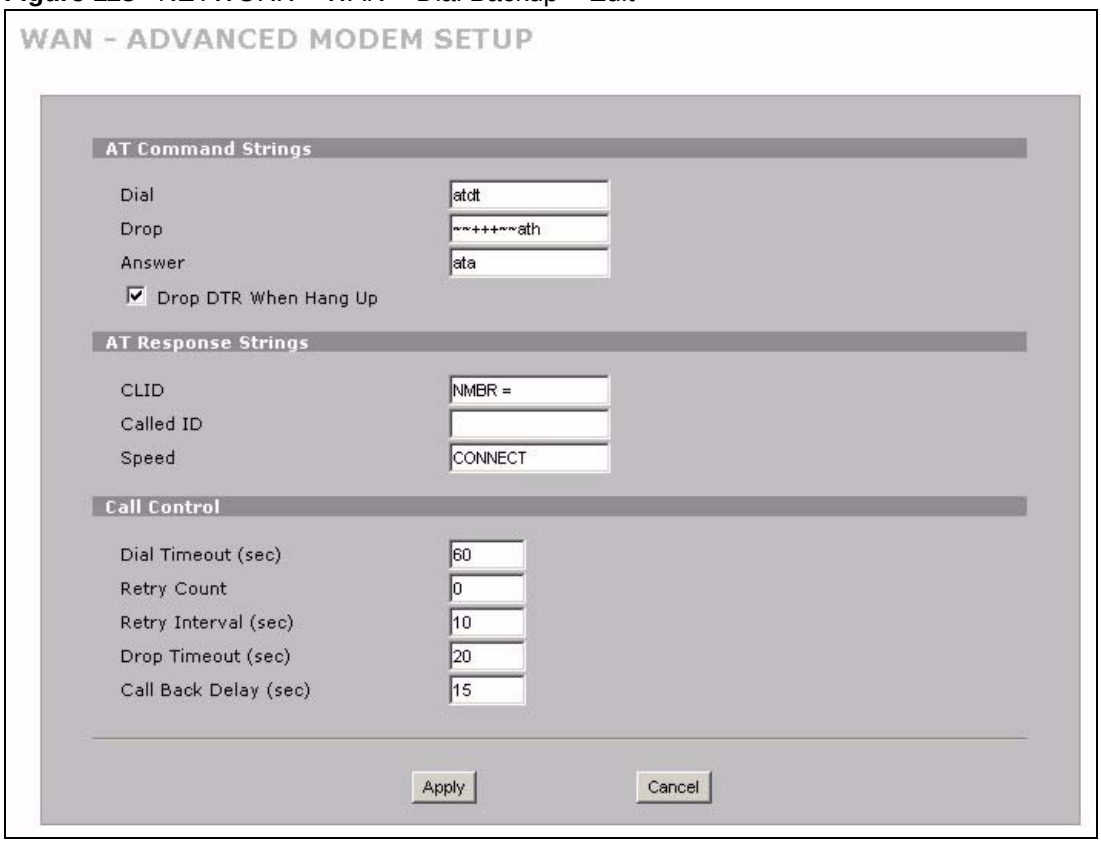
The response strings tell the ZyWALL the tags, or labels, immediately preceding the various call parameters sent from the WAN device. The response strings have not been standardized; please consult the documentation of your WAN device to find the correct tags.

## 9.7.2 Configuring the Advanced Modem Setup Screen

Click the **Edit** button in the **Dial Backup** screen to display the **Advanced Setup** screen.

Consult the manual of your WAN device connected to your dial backup port for specific AT commands.

**Figure 113** NETWORK > WAN > Dial Backup > Edit




The following table describes the labels in this screen.

**Table 48** NETWORK > WAN > Dial Backup > Edit

| LABEL | DESCRIPTION |
|---|---|
| AT Command Strings | |
| Dial | Type the AT Command string to make a call. |
| Drop | Type the AT Command string to drop a call. "~" represents a one second wait, for example, "~~~+++~~ath" can be used if your modem has a slow response time. |
| Answer | Type the AT Command string to answer a call. |
| Drop DTR When Hang Up | Select this check box to have the ZyWALL drop the DTR (Data Terminal Ready) signal after the "AT Command String: Drop" is sent out. |
| AT Response Strings | |
| CLID | Type the keyword that precedes the CLID (Calling Line Identification) in the AT response string. This lets the ZyWALL capture the CLID in the AT response string that comes from the WAN device. CLID is required for CLID authentication. |
| Called ID | Type the keyword preceding the dialed number. |
| Speed | Type the keyword preceding the connection speed. |
| Call Control | |
| Dial Timeout (sec) | Type a number of seconds for the ZyWALL to try to set up an outgoing call before timing out (stopping). |
| Retry Count | Type a number of times for the ZyWALL to retry a busy or no-answer phone number before blacklisting the number. |

**Table 48** NETWORK > WAN > Dial Backup > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Retry Interval (sec) | Type a number of seconds for the ZyWALL to wait before trying another call after a call has failed. This applies before a phone number is blacklisted. |
| Drop Timeout (sec) | Type the number of seconds for the ZyWALL to wait before dropping the DTR signal if it does not receive a positive disconnect confirmation. |
| Call Back Delay (sec) | Type a number of seconds for the ZyWALL to wait between dropping a callback request call and dialing the corresponding callback call. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving. |

## 9.8 WAN Technical Reference

## 3G Comparison Table

See the following table for a comparison between 2G, 2.5G, 2.75G and 3G wireless technologies.

**Table 49** 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 ↓ Fast |
| 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>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. | | |

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

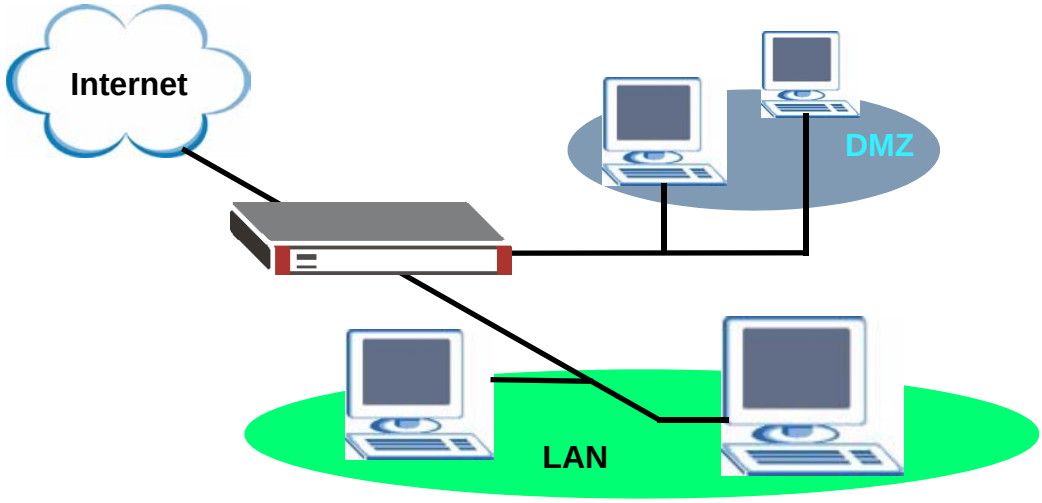
# 10

# DMZ Screens

## 10.1 Overview

The DeMilitarized Zone (DMZ) provides a way for public servers (Web, e-mail, FTP, etc.) to be visible to the outside world (while still being protected from DoS (Denial of Service) attacks such as SYN flooding and Ping of Death). These public servers can also still be accessed from the secure LAN.

**Figure 114** DMZ Overview




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

- Use the **DMZ** screen (Section 10.2 on page 210) to configure TCP/IP, DHCP, IP/MAC binding and NetBIOS settings on the DMZ.
- Use the **Static DHCP** screen (Section 10.3 on page 213) to configure the IP addresses assigned to devices in the DMZ by DHCP.
- Use the **IP Alias** screen (Section 10.4 on page 214) to configure IP alias settings on the ZyWALL's DMZ ports.
- Use the **Port Roles** screen (Section 10.5 on page 216) to configure DMZ ports on the ZyWALL.

## 10.1.2 What You Need To Know About DMZ

### DMZ and Security

It is highly recommended that you connect all of your public servers to the DMZ port(s).

It is also highly recommended that you keep all sensitive information off of the public servers connected to the DMZ port. Store sensitive information on LAN computers.

### DMZ and Firewall Rules

By default the firewall allows traffic between the WAN and the DMZ, traffic from the DMZ to the LAN is denied, and traffic from the LAN to the DMZ is allowed. Internet users can have access to host servers on the DMZ but no access to the LAN, unless special filter rules allowing access were configured by the administrator or the user is an authorized remote user.

### DMZ and NAT

See Chapter 22 on page 435 for an overview of NAT.

If you do not configure SUA NAT or any full feature NAT mapping rules for the public IP addresses on the DMZ, the ZyWALL will route traffic to the public IP addresses on the DMZ without performing NAT. This may be useful for hosting servers for NAT unfriendly applications.

If the DMZ computers use private IP addresses, use NAT if you want to make them publicly accessible.

### DHCP

See Section 7.1.2 on page 150 for more information on DHCP.

Like the LAN, the ZyWALL can also assign TCP/IP configuration via DHCP to computers connected to the DMZ ports.

### IP alias

See Section 7.4 on page 156 for more information on IP alias.

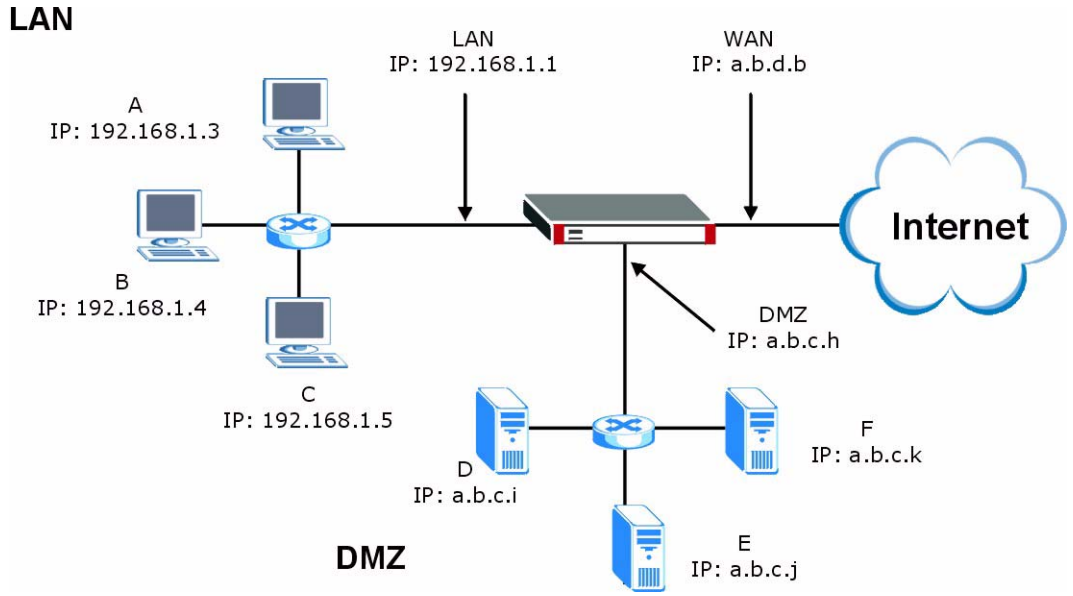
### Port roles

See Section 7.5 on page 158 for more information on port roles.

## 10.1.3 DMZ Public IP Address Example

The following figure shows a simple network setup with public IP addresses on the WAN and DMZ and private IP addresses on the LAN. Lower case letters represent public IP addresses (like a.b.c.d for example). The LAN port and connected computers (A through C) use private IP addresses that are in one subnet. The DMZ port and connected servers (D through F) use public IP addresses that are in another subnet. The public IP addresses of the DMZ and WAN ports are in separate subnets.

**Figure 115** DMZ Public Address Example

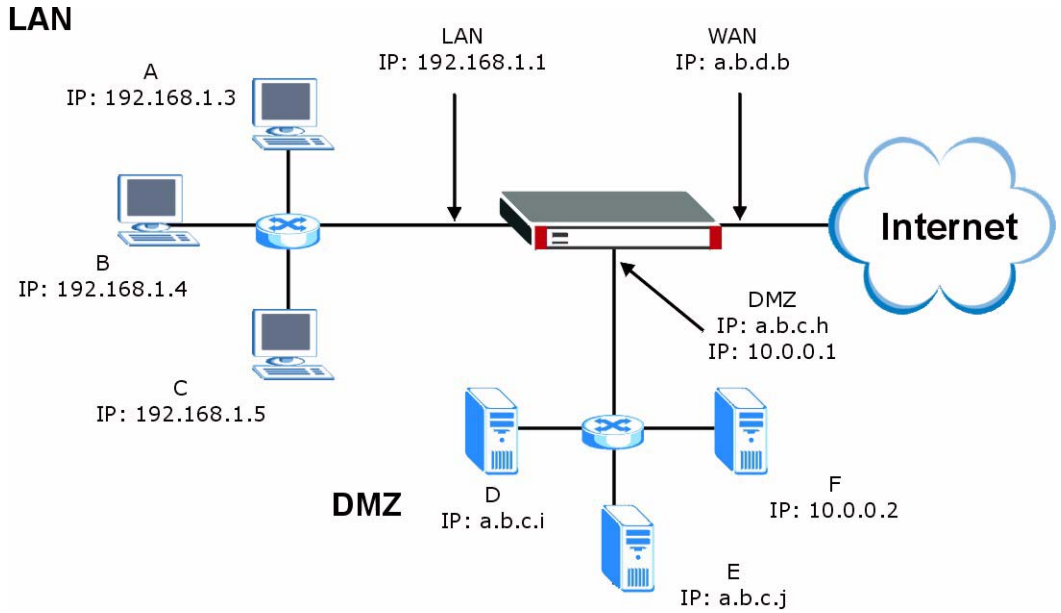



## 10.1.4 DMZ Private and Public IP Address Example

The following figure shows a network setup with both private and public IP addresses on the DMZ. Lower case letters represent public IP addresses (like a.b.c.d for example). The LAN port and connected computers (A through C) use private IP addresses that are in one subnet. The DMZ port and server F use private IP addresses that are in one subnet. The private IP addresses of the LAN and DMZ are on separate subnets. The DMZ port and connected servers (D and E) use public IP addresses that are in one subnet. The public IP addresses of the DMZ and WAN are on separate subnets.

Configure one subnet (either the public or the private) in the **Network > DMZ** screen (see Figure 117 on page 211) and configure the other subnet in the **Network > DMZ > IP Alias** screen (see Figure 119 on page 215) to use this kind of network setup. You also need to configure NAT for the private DMZ IP addresses.

**Figure 116** DMZ Private and Public Address Example



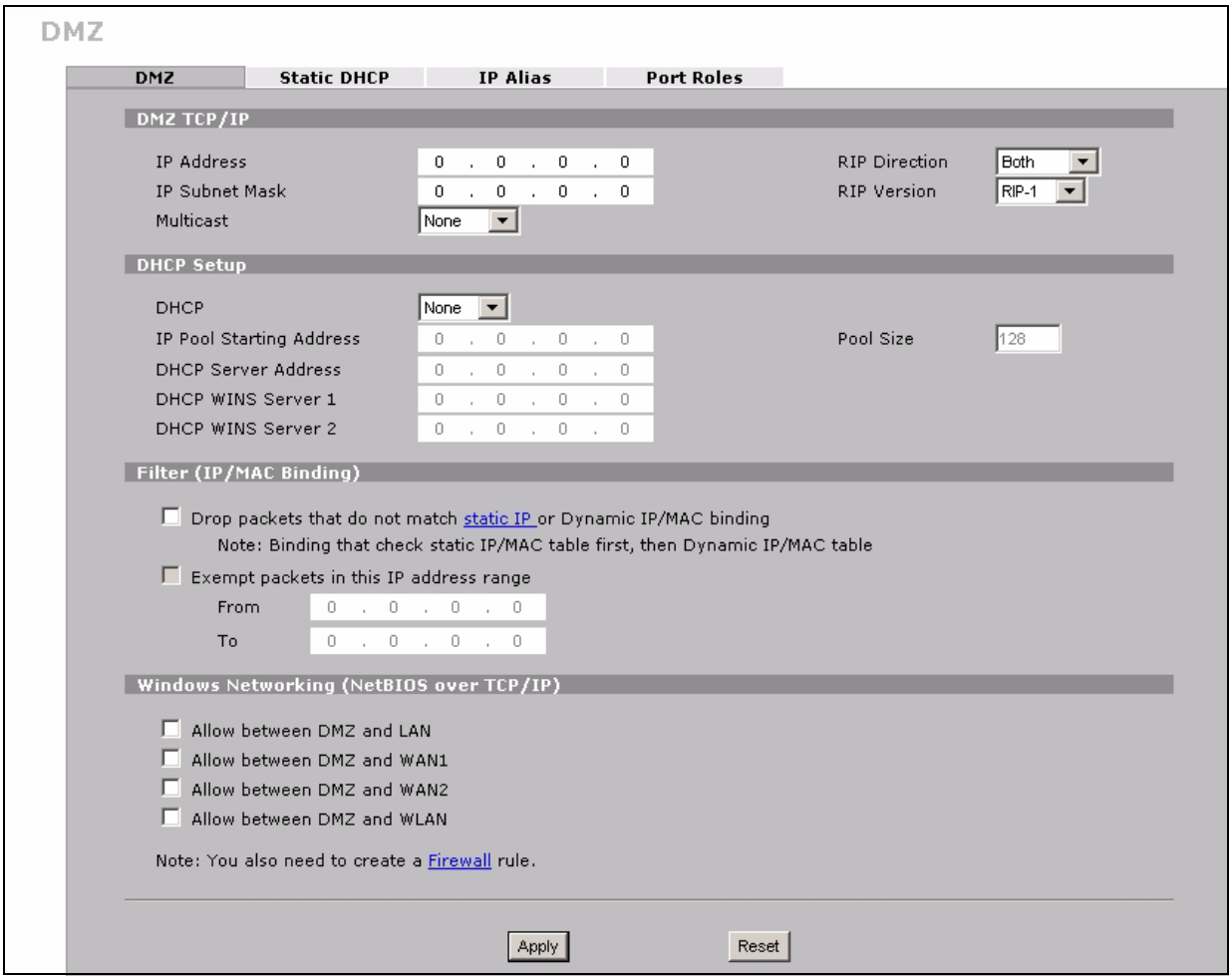

## 10.2 The DMZ Screen

Use this screen to configure TCP/IP, DHCP, IP/MAC binding and NetBIOS settings on the DMZ.

The DMZ and the connected computers can have private or public IP addresses. When the DMZ uses public IP addresses, the WAN and DMZ ports must use public IP addresses that are on separate subnets. See Appendix E on page 817 for information on IP subnetting.

From the main menu, click **NETWORK** > **DMZ** to open the **DMZ** screen. The screen appears as shown next.

**Figure 117** NETWORK > DMZ




The following table describes the labels in this screen.

**Table 50** NETWORK > DMZ

| LABEL | DESCRIPTION |
|---|---|
| DMZ TCP/IP | |
| IP Address | Type the IP address of your ZyWALL's DMZ port in dotted decimal notation.<br><br>Note: Make sure the IP addresses of the LAN, WAN, WLAN and DMZ are on separate subnets. |
| IP Subnet Mask | The subnet mask specifies the network number portion of an IP address. Your ZyWALL will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyWALL 255.255.255.0. |
| RIP Direction | RIP (Routing Information Protocol, RFC1058 and RFC 1389) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Select the RIP direction from **Both**/**In Only**/**Out Only**/**None**. When set to **Both** or **Out Only**, the ZyWALL will broadcast its routing table periodically. When set to **Both** or **In Only**, it will incorporate the RIP information that it receives; when set to **None**, it will not send any RIP packets and will ignore any RIP packets received. **Both** is the default. |

**Table 50** NETWORK > DMZ (continued)

| LABEL | DESCRIPTION |
|---|---|
| RIP Version | The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyWALL sends (it recognizes both formats when receiving). **RIP-1** is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to **Both** and the Version set to **RIP-1**. |
| Multicast | Select **IGMP V-1** or **IGMP V-2** or **None**. IGMP (Internet Group Management Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about inter-operability between IGMP version 2 and version 1, please see *sections 4 and 5 of RFC 2236*. |
| DHCP Setup | |
| DHCP | DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (workstations) to obtain TCP/IP configuration at startup from a server. Unless you are instructed by your ISP, leave this field set to **Server**. When configured as a server, the ZyWALL provides TCP/IP configuration for the clients. When set as a server, fill in the **IP Pool Starting Address** and **Pool Size** fields.<br>Select **Relay** to have the ZyWALL forward DHCP requests to another DHCP server. When set to **Relay**, fill in the **DHCP Server Address** field.<br>Select **None** to stop the ZyWALL from acting as a DHCP server. When you select **None**, you must have another DHCP server on your LAN, or else the computers must be manually configured. |
| IP Pool Starting Address | This field specifies the first of the contiguous addresses in the IP address pool. |
| Pool Size | This field specifies the size, or count of the IP address pool. |
| DHCP Server Address | Type the IP address of the DHCP server to which you want the ZyWALL to relay DHCP requests. Use dotted decimal notation. Alternatively, click the right mouse button to copy and/or paste the IP address. |
| DHCP WINS Server 1, 2 | 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. |
| Filter (IP/MAC Binding | |
| Drop packets that do not match static IP or Dynamic IP/MAC binding | Select this to allow traffic only from devices on the DMZ which have received an IP address from the ZyWALL. This is done by allowing traffic only from devices on the DMZ with specific combinations of IP and MAC addresses. These IP addresses are dynamically assigned by the ZyWALL or manually set using static DHCP.<br>See the **Static DHCP** screen for a list of static IP/MAC address combinations. See the **DHCP Table** available from the **Home** screen for a list of dynamically assigned IP addresses (and their corresponding MAC addresses). |
| Exempt packets in this IP address range. | Set the ZyWALL to allow packets from the DMZ with source IP addresses within a specified range. This allows packets even when their IP and MAC addresses do not match those specified in the **Static DHCP** screen or **DHCP Table**.<br>Type this range of IP addresses in the **From** and **To** fields. |

**Table 50** NETWORK > DMZ (continued)

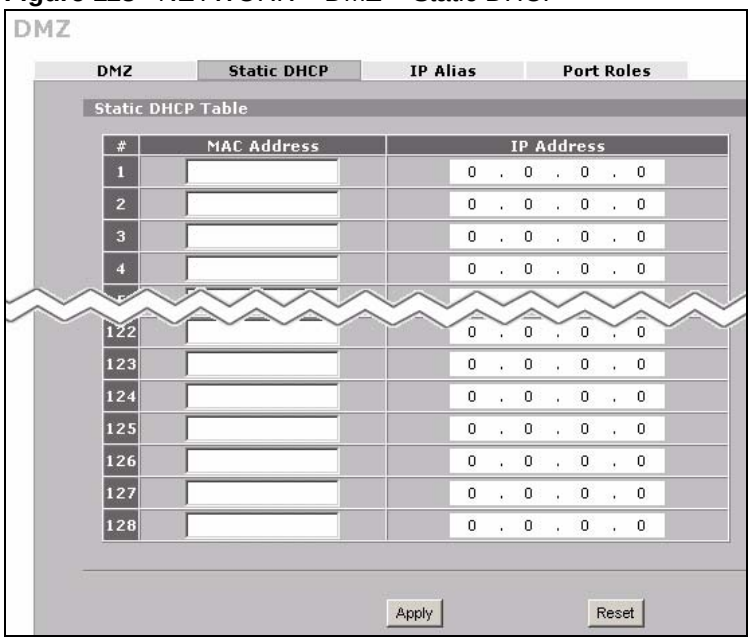
| LABEL | DESCRIPTION |
|---|---|
| Windows Networking (NetBIOS over TCP/IP) | |
| Allow between DMZ and LAN | Select this check box to forward NetBIOS packets from the LAN to the DMZ and from the DMZ to the LAN. If your firewall is enabled with the default policy set to block DMZ to LAN traffic, you also need to configure a DMZ to LAN firewall rule that forwards NetBIOS traffic.<br>Clear this check box to block all NetBIOS packets going from the LAN to the DMZ and from the DMZ to the LAN. |
| Allow between DMZ and WAN 1 | Select this check box to forward NetBIOS packets from the DMZ to WAN 1and from WAN 1 to the DMZ.<br>Clear this check box to block all NetBIOS packets going from the DMZ to WAN 1 and from WAN 1 to the DMZ. |
| Allow between DMZ and WAN 2 | Select this check box to forward NetBIOS packets from the DMZ to WAN 2 and from WAN 2 to the DMZ.<br>Clear this check box to block all NetBIOS packets going from the DMZ to WAN 2 and from WAN 2 to the DMZ. |
| Allow between DMZ and WLAN | Select this check box to forward NetBIOS packets from the WLAN to the DMZ and from the DMZ to the WLAN. If your firewall is enabled with the default policy set to block DMZ to WLAN traffic and WLAN to DMZ traffic, you also need to configure DMZ to WLAN and WLAN to DMZ firewall rules that forward NetBIOS traffic.<br>Clear this check box to block all NetBIOS packets going from the WLAN to the DMZ and from the DMZ to the WLAN. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 10.3 The Static DHCP Screen

This table allows you to assign IP addresses on the DMZ to specific individual computers based on their MAC Addresses.

To change your ZyWALL's static DHCP settings on the DMZ, click **NETWORK** > **DMZ** > **Static DHCP**. The screen appears as shown.

**Figure 118** NETWORK > DMZ > Static DHCP




The following table describes the labels in this screen.

**Table 51** NETWORK > DMZ > Static DHCP

| LABEL | DESCRIPTION |
|---|---|
| # | This is the index number of the static IP table entry (row). |
| MAC Address | Type the MAC address of a computer on your DMZ. |
| IP Address | Type the IP address that you want to assign to the computer on your DMZ. Alternatively, click the right mouse button to copy and/or paste the IP address. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 10.4 The IP Alias Screen

Configure IP alias settings to partition a physical network into different logical networks over the same Ethernet interface.

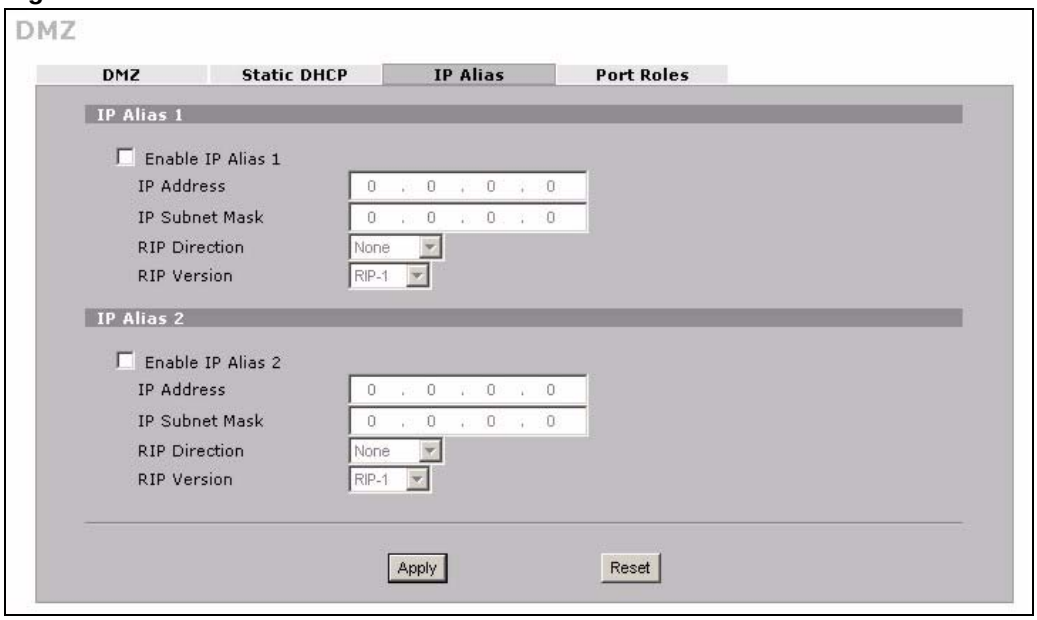
See Section 7.4 on page 156 for more information on IP alias.

The IP alias IP addresses can be either private or public regardless of whether the physical DMZ interface is set to use a private or public IP address. Use NAT if you want to make DMZ computers with private IP addresses publicly accessible. When you use IP alias, you can have the DMZ use both public and private IP addresses at the same time.

Make sure that the subnets of the logical networks do not overlap.

To change your ZyWALL's IP alias settings, click **NETWORK** > **DMZ** > **IP Alias**. The screen appears as shown.

**Figure 119** NETWORK > DMZ > IP Alias




The following table describes the labels in this screen.

**Table 52** NETWORK > DMZ > IP Alias

| LABEL | DESCRIPTION |
|---|---|
| Enable IP Alias 1, 2 | Select the check box to configure another DMZ network for the ZyWALL. |
| IP Address | Enter the IP address of your ZyWALL in dotted decimal notation.<br><br>Note: Make sure the IP addresses of the LAN, WAN, WLAN and DMZ are on separate subnets. |
| IP Subnet Mask | Your ZyWALL will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyWALL. |
| RIP Direction | RIP (Routing Information Protocol, RFC1058 and RFC 1389) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Select the RIP direction from **Both**/**In Only**/**Out Only**/**None**. When set to **Both** or **Out Only**, the ZyWALL will broadcast its routing table periodically. When set to **Both** or **In Only**, it will incorporate the RIP information that it receives; when set to **None**, it will not send any RIP packets and will ignore any RIP packets received. |
| RIP Version | The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyWALL sends (it recognizes both formats when receiving). **RIP-1** is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to **Both** and the Version set to **RIP-1**. |

**Table 52** NETWORK > DMZ > IP Alias (continued)

| LABEL | DESCRIPTION |
|---|---|
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 10.5 The DMZ Port Roles Screen

Use the **Port Roles** screen to set ports as part of the LAN, DMZ and/or WLAN interface.

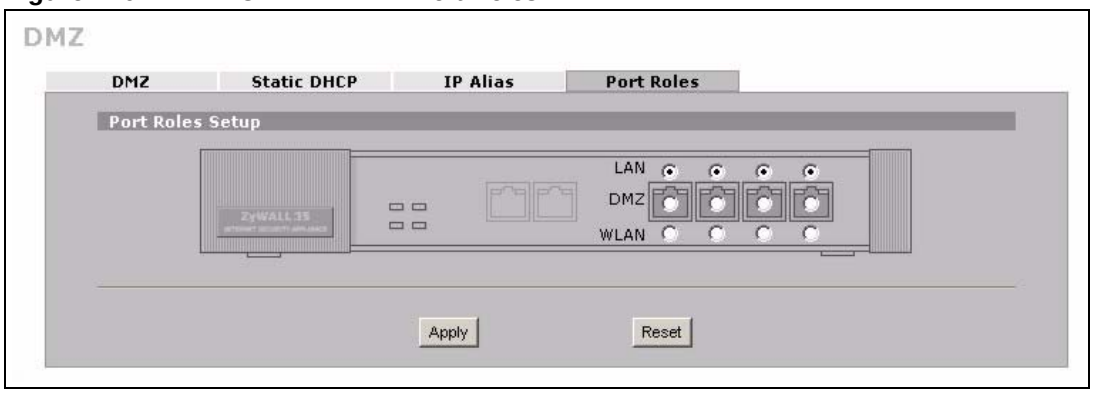
See Section 7.5 on page 158 for more information on port roles.

To change your ZyWALL's port role settings, click **NETWORK** > **DMZ** > **Port Roles**. The screen appears as shown.

The radio buttons correspond to Ethernet ports on the front panel of the ZyWALL. On the ZyWALL 70, ports 1 to 4 are all DMZ ports by default. On the ZyWALL 5 or ZyWALL 35, ports 1 to 4 are all LAN ports by default.

Your changes are also reflected in the **LAN** and/or **WLAN Port Roles** screens.

**Figure 120** NETWORK > DMZ > Port Roles




The following table describes the labels in this screen.

**Table 53** NETWORK > DMZ > Port Roles

| LABEL | DESCRIPTION |
|---|---|
| LAN | Select a port's LAN radio button to use the port as part of the LAN. The port will use the ZyWALL's LAN IP address and MAC address. |
| DMZ | Select a port's DMZ radio button to use the port as part of the DMZ. The port will use the ZyWALL's DMZ IP address and MAC address. |
| WLAN | Select a port's WLAN radio button to use the port as part of the WLAN. The port will use the ZyWALL's WLAN IP address and MAC address. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# 11

# WLAN Screens

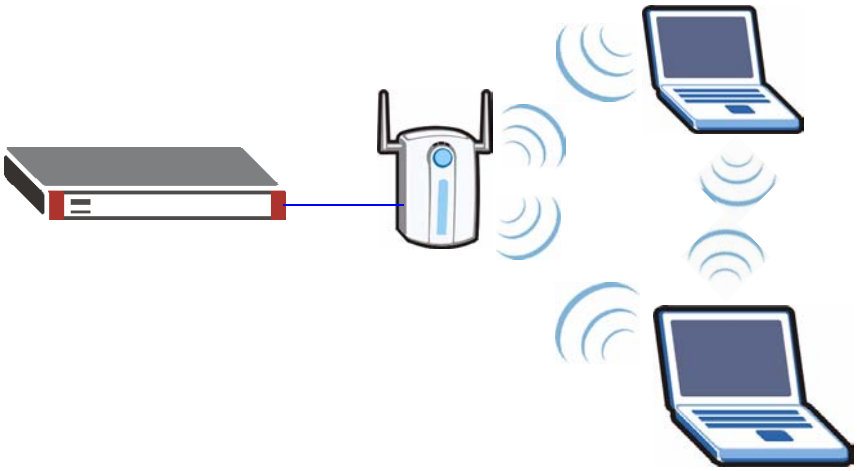
## 11.1 Overview

A wireless LAN can be as simple as two computers with wireless LAN adapters communicating in a peer-to-peer network or as complex as a number of computers with wireless LAN adapters communicating through access points which bridge network traffic to the wired LAN.

To add a wireless network to the ZyWALL, install a wireless card or connect a wireless device such as an Access Point to one of the ZyWALL's Ethernet ports. This chapter describes configuring one (or more) of the ZyWALL's Ethernet ports to use as a separate network for connecting wireless devices. See Section 12.2 on page 232 for information on configuring wireless LAN settings for a wireless card installed in the ZyWALL.

The following diagram shows the ZyWALL connecting to a wireless LAN through an AP.

**Figure 121** WLAN Overview



### 11.1.1 What You Can Do in the WLAN Screens

- Use the **WLAN** screen (Section 11.2 on page 220) to configure TCP/IP, DHCP, IP/MAC binding and NetBIOS settings on the WLAN.
- Use the **Static DHCP** screen (Section 11.3 on page 223) to configure the IP addresses assigned to devices in the LAN by DHCP.
- Use the **IP Alias** screen (Section 11.4 on page 224) to configure IP alias settings on the ZyWALL's LAN ports.

- Use the **Port Roles** screen (Section 11.5 on page 226) to set a port to be part of the WLAN and connect an Access Point (AP) to the WLAN interface to extend the ZyWALL's wireless LAN coverage.

### 11.1.2 What You Need to Know About WLAN

#### DHCP

See Section 7.1.2 on page 150 for more information on DHCP.

Like the LAN, the ZyWALL can also assign TCP/IP configuration via DHCP to computers connected to the WLAN ports.

#### IP alias

See Section 7.4 on page 156 for more information on IP alias.

#### Port roles

See Section 7.5 on page 158 for more information on port roles.

#### Finding Out More

- See Section 2.5 on page 58 for how to install a WLAN card.
- See the WLAN appendix for more detailed information on WLANs.

## 11.2 The WLAN Screen

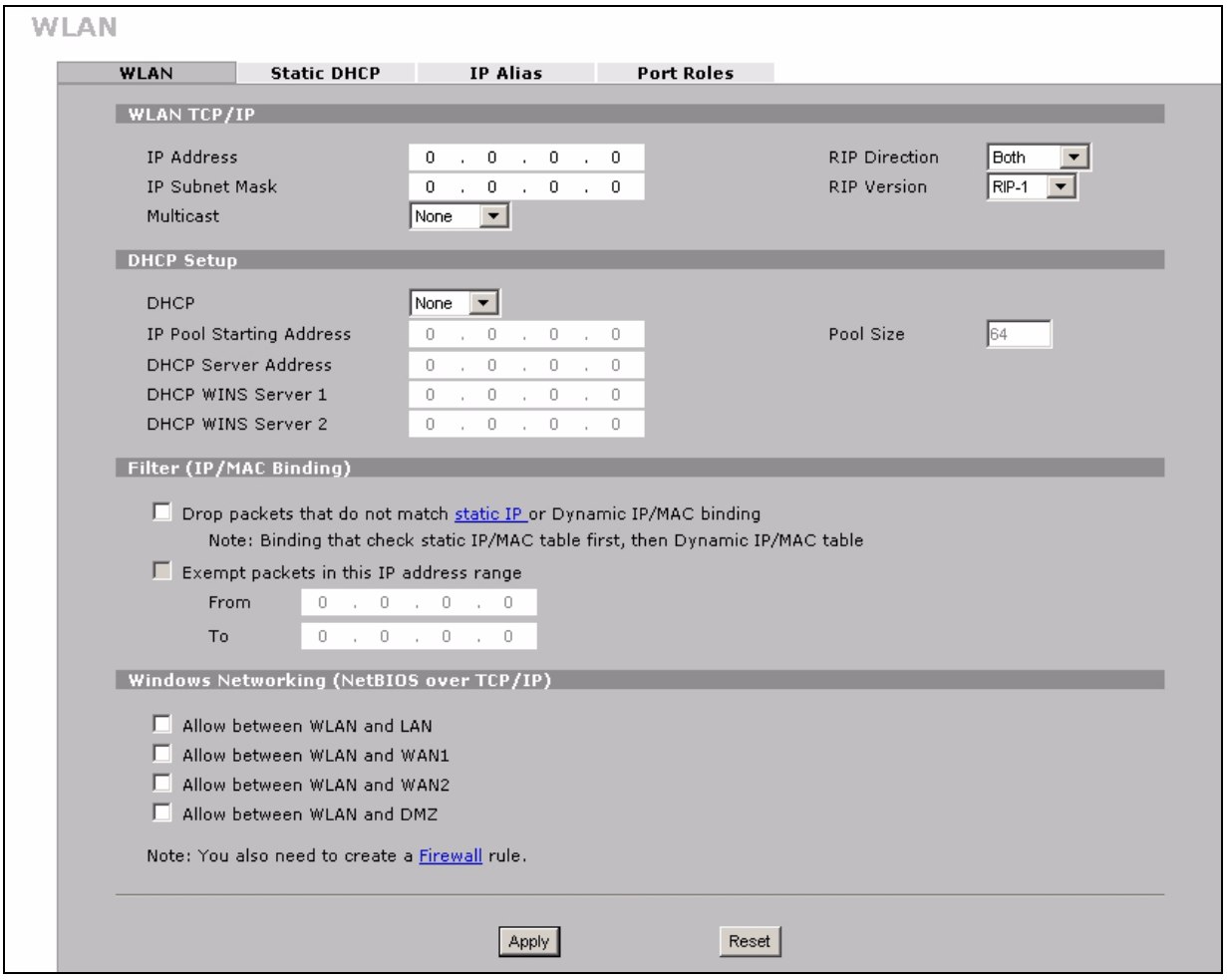
Do one of the following to add a local wireless LAN to the ZyWALL. See Section 9.4 on page 192 if you need to configure a 3G connection (a 3G connection is for Internet access instead of providing a local wireless LAN).

Turn the ZyWALL off before you install or remove the wireless LAN card. See the product specifications chapter for a table of compatible ZyXEL WLAN cards (and the WLAN security features each card supports) and how to install a WLAN card.

Insert a compatible wireless LAN card and enable the card in the **WIRELESS** > **Wi-Fi** screen (see Figure 130 on page 232).

Click **NETWORK** > **WLAN** to open the **WLAN** screen to configure the IP address for the ZyWALL's WLAN interface, other TCP/IP and DHCP settings.

**Figure 122** NETWORK > WLAN




The following table describes the labels in this screen.

**Table 54** NETWORK > WLAN

| LABEL | DESCRIPTION |
|---|---|
| WLAN TCP/IP | |
| IP Address | Type the IP address of your ZyWALL's WLAN interface in dotted decimal notation. Alternatively, click the right mouse button to copy and/or paste the IP address.<br><br>Note: Make sure the IP addresses of the LAN, WAN, WLAN and DMZ are on separate subnets. |
| IP Subnet Mask | The subnet mask specifies the network number portion of an IP address. Your ZyWALL automatically calculates the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyWALL. |
| RIP Direction | RIP (Routing Information Protocol, RFC1058 and RFC 1389) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Select the RIP direction from **Both**/**In Only**/**Out Only**/**None**. When set to **Both** or **Out Only**, the ZyWALL will broadcast its routing table periodically. When set to **Both** or **In Only**, it will incorporate the RIP information that it receives; when set to **None**, it will not send any RIP packets and will ignore any RIP packets received. **Both** is the default. |

**Table 54** NETWORK > WLAN (continued)

| LABEL | DESCRIPTION |
|---|---|
| RIP Version | The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyWALL sends (it recognizes both formats when receiving). **RIP-1** is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to **Both** and the Version set to **RIP-1**. |
| Multicast | Select **IGMP V-1** or **IGMP V-2** or **None**. IGMP (Internet Group Management Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about inter-operability between IGMP version 2 and version 1, please see *sections 4 and 5 of RFC 2236*. |
| DHCP Setup | |
| DHCP | DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (workstations) to obtain TCP/IP configuration at startup from a server. Unless you are instructed by your ISP, leave this field set to **Server**. When configured as a server, the ZyWALL provides TCP/IP configuration for the clients. When set as a server, fill in the **IP Pool Starting Address** and **Pool Size** fields.<br>Select **Relay** to have the ZyWALL forward DHCP requests to another DHCP server. When set to **Relay**, fill in the **DHCP Server Address** field.<br>Select **None** to stop the ZyWALL from acting as a DHCP server. When you select **None**, you must have another DHCP server on your WLAN, or else the computers must be manually configured. |
| IP Pool Starting Address | This field specifies the first of the contiguous addresses in the IP address pool. |
| Pool Size | This field specifies the size, or count of the IP address pool. |
| DHCP Server Address | Type the IP address of the DHCP server to which you want the ZyWALL to relay DHCP requests. Use dotted decimal notation. Alternatively, click the right mouse button to copy and/or paste the IP address. |
| DHCP WINS Server 1, 2 | 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. |
| Filter (IP/MAC Binding | |
| Drop packets that do not match static IP or Dynamic IP/MAC binding | Select this to allow traffic only from devices on the WLAN which have received an IP address from the ZyWALL. This is done by allowing traffic only from devices on the WLAN with specific combinations of IP and MAC addresses. These IP addresses are dynamically assigned by the ZyWALL or manually set using static DHCP.<br>See the **Static DHCP** screen for a list of static IP/MAC address combinations. See the **DHCP Table** available from the **Home** screen for a list of dynamically assigned IP addresses (and their corresponding MAC addresses). |
| Exempt packets in this IP address range. | Set the ZyWALL to allow packets from the WLAN with source IP addresses within a specified range. This allows packets even when their IP and MAC addresses do not match those specified in the **Static DHCP** screen or **DHCP Table**.<br>Type this range of IP addresses in the **From** and **To** fields. |

**Table 54** NETWORK > WLAN (continued)

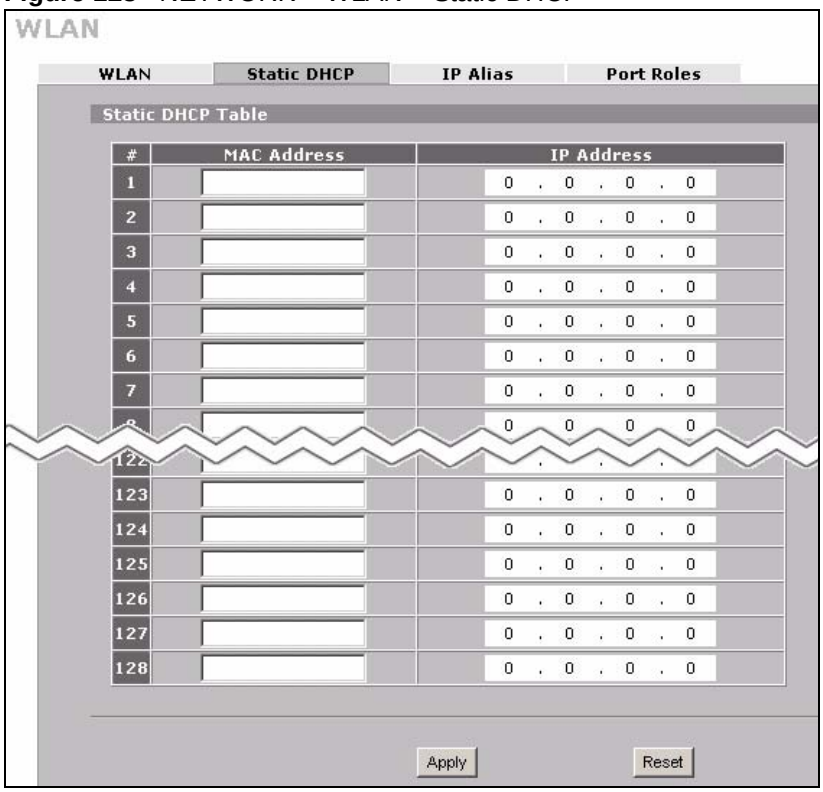
| LABEL | DESCRIPTION |
|---|---|
| Windows Networking (NetBIOS over TCP/IP) | NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls. However it may sometimes be necessary to allow NetBIOS packets to pass through to the WAN in order to find a computer on the WAN. |
| Allow between WLAN and LAN | Select this check box to forward NetBIOS packets from the WLAN to the LAN and from the LAN to the WLAN.<br>Clear this check box to block all NetBIOS packets going from the LAN to the WLAN and from the WLAN to the LAN. |
| Allow between WLAN and WAN 1 | Select this check box to forward NetBIOS packets from the WLAN to WAN 1 and from WAN 1 to the WLAN.<br>Clear this check box to block all NetBIOS packets going from the WLAN to WAN 1 and from WAN 1 to the WLAN. |
| Allow between WLAN and WAN 2 | Select this check box to forward NetBIOS packets from the WLAN to WAN 2 and from WAN 2 to the WLAN.<br>Clear this check box to block all NetBIOS packets going from the WLAN to WAN 2 and from WAN 2 to the WLAN. |
| Allow between WLAN and DMZ | Select this check box to forward NetBIOS packets from the WLAN to the DMZ and from the DMZ to the WLAN. If your firewall is enabled with the default policy set to block WLAN to DMZ traffic and DMZ to WLAN traffic, you also need to configure WLAN to DMZ and DMZ to WLAN firewall rules that forward NetBIOS traffic.<br>Clear this check box to block all NetBIOS packets going from the WLAN to the DMZ and from the DMZ to the WLAN. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 11.3 WLAN Static DHCP

This table allows you to assign IP addresses on the WLAN to specific individual computers based on their MAC addresses.

To change your ZyWALL's WLAN static DHCP settings, click **NETWORK** >**WLAN** > **Static DHCP**. The screen appears as shown.

**Figure 123** NETWORK > WLAN > Static DHCP




The following table describes the labels in this screen.

**Table 55** NETWORK > WLAN > Static DHCP

| LABEL | DESCRIPTION |
|---|---|
| # | This is the index number of the static IP table entry (row). |
| MAC Address | Type the MAC address of a computer on your WLAN. |
| IP Address | Type the IP address that you want to assign to the computer on your WLAN. Alternatively, click the right mouse button to copy and/or paste the IP address. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 11.4 WLAN IP Alias

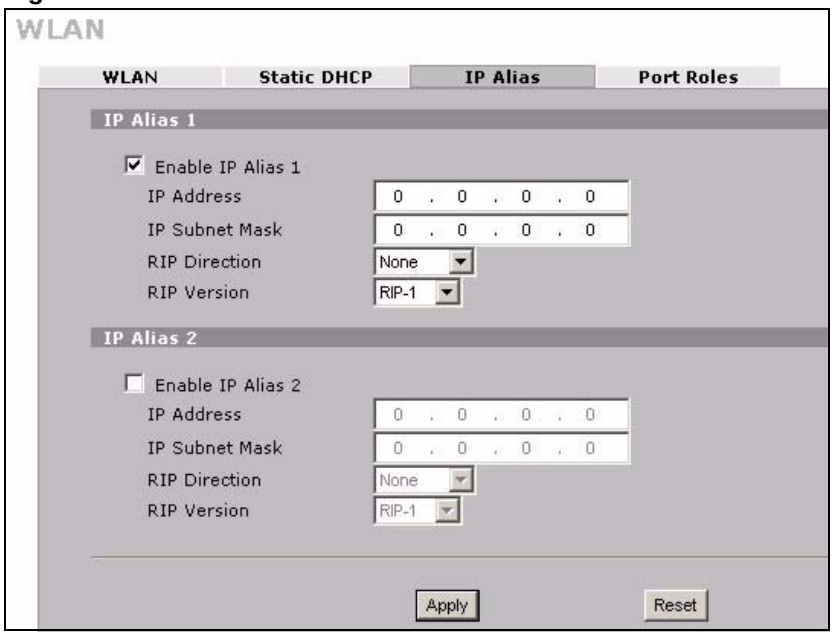
IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface.

See Section 7.4 on page 156 for more information on IP alias.

Make sure that the subnets of the logical networks do not overlap.

To change your ZyWALL's IP alias settings, click **NETWORK** > **WLAN** > **IP Alias**. The screen appears as shown.

**Figure 124** NETWORK > WLAN > IP Alias




The following table describes the labels in this screen.

**Table 56** NETWORK > WLAN > IP Alias

| LABEL | DESCRIPTION |
|---|---|
| Enable IP Alias 1, 2 | Select the check box to configure another WLAN network for the ZyWALL. |
| IP Address | Enter the IP address of your ZyWALL in dotted decimal notation.<br>Alternatively, click the right mouse button to copy and/or paste the IP address. |
| IP Subnet Mask | Your ZyWALL will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyWALL. |
| RIP Direction | RIP (Routing Information Protocol, RFC 1058 and RFC 1389) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Select the RIP direction from **Both**/**In Only**/**Out Only**/**None**. When set to **Both** or **Out Only**, the ZyWALL will broadcast its routing table periodically. When set to **Both** or **In Only**, it will incorporate the RIP information that it receives; when set to **None**, it will not send any RIP packets and will ignore any RIP packets received. |
| RIP Version | The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyWALL sends (it recognizes both formats when receiving). **RIP-1** is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to **Both** and the Version set to **RIP-1**. |

**Table 56** NETWORK > WLAN > IP Alias (continued)

| LABEL | DESCRIPTION |
|---|---|
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

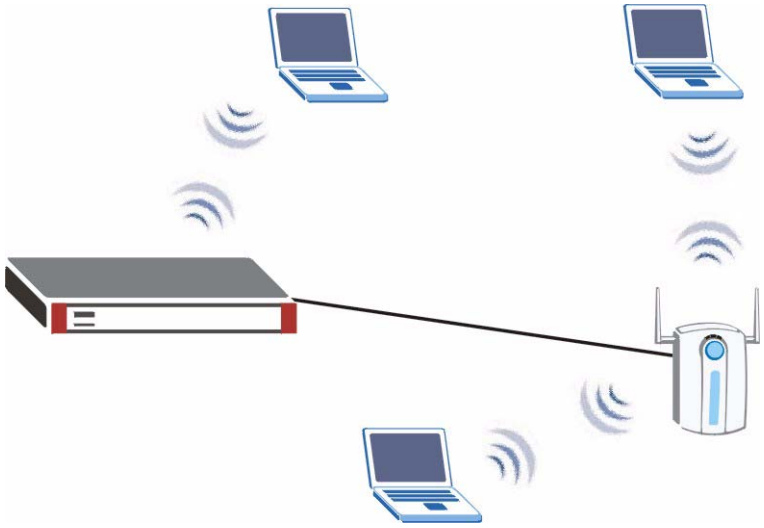
## 11.5 WLAN Port Roles

Use the **Port Roles** screen to set ports as part of the LAN, DMZ and/or WLAN interface.

Connect wireless LAN Access Points (APs) to WLAN interfaces to extend the ZyWALL's wireless LAN coverage. The WLAN port role allows the ZyWALL's firewall to treat traffic from connected APs as part of the ZyWALL's WLAN. You can specify firewall rules for traffic going to or from the WLAN. The WLAN includes the ZyWALL's own WLAN and the Ethernet ports in the WLAN port role.

The following figure shows the ZyWALL with a wireless card installed and an AP connected to an Ethernet port in the WLAN port role.

**Figure 125** WLAN Port Role Example



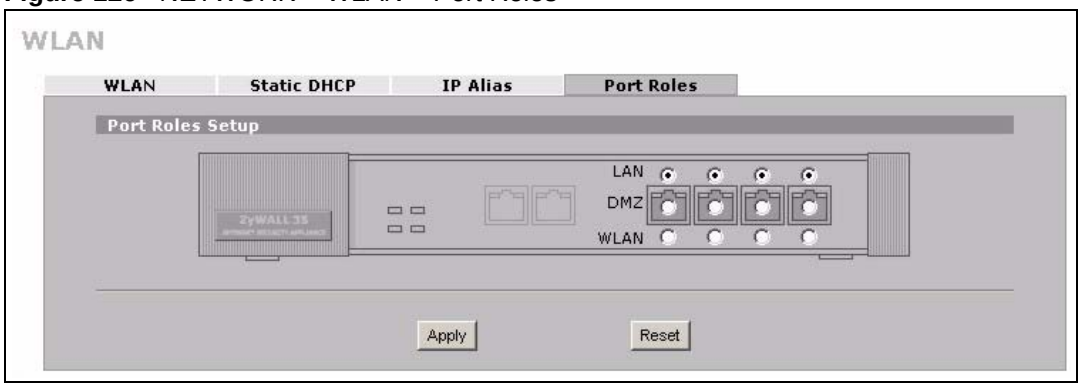
See Section 7.5 on page 158 for more information on port roles.

To change your ZyWALL's port role settings, click **NETWORK** > **WLAN** > **Port Roles**. The screen appears as shown.

The radio buttons correspond to Ethernet ports on the front panel of the ZyWALL. On the ZyWALL 70, ports 1 to 4 are all DMZ ports by default. On the ZyWALL 5 or ZyWALL 35, ports 1 to 4 are all LAN ports by default.

Your changes are also reflected in the **LAN** and/or **DMZ Port Roles** screen.

**Figure 126** NETWORK > WLAN > Port Roles




The following table describes the labels in this screen.

**Table 57** NETWORK > WLAN > Port Roles

| LABEL | DESCRIPTION |
|---|---|
| LAN | Select a port's LAN radio button to use the port as part of the LAN. The port will use the LAN IP address. |
| DMZ | Select a port's DMZ radio button to use the port as part of the DMZ. The port will use the DMZ IP address. |
| WLAN | Select a port's WLAN radio button to use the port as part of the WLAN. The port will use the WLAN IP address. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

After you change the LAN/DMZ/WLAN port roles and click **Apply**, please wait for few seconds until the following screen appears. Click **Return** to go back to the **Port Roles** screen.

**Figure 127** NETWORK > WLAN > Port Roles: Change Complete

# 12

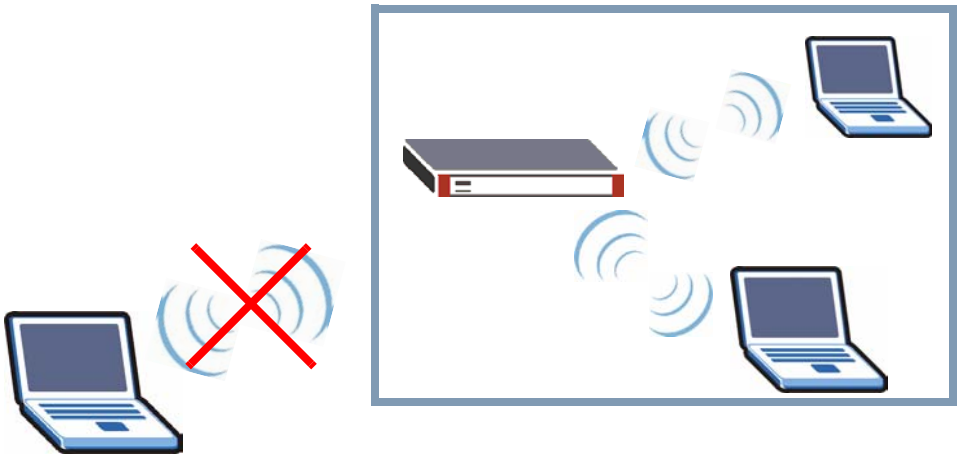
# Wireless Screens

## 12.1 Overview

In this section you can enable your wireless card and configure wireless security. You can configure the ZyWALL to use data encryption and user authentication methods to help protect data transmitted on your network and to ensure only devices with permission to access your network can do so.

The following diagram shows authenticated wireless devices transmitting encrypted data on a wireless network which an unauthenticated device cannot access.

**Figure 128** WLAN Overview



### 12.1.1 What You Can Do in the Wireless Screens

- Use the **Wireless Card** screen (Section 12.2 on page 232) to configure wireless network settings such as wireless security for the ZyWALL.
- Use the **MAC Filter** screen (Section 12.3 on page 243) to set the ZyWALL to allow or disallow access to devices on your wireless network based on their MAC address.

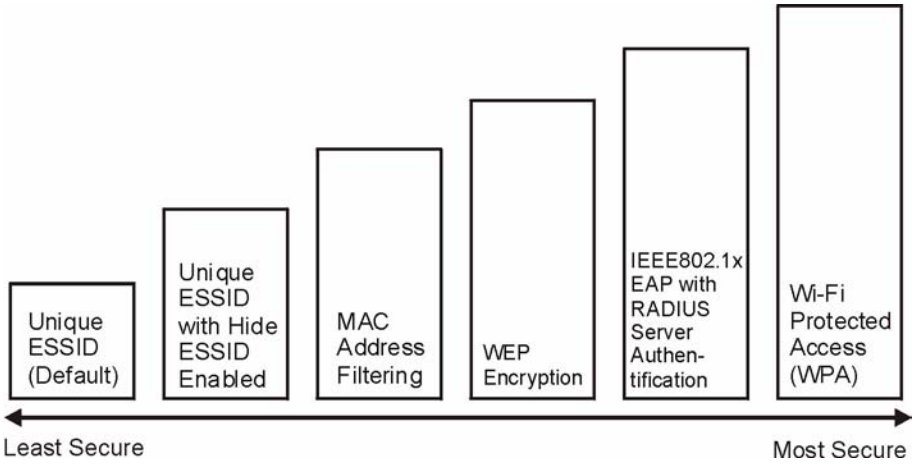
### 12.1.2 What You Need to Know

#### Wireless Security

Wireless security is vital to your network to protect wireless communication between wireless stations, access points and other wireless devices.

The figure below shows the possible wireless security levels on your ZyWALL.

**Figure 129** ZyWALL Wireless Security Levels




If you do not enable any wireless security on your ZyWALL, your network is accessible to any wireless networking device that is within range.

### ESSID

ESSID (Extended Service Set IDentity) identifies the Service Set with which a wireless station is associated. If you hide the ESSID, then the ZyWALL cannot be seen when a wireless client scans for local APs. The trade-off for the extra security of “hiding” the ZyWALL may be inconvenience for some valid WLAN clients.

### MAC Address Filtering

This gives exclusive access to specific devices or excludes specific devices from accessing the ZyWALL based on the device’s MAC address.

### WEP Encryption

WEP (Wired Equivalent Privacy) as specified in the IEEE 802.11 standard provides methods for both data encryption and wireless station authentication. WEP provides a mechanism for encrypting data using encryption keys. Both the AP 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.

### IEEE 802.1x

The IEEE 802.1x standard outlines enhanced security methods for both the authentication of wireless stations and encryption key management. Authentication can be done using the local user database internal to the ZyWALL (authenticate up to 32 users) or an external RADIUS server for an unlimited number of users.

To use 802.1x you need the following.

- A computer with an IEEE 802.11b wireless LAN card.
- A computer equipped with a web browser (with JavaScript enabled) and/or Telnet.
- A wireless station must be running IEEE 802.1x-compliant software. Currently, this is offered in Windows XP.

- An optional network RADIUS server for remote user authentication and accounting.

### EAP Authentication

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, the access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server or the AP.

Your ZyWALL supports EAP-MD5 (Message-Digest Algorithm 5) with the local user database.

### RADIUS

A RADIUS (Remote Authentication Dial In User Service) server enables user authentication, authorization and accounting. RADIUS is based on a client-sever model that supports authentication and accounting, where the access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks among others:

- Authentication
  Determines the identity of the users.
- Accounting
  Keeps track of the client’s network activity.

### WPA

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. Key differences between WPA and WEP are user authentication and improved data encryption.

### Choosing an Encryption Method

- Use WPA security if you have WPA-aware wireless clients and a RADIUS server. WPA has user authentication and improved data encryption over WEP.
- Use WPA-PSK if you have WPA-aware wireless clients but no RADIUS server.
- If you don’t have WPA-aware wireless clients, then use WEP key encrypting. A higher bit key offers better security at a throughput trade-off. You can use Passphrase to automatically generate 64-bit or 128-bit WEP keys or manually enter 64-bit, 128-bit or 256-bit WEP keys.

### Choosing an Authentication Method

- Use RADIUS authentication if you have a RADIUS server.
- Use the Local User Database if you have less than 32 wireless clients in your network. You can't use the ZyWALL's Local User Database for WPA authentication purposes since the Local User Database uses EAP-MD5 which cannot be used to generate keys.
- If you don't have an external RADIUS server you should use WPA-PSK (WPA-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 client will be granted access to a WLAN.

### Finding Out More

- See Section 12.4 on page 244 for technical details on wireless security.

## 12.2 Wireless Card

The wireless card provides wireless functionality to your ZyWALL.

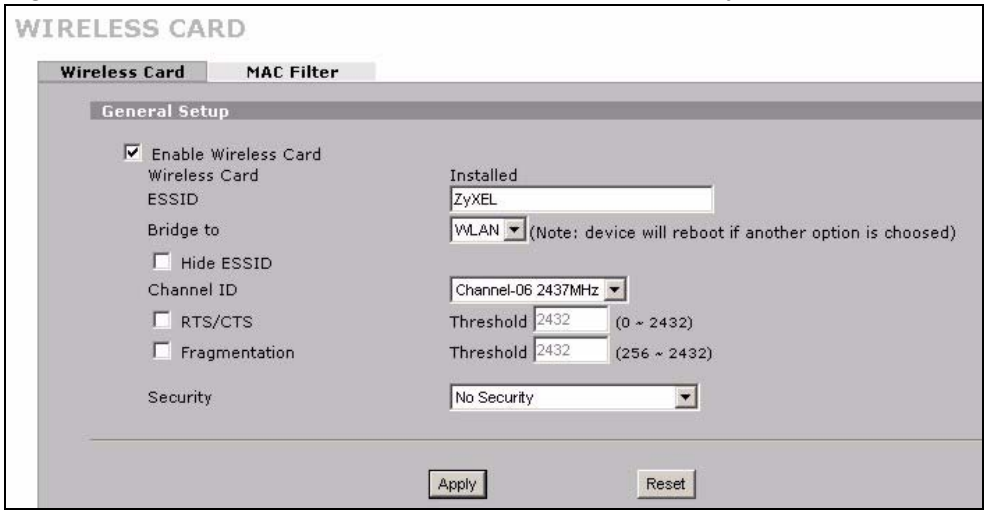
Turn the ZyWALL off before you install or remove the wireless LAN card. See the product specifications chapter for a list of compatible ZyXEL WLAN cards (and the WLAN security features each card supports) and how to install a WLAN card.

You can install either a ZyWALL Turbo Card or a wireless card or a 3G card, but not both at the same time. When you have a wireless card or 3G card installed, you cannot use the anti-virus and IDP features.

If you are configuring the ZyWALL from a computer connected to the wireless LAN and you change the ZyWALL's ESSID or security settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the ZyWALL's new settings.

Click **WIRELESS** > **Wi-Fi** > **Wireless Card** to open the **Wireless Card** screen. The screen varies according to the security features you select.

**Figure 130** WIRELESS > Wi-Fi > Wireless Card: No Security



The following table describes the labels in this screen.

**Table 58** WIRELESS > Wi-Fi > Wireless Card: No Security

| LABEL | DESCRIPTION |
|---|---|
| Enable Wireless Card | The wireless LAN through a wireless LAN card is turned off by default, before you enable the wireless LAN you should configure some security by setting MAC filters and/or 802.1x security; otherwise your wireless LAN will be vulnerable upon enabling it. Select the check box to enable the wireless LAN. |
| Wireless Card | This field displays whether or not a compatible ZyXEL wireless LAN card is installed. |
| ESSID | (Extended Service Set IDentity) The ESSID identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same ESSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN. |
| Bridge to | Select **LAN** to use the wireless card as part of the LAN.<br>Select **DMZ** to use the wireless card as part of the DMZ.<br>Select **WLAN** to use the wireless card as part of the WLAN.<br>The ZyWALL restarts after you change the wireless card setting.<br><br>Note: If you set the wireless card to be part of the LAN or DMZ, you can still use wireless access. The firewall will treat the wireless card as part of the LAN or DMZ respectively. |
| Hide ESSID | Select this to hide the ESSID in the outgoing beacon frame so a station cannot obtain the ESSID through scanning. |
| Channel ID | This allows you to set the operating frequency/channel depending on your particular region. Select a channel from the drop-down list box. |
| RTS/CTS Threshold | Use RTS/CTS 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>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. |

**Table 58** WIRELESS > Wi-Fi > Wireless Card: No Security (continued)

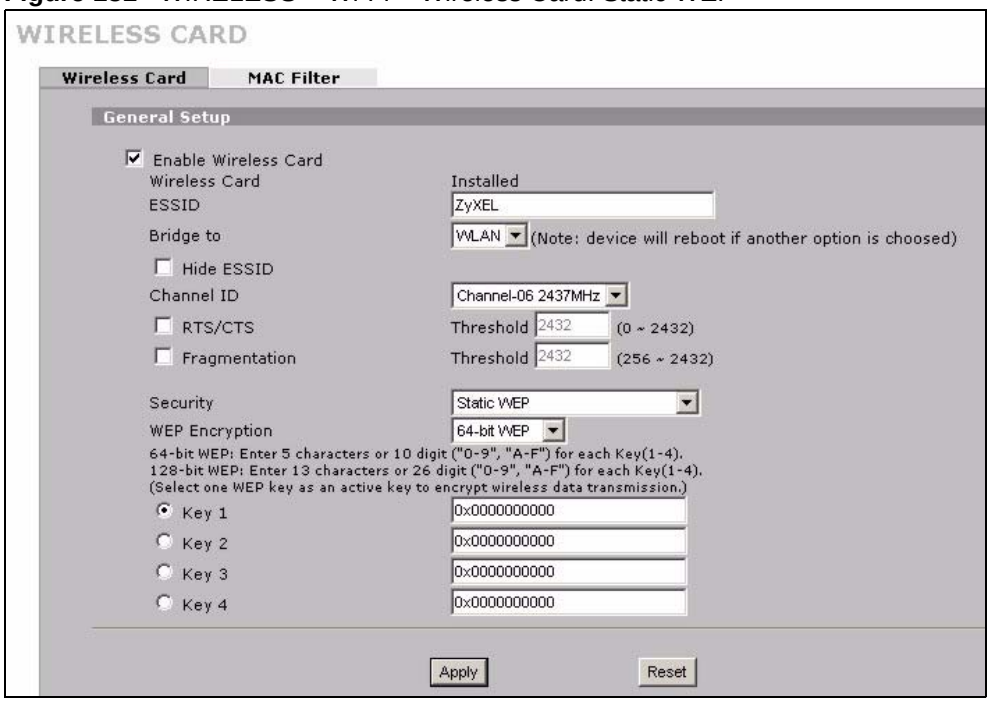
| LABEL | DESCRIPTION |
|---|---|
| Security | Select one of the security settings.<br>**No Security**<br>**Static WEP**<br>**WPA-PSK**<br>**WPA**<br>**802.1x + Dynamic WEP**<br>**802.1x + Static WEP**<br>**802.1x + No WEP**<br>**No Access 802.1x + Static WEP**<br>**No Access 802.1x + No WEP**<br>Select **No Security** to allow wireless stations to communicate with the access points without any data encryption. Otherwise, select the security you need and see the following sections for more information.<br><br>Note: The installed ZyXEL WLAN card may not support all of the WLAN security features you can configure in the ZyWALL.<br><br>Please see the product specifications chapter for a table of compatible ZyXEL WLAN cards and the WLAN security features each card supports. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 12.2.1 Static WEP

Static WEP provides a mechanism for encrypting data using encryption keys. Both the AP 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.

In order to configure and enable WEP encryption, click **WIRELESS** > **Wi-Fi** > **Wireless Card** to display the **Wireless Card** screen. Select **Static WEP** from the **Security** list.

**Figure 131** WIRELESS > Wi-Fi > Wireless Card: Static WEP




The following table describes the wireless LAN security labels in this screen.

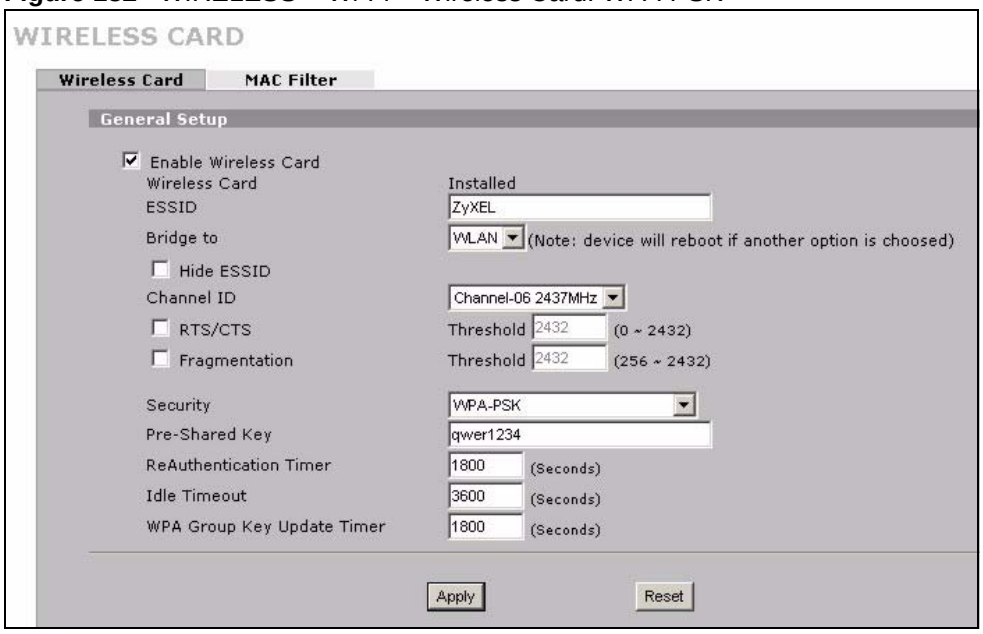
**Table 59** WIRELESS > Wi-Fi > Wireless Card: Static WEP

| LABEL | DESCRIPTION |
|---|---|
| Security | Select **Static WEP** from the drop-down list. |
| 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 10 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 26 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key.<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. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 12.2.2 WPA-PSK

Click **WIRELESS** > **Wi-Fi** > **Wireless Card** to display the **Wireless Card** screen. Select **WPA-PSK** from the **Security** list.

**Figure 132** WIRELESS > Wi-Fi > Wireless Card: WPA-PSK




The following wireless LAN security fields become available when you select **WPA-PSK** in the **Security** drop down list-box.

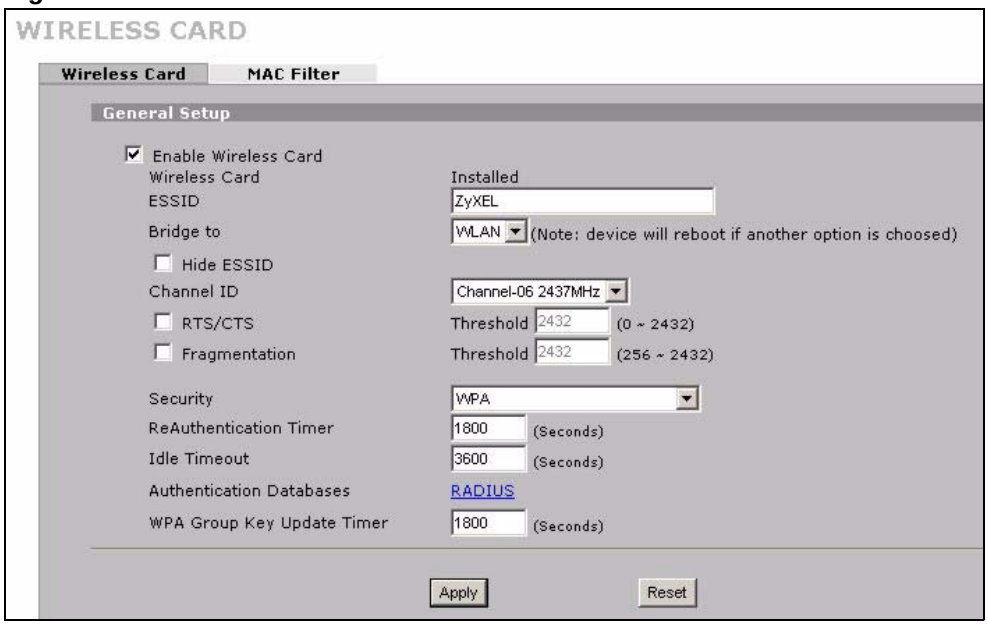
**Table 60** WIRELESS > Wi-Fi > Wireless Card: WPA-PSK

| LABEL | DESCRIPTION |
|---|---|
| Security | Select **WPA-PSK** from the drop-down list. |
| 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>Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols). |
| ReAuthentication Timer (Seconds) | Specify how often wireless stations have to resend user names and passwords in order to stay connected. Enter a time interval between 10 and 65535 seconds.<br>If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority. |
| Idle Timeout (Seconds) | The ZyWALL automatically disconnects a wireless station from the wireless network after a period of inactivity. The wireless station needs to send the username and password again before it can use the wireless network again. Some wireless clients may prompt users for a username and password; other clients may use saved login credentials. In either case, there is usually a short delay while the wireless client logs in to the wireless network again.<br>This value is usually smaller when the wireless network is keeping track of how much time each wireless station is connected to the wireless network (for example, using an authentication server). If the wireless network is not keeping track of this information, you can usually set this value higher to reduce the number of delays caused by logging in again. |
| WPA Group Key Update Timer (Seconds) | The **WPA Group Key Update Timer** is the rate at which the AP (if using **WPA-PSK** key management) or RADIUS server (if using **WPA** key management) sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the **WPA Group Key Update Timer** is also supported in **WPA-PSK** mode. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

### 12.2.3 WPA

Click **WIRELESS** > **Wi-Fi** > **Wireless Card** to display the **Wireless Card** screen. Select **WPA** from the **Security** list.

**Figure 133** WIRELESS > Wi-Fi > Wireless Card: WPA




The following wireless LAN security fields become available when you select **WPA** in the **Security** drop down list-box.

**Table 61** WIRELESS > Wi-Fi > Wireless Card: WPA

| LABEL | DESCRIPTION |
|---|---|
| Security | Select **WPA** from the drop-down list. |
| ReAuthentication Timer (Seconds) | Specify how often wireless stations have to resend user names and passwords in order to stay connected. Enter a time interval between 10 and 65535 seconds.<br>If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority. |
| Idle Timeout (Seconds) | The ZyWALL automatically disconnects a wireless station from the wireless network after a period of inactivity. The wireless station needs to send the username and password again before it can use the wireless network again. Some wireless clients may prompt users for a username and password; other clients may use saved login credentials. In either case, there is usually a short delay while the wireless client logs in to the wireless network again.<br>This value is usually smaller when the wireless network is keeping track of how much time each wireless station is connected to the wireless network (for example, using an authentication server). If the wireless network is not keeping track of this information, you can usually set this value higher to reduce the number of delays caused by logging in again. |
| Authentication Databases | Click **RADIUS** to go to the **RADIUS** screen where you can configure the ZyWALL to check an external RADIUS server. |
| WPA Group Key Update Timer (Seconds) | The **WPA Group Key Update Timer** is the rate at which the AP (if using **WPA-PSK** key management) or RADIUS server (if using **WPA** key management) sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the **WPA Group Key Update Timer** is also supported in **WPA-PSK** mode. |

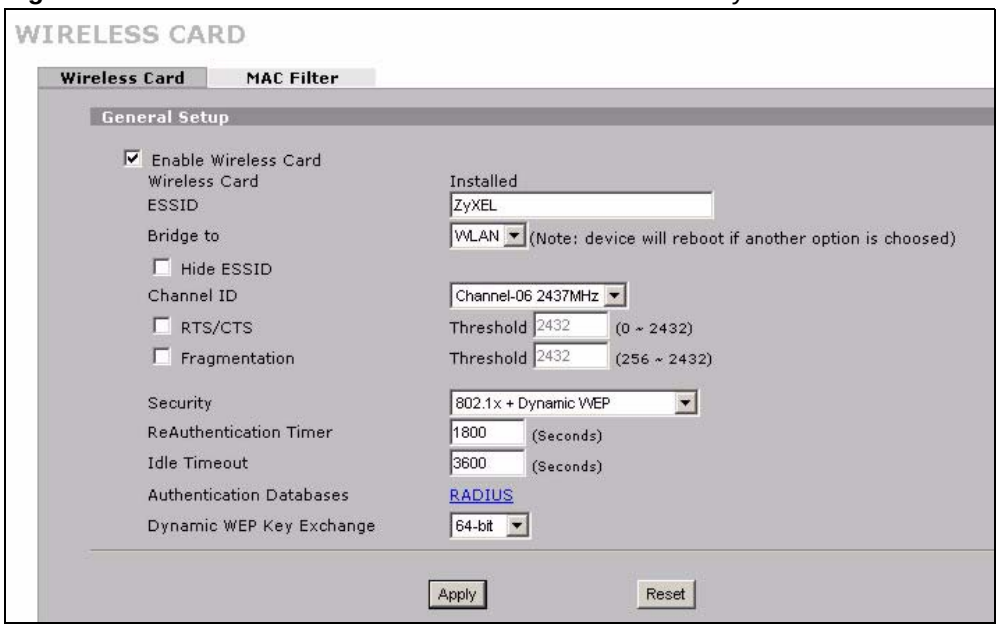
**Table 61** WIRELESS > Wi-Fi > Wireless Card: WPA (continued)

| LABEL | DESCRIPTION |
|---|---|
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 12.2.4 IEEE 802.1x + Dynamic WEP

Click **WIRELESS** > **Wi-Fi** > **Wireless Card** to display the **Wireless Card** screen. Select **802.1x + Dynamic WEP** from the **Security** list.

**Figure 134** WIRELESS > Wi-Fi > Wireless Card: 802.1x + Dynamic WEP




The following wireless LAN security fields become available when you select **802.1x + Dynamic WEP** in the **Security** drop down list-box.

**Table 62** WIRELESS > Wi-Fi > Wireless Card: 802.1x + Dynamic WEP

| LABEL | DESCRIPTION |
|---|---|
| Security | Select **802.1x + Dynamic WEP** from the drop-down list. |
| ReAuthentication Timer (Seconds) | Specify how often wireless stations have to resend user names and passwords in order to stay connected. Enter a time interval between 10 and 65535 seconds.<br>If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority. |
| Idle Timeout (Seconds) | The ZyWALL automatically disconnects a wireless station from the wireless network after a period of inactivity. The wireless station needs to send the username and password again before it can use the wireless network again. Some wireless clients may prompt users for a username and password; other clients may use saved login credentials. In either case, there is usually a short delay while the wireless client logs in to the wireless network again.<br>This value is usually smaller when the wireless network is keeping track of how much time each wireless station is connected to the wireless network (for example, using an authentication server). If the wireless network is not keeping track of this information, you can usually set this value higher to reduce the number of delays caused by logging in again. |

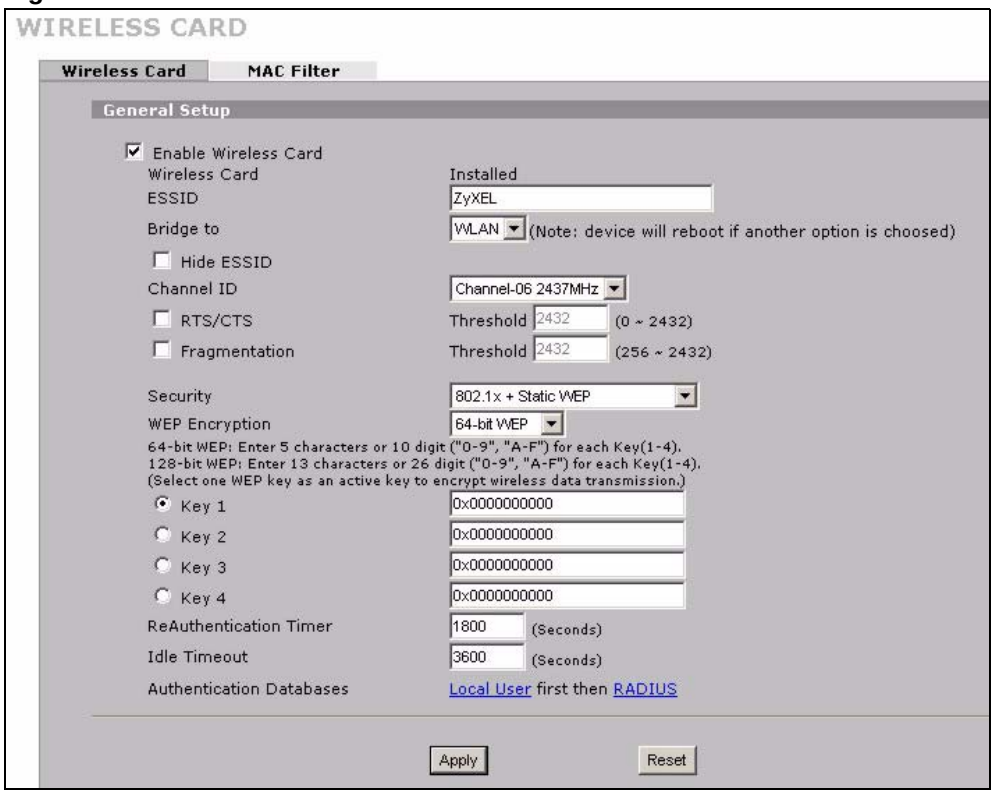
**Table 62** WIRELESS > Wi-Fi > Wireless Card: 802.1x + Dynamic WEP

| LABEL | DESCRIPTION |
|---|---|
| Authentication Databases | Click **RADIUS** to go to the **RADIUS** screen where you can configure the ZyWALL to check an external RADIUS server. |
| Dynamic WEP Key Exchange | Select **64-bit WEP** or **128-bit WEP** to enable data encryption. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 12.2.5 IEEE 802.1x + Static WEP

Click **WIRELESS** > **Wi-Fi** > **Wireless Card** to display the **Wireless Card** screen. Select **802.1x + Static WEP** from the **Security** list.

**Figure 135** WIRELESS > Wi-Fi > Wireless Card: 802.1x + Static WEP




The following wireless LAN security fields become available when you select **802.1x + Static WEP** in the **Security** drop down list-box.

**Table 63** WIRELESS > Wi-Fi > Wireless Card: 802.1x + Static WEP

| LABEL | DESCRIPTION |
|---|---|
| Security | Select **802.1x + Static WEP** from the drop-down list. |
| WEP Encryption | WEP (Wired Equivalent Privacy) provides data encryption to prevent unauthorized wireless stations from accessing data transmitted over the wireless network. Select **64-bit WEP** or **128-bit WEP** to enable data encryption. |

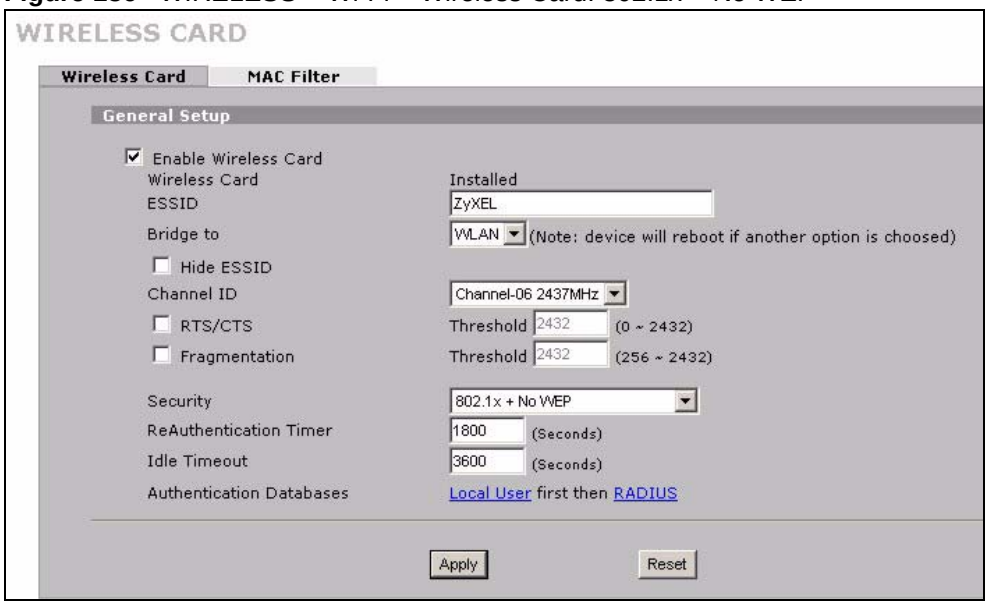
**Table 63** WIRELESS > Wi-Fi > Wireless Card: 802.1x + Static WEP (continued)

| LABEL | DESCRIPTION |
|---|---|
| Key 1 to Key 4 | If you chose **64-bit WEP** in the **WEP Encryption** field, then enter any 5 characters (ASCII string) or 10 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 26 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key.<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. |
| ReAuthentication Timer (Seconds) | Specify how often wireless stations have to resend user names and passwords in order to stay connected. Enter a time interval between 10 and 65535 seconds.<br>If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority. |
| Idle Timeout (Seconds) | The ZyWALL automatically disconnects a wireless station from the wireless network after a period of inactivity. The wireless station needs to send the username and password again before it can use the wireless network again. Some wireless clients may prompt users for a username and password; other clients may use saved login credentials. In either case, there is usually a short delay while the wireless client logs in to the wireless network again.<br>This value is usually smaller when the wireless network is keeping track of how much time each wireless station is connected to the wireless network (for example, using an authentication server). If the wireless network is not keeping track of this information, you can usually set this value higher to reduce the number of delays caused by logging in again. |
| Authentication Databases | Click **Local User** to go to the **Local User Database** screen where you can view and/or edit the list of users and passwords. Click **RADIUS** to go to the **RADIUS** screen where you can configure the ZyWALL to check an external RADIUS server. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 12.2.6 IEEE 802.1x + No WEP

Click **WIRELESS** > **Wi-Fi** > **Wireless Card** to display the **Wireless Card** screen. Select **802.1x + No WEP** from the **Security** list.

**Figure 136** WIRELESS > Wi-Fi > Wireless Card: 802.1x + No WEP




The following wireless LAN security fields become available when you select **802.1x + No WEP** in the **Security** drop down list-box.

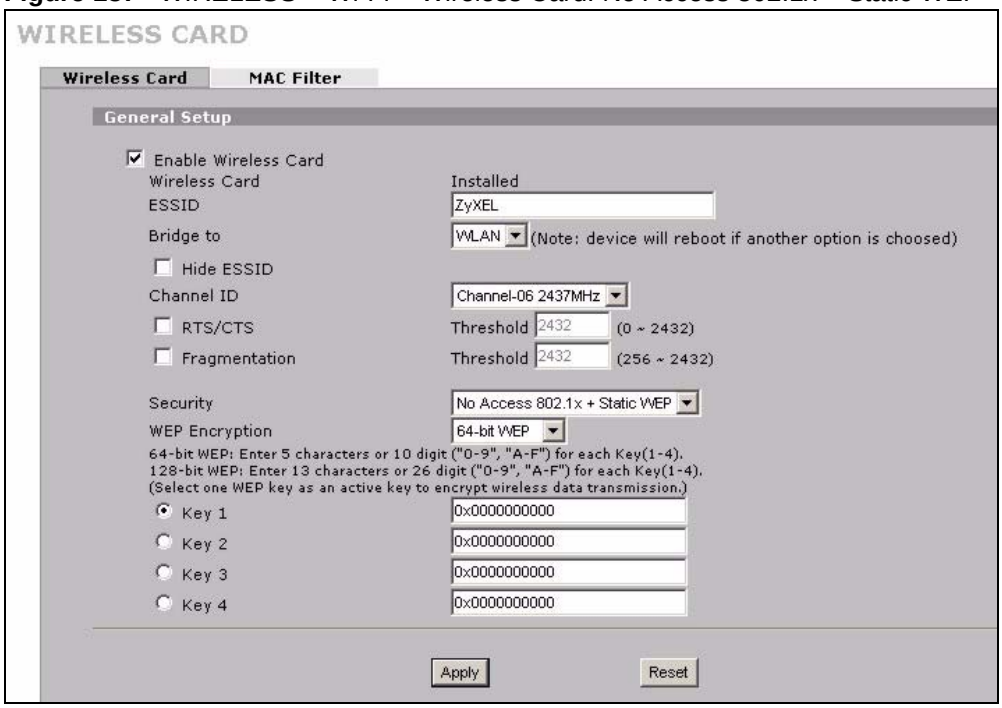
**Table 64** WIRELESS > Wi-Fi > Wireless Card: 802.1x + No WEP

| LABEL | DESCRIPTION |
|---|---|
| Security | Select **802.1x + No WEP** from the drop-down list. |
| ReAuthentication Timer (Seconds) | Specify how often wireless stations have to resend user names and passwords in order to stay connected. Enter a time interval between 10 and 65535 seconds.<br>If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority. |
| Idle Timeout (Seconds) | The ZyWALL automatically disconnects a wireless station from the wireless network after a period of inactivity. The wireless station needs to send the username and password again before it can use the wireless network again. Some wireless clients may prompt users for a username and password; other clients may use saved login credentials. In either case, there is usually a short delay while the wireless client logs in to the wireless network again.<br>This value is usually smaller when the wireless network is keeping track of how much time each wireless station is connected to the wireless network (for example, using an authentication server). If the wireless network is not keeping track of this information, you can usually set this value higher to reduce the number of delays caused by logging in again. |
| Authentication Databases | Click **Local User** to go to the **Local User Database** screen where you can view and/or edit the list of users and passwords. Click **RADIUS** to go to the **RADIUS** screen where you can configure the ZyWALL to check an external RADIUS server. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 12.2.7 No Access 802.1x + Static WEP

Click **WIRELESS** > **Wi-Fi** > **Wireless Card** to display the **Wireless Card** screen. Select **No Access 802.1x + Static WEP** to deny all wireless stations access to your wired network and allow wireless stations to communicate with the ZyWALL using static WEP keys for data encryption.

**Figure 137** WIRELESS > Wi-Fi > Wireless Card: No Access 802.1x + Static WEP




The following wireless LAN security fields become available when you select **No Access 802.1x + Static WEP** in the **Security** drop down list-box.

**Table 65** WIRELESS > Wi-Fi > Wireless Card: No Access 802.1x + Static WEP

| LABEL | DESCRIPTION |
|---|---|
| Security | Select **No Access 802.1x + Static WEP** from the drop-down list. |
| 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 10 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 26 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key.<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. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 12.2.8 No Access 802.1x + No WEP

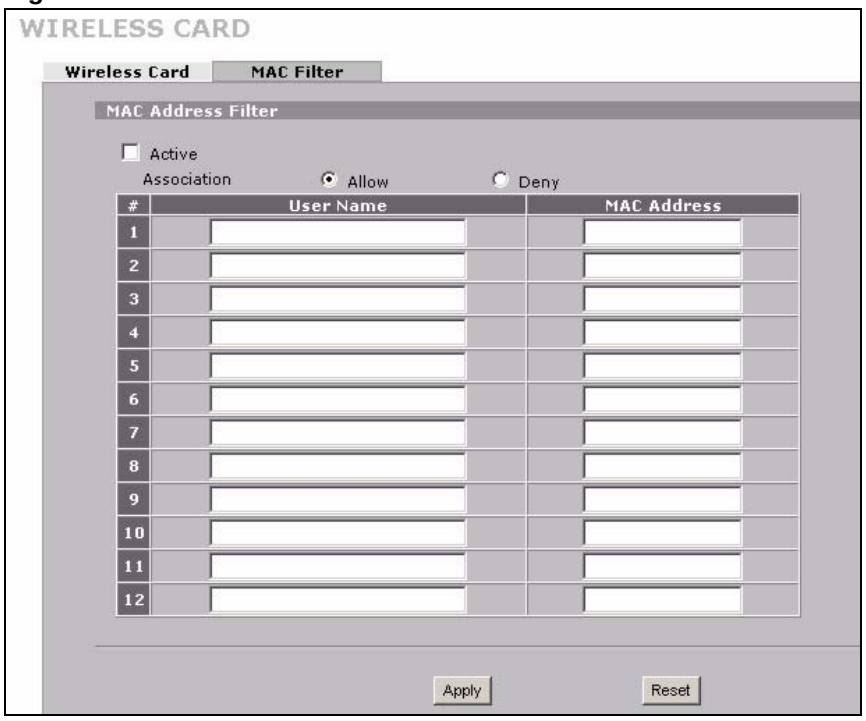
Click the **NETWORK** > **WIRELESS CARD** or **NETWORK** > **Wi-Fi** to display the **Wireless Card** screen. Select **No Access 802.1x + No WEP** to deny all wireless stations access to your wired network and block all wireless stations from communicating with the ZyWALL.

# 12.3 MAC Filter

The MAC filter screen allows you to configure the ZyWALL to give exclusive access to specific devices (**Allow Association**) or exclude specific devices from accessing the ZyWALL (**Deny Association**). You need to know the MAC addresses of the devices to configure this screen.

To change your ZyWALL's MAC filter settings, click **WIRELESS** > **Wi-Fi** > **MAC Filter**. The screen appears as shown.

**Figure 138** WIRELESS > Wi-Fi > MAC Filter




The following table describes the labels in this menu.

**Table 66** WIRELESS > Wi-Fi > MAC Filter

| LABEL | DESCRIPTION |
|---|---|
| Active | Select or clear the check box to enable or disable MAC address filtering.<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>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. |
| # | This is the index number of the MAC address. |
| User Name | Enter a descriptive name for the MAC address. |
| MAC Address | Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the wireless stations that are allowed or denied access to the ZyWALL in these address fields. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 12.4 Technical Reference

# IRADIUS

RADIUS user is a simple package exchange in which your ZyWALL acts as a message relay between the wireless station and the network RADIUS server. See RFC 2138 and RFC 2139 for more on RADIUS.

### 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:

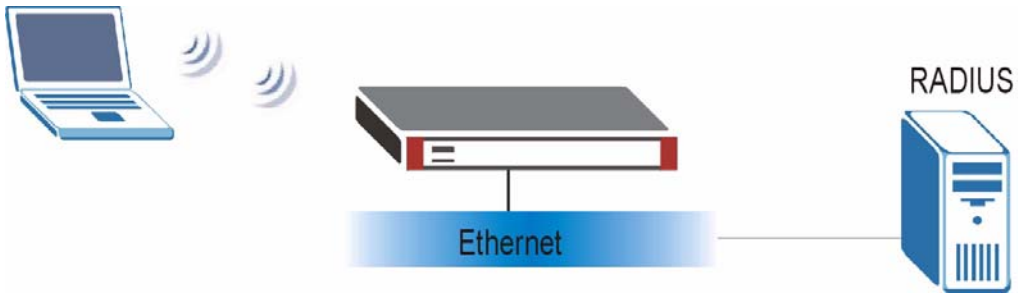
- **Accounting-Request**
  Sent by the access point requesting accounting.
- **Accounting-Response**
  Sent by the RADIUS server to indicate that it has started or stopped accounting.

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.

# EAP Authentication

The following figure shows an overview of authentication when you specify a RADIUS server on your access point.

**Figure 139** EAP Authentication




The details below provide a general description of how IEEE 802.1x EAP authentication works.

- The wireless station sends a start message to the ZyWALL.
- The ZyWALL sends a request identity message to the wireless station for identity information.
- The wireless station replies with identity information, including user name and password.
- The RADIUS server checks the user information against its user profile database and determines whether or not to authenticate the wireless station.

# WPA

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. Key differences between WPA and WEP are user authentication and improved data encryption.

## User Authentication

WPA applies IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database.

## Encryption

WPA improves data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x.

Temporal Key Integrity Protocol (TKIP) uses 128-bit keys that are dynamically generated and distributed by the authentication server. It includes 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.

TKIP regularly changes and rotates 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 pair-wise key 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), TKIP makes it much more difficult to decode data on a Wi-Fi network than WEP, making it difficult for an intruder to break into the network.

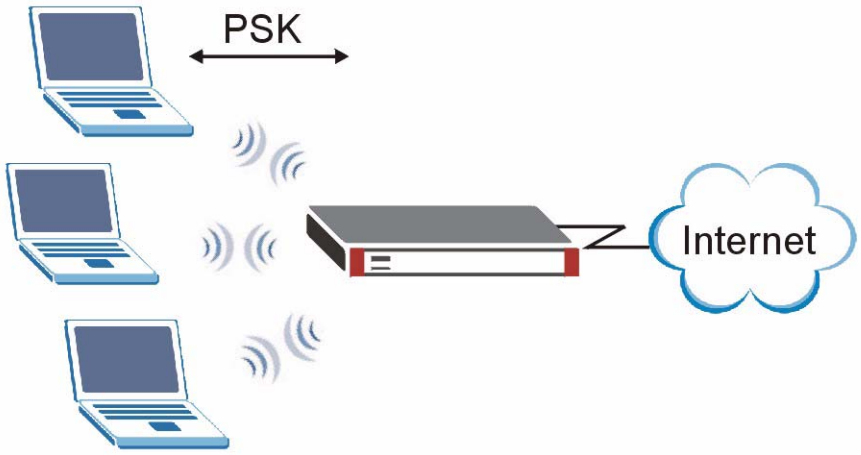
The encryption mechanisms used for WPA and WPA-PSK are the same. The only difference between the two is that WPA-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs an easier-to-use, consistent, single, alphanumeric password.

### WPA-PSK Application

A WPA-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 (including spaces and symbols).
2. The AP checks each client's password and (only) allows it to join the network if it matches its password.
3. The AP derives and distributes keys to the wireless clients.
4. The AP and wireless clients use the TKIP encryption process to encrypt data exchanged between them.

**Figure 140** WPA-PSK Authentication




## WPA with RADIUS Application

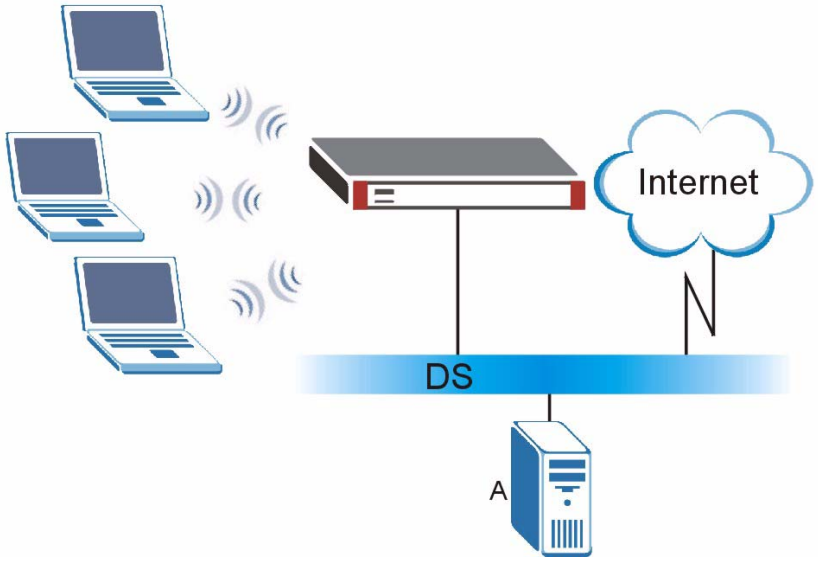
You need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

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 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 pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

**Figure 141** WPA with RADIUS Application Example




## 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 supplicants are the WPA patch for Windows XP, Funk Software's Odyssey client, and Meetinghouse Data Communications' AEGIS 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.

# PART III
# Security

# 13

# Firewall Screens

This chapter shows you how to configure your ZyWALL's firewall.

## 13.1 Overview

A firewall is a system that enforces an access-control policy between two networks. It is generally a mechanism used to protect a trusted network from an untrusted network.

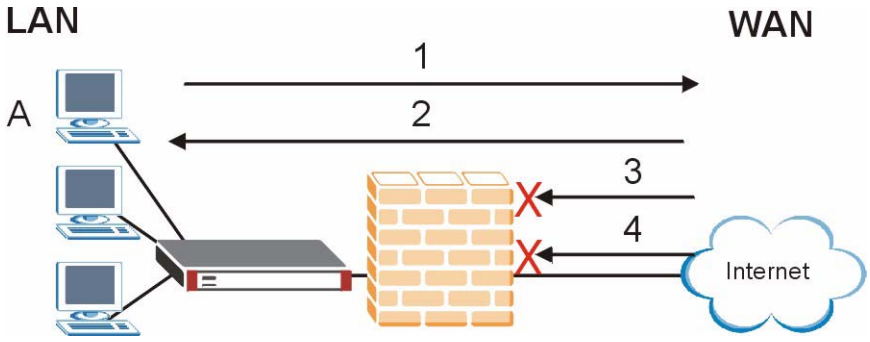
The ZyWALL physically separates the LAN, DMZ, WLAN and the WAN and acts as a secure gateway for all data passing between the networks. The ZyWALL protects against Denial of Service (DoS) attacks, prevents theft, destruction and modification of data, and logs events.

Enable the firewall to protect your LAN computers from attacks by hackers on the Internet and control access between the LAN, DMZ, WLAN and WAN. By default the firewall:

- allows traffic that originates from your LAN computers to go to all of the networks.
- blocks traffic that originates on the other networks from going to the LAN.
- allows traffic that originates on the WLAN to go to the WAN.
- allows traffic that originates on the WAN to go to the DMZ and protects your DMZ computers against DoS attacks.
- allows VPN traffic between any of the networks.

The following figure illustrates the default firewall action. User A can initiate an IM (Instant Messaging) session from the LAN to the WAN (1). Return traffic for this session is also allowed (2). However other traffic initiated from the WAN is blocked (3 and 4).

**Figure 142** Default Firewall Action




Your customized rules take precedence and override the ZyWALL's default settings. The ZyWALL checks the 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.

### 13.1.1 What You Can Do Using the Firewall Screens

- Use the **Default Rule** screens (Section 13.4 on page 256) to configure general firewall settings when the ZyWALL is set to router mode or bridge mode.
- Use the **Rule Summary** screens (Section 13.5 on page 259) to configure firewall rules.
- Use the **Anti-Probing** screen (Section 13.6 on page 263) to specify which of the ZyWALL's interfaces will respond to Ping requests and whether or not the ZyWALL is to respond to probing for unused ports.
- Use the **Threshold** (Section 13.7 on page 264) screen to configure DoS thresholds and actions to be taken when a threshold is reached
- Use the **Service** (Section 13.8 on page 266) screen to configure custom services for use in firewall rules or view the services that are predefined in the ZyWALL.

### 13.1.2 What You Need To Know About the ZyWALL Firewall

#### Packet Direction

Packets have source and destination address headers. You can set what the ZyWALL does with packets traveling in a specific direction (including going to/coming from a VPN tunnel) that do not match any of the firewall rules. See also Packet Direction on page 252.

#### Asymmetrical Routes

Asymmetrical routes only apply if you have another gateway on your LAN, the ZyWALL is in **Router** mode, and the firewall is enabled. If return traffic is routed through the LAN gateway (instead of the ZyWALL), then the ZyWALL may reset the 'incomplete' connection. When you enable asymmetrical routes, interface to same interface (for example WAN 1 to WAN 1, VPN to VPN and so on) traffic is not checked by the firewall. See Asymmetrical Routes and IP Alias on page 274 for information on how to use IP alias instead of asymmetrical routes.

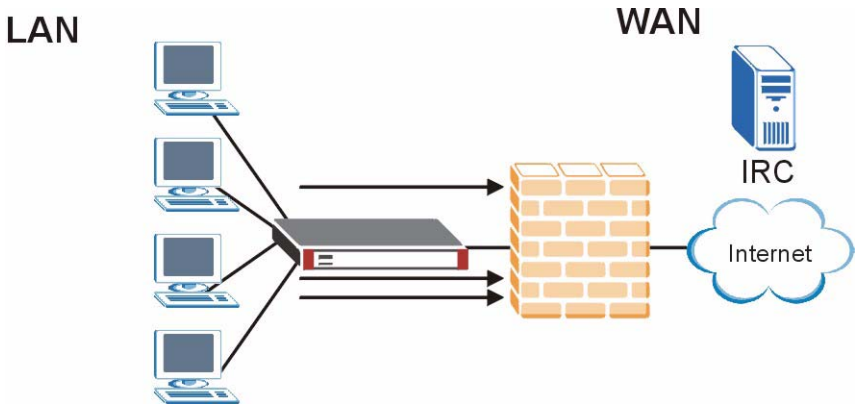
### 13.1.3 Before You Begin

Before you configure the firewall, you must first decide if the ZyWALL will act as a **Router** or a **Bridge**. When the ZyWALL is in **Bridge** mode, the firewall is transparent to your network. You do not have to reconfigure existing network configurations.

## 13.2 Firewall Rules Example

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 143** Blocking All LAN to WAN IRC Traffic Example




Your firewall would have the following configuration.

**Table 67** Blocking All LAN to WAN IRC Traffic Example

| # | SOURCE | DESTINATION | SCHEDULE | SERVICE | ACTION |
|---|---|---|---|---|---|
| 1 | Any | Any | Any | IRC | Drop |
| Default | 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 traffic from the LAN to go to the WAN.

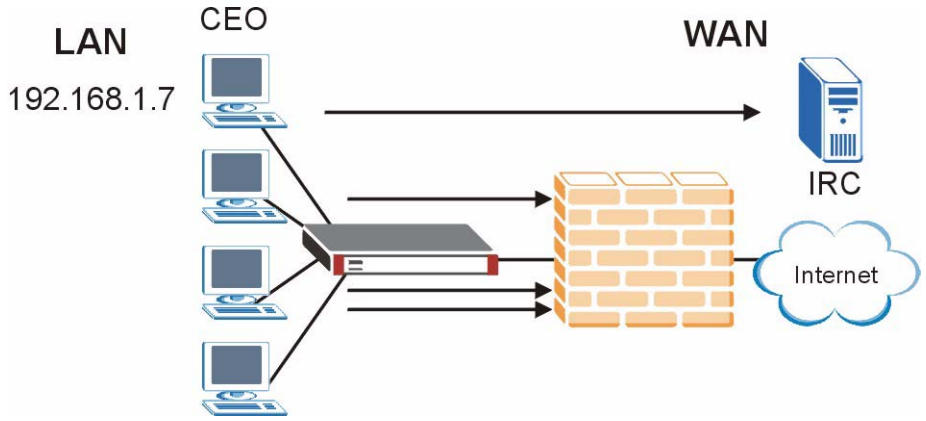
The ZyWALL applies the firewall rules in order. So for this example, when the ZyWALL receives traffic from the LAN, it checks it against the first rule. If the traffic matches (if it is IRC traffic) the firewall takes the action in the rule (drop) and stops checking the firewall rules. Any traffic that does not match the first firewall rule will match the default rule and the ZyWALL forwards it.

Now suppose that your company wants to let the CEO use IRC. You can configure a LAN to WAN firewall rule that allows IRC traffic from the IP address of the CEO's computer. 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 Section 7.3 on page 155 for information on static DHCP).

Now you configure a LAN 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 144** Limited LAN to WAN IRC Traffic Example




Your firewall would have the following configuration.

**Table 68** Limited LAN to WAN IRC Traffic Example

| # | SOURCE | DESTINATION | SCHEDULE | SERVICE | ACTION |
|---|---|---|---|---|---|
| 1 | 192.168.1.7 | Any | Any | IRC | Allow |
| 2 | Any | Any | Any | IRC | Drop |
| Default | Any | Any | Any | Any | Allow |

- The first row allows the LAN computer at IP address 192.168.1.7 to access the IRC service on the WAN.
- The second row blocks LAN access to the IRC service on the WAN.
- The third row is (still) the firewall's default policy of allowing all traffic from the LAN to go to the WAN.

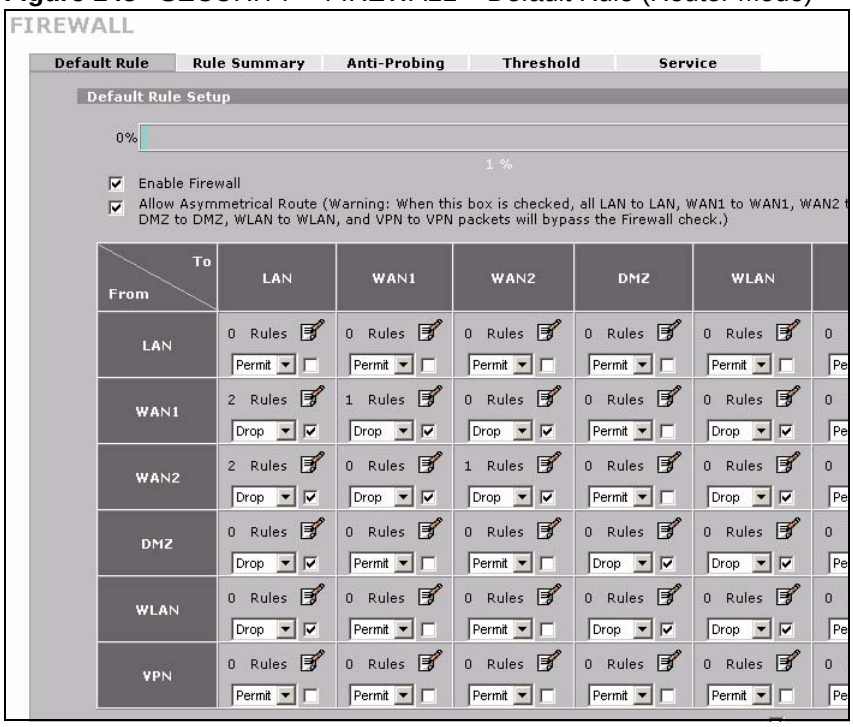
The rule for the CEO must come before the rule that blocks all LAN to WAN IRC traffic. If the rule that blocks all LAN to WAN IRC traffic came first, the CEO's IRC traffic would match that rule and the ZyWALL would drop it and not check any other firewall rules.

## 13.3 The Firewall Default Rule Screen

Click **SECURITY** > **FIREWALL** to open the **Default Rule** screen.

Use this screen to configure general firewall settings when the ZyWALL is in **Router** mode.

**Figure 145** SECURITY > FIREWALL > Default Rule (Router Mode)




The following table describes the labels in this screen.

**Table 69** SECURITY > FIREWALL > Default Rule (Router Mode)

| LABEL | DESCRIPTION |
|---|---|
| 0-100% | This bar displays the percentage of the ZyWALL's firewall rules storage space that is currently in use. When the storage space is almost full, you should consider deleting unnecessary firewall rules before adding more firewall rules. |
| Enable Firewall | Select this check box to activate the firewall. The ZyWALL performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.<br><br>Note: When you activate the firewall, all current connections through the ZyWALL are dropped when you apply your changes. |
| 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>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 IP alias to put the ZyWALL and the backup gateway on separate subnets. See Section 13.9 on page 271 for an example. |

**Table 69** SECURITY > FIREWALL > Default Rule (Router Mode) (continued)

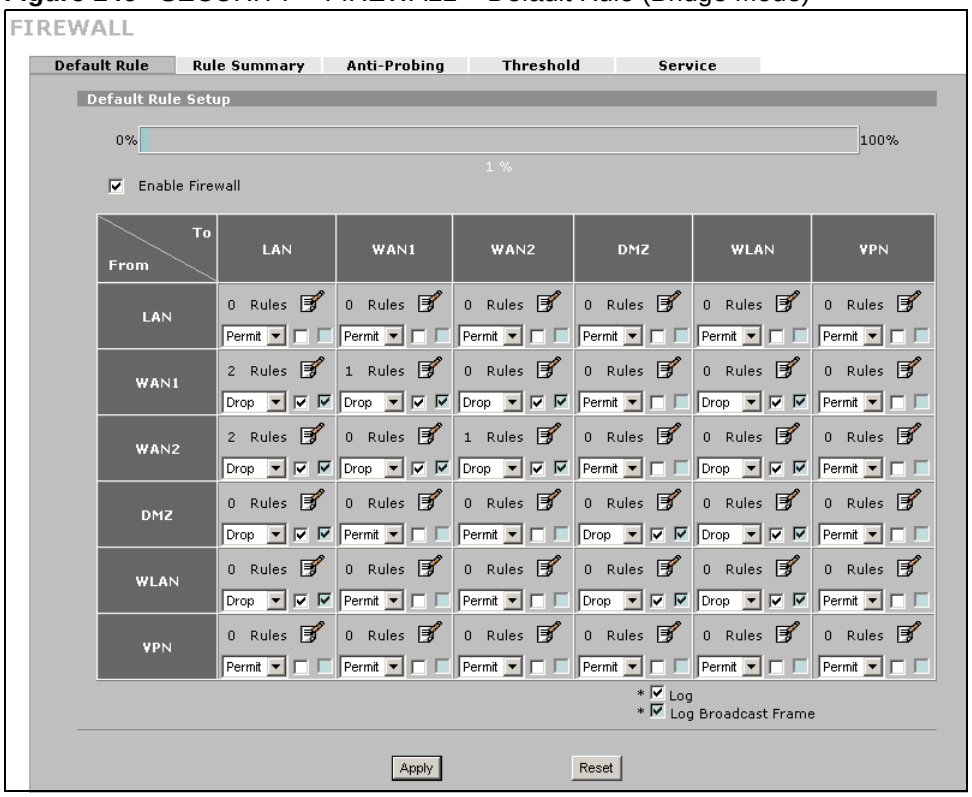
| LABEL | DESCRIPTION |
|---|---|
| From, To | The firewall rules are grouped by the direction of packet travel. The number of rules for each packet direction displays. Click **Edit** to go to a summary screen of the rules for that packet direction.<br>Here are some example descriptions of the directions of travel.<br>**From LAN To LAN** means packets traveling from a computer on one LAN subnet to a computer on another LAN subnet on the LAN interface of the ZyWALL or the ZyWALL itself. The ZyWALL does not apply the firewall to packets traveling from a LAN computer to another LAN computer on the same subnet.<br>**From VPN** means traffic that came into the ZyWALL through a VPN tunnel and is going to the selected "to" interface. For example, **From VPN To LAN** specifies the VPN traffic that is going to the LAN. The ZyWALL applies the firewall to the traffic after decrypting it.<br>**To VPN** is traffic that comes in through the selected "from" interface and goes out through any VPN tunnel. For example, **From LAN To VPN** specifies the traffic that is coming from the LAN and going out through a VPN tunnel. The ZyWALL applies the firewall to the traffic before encrypting it.<br>**From VPN To VPN** means traffic that comes in through a VPN tunnel and goes out through (another) VPN tunnel or terminates at the ZyWALL. This is the case when the ZyWALL is the hub in a hub-and-spoke VPN. This is also the case if you allow someone to use a service (like Telnet or HTTP) through a VPN tunnel to manage the ZyWALL. The ZyWALL applies the firewall to the traffic after decrypting it.<br>Note: The VPN connection directions apply to the traffic going to or from the ZyWALL's VPN tunnels. They do not apply to other VPN traffic for which the ZyWALL is not one of the gateways (VPN pass-through traffic).<br>Use the drop-down list box to set the firewall's default actions based on the direction of travel of packets.<br>Select **Drop** to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender.<br>Select **Reject** to deny the packets and send a TCP reset packet (for a TCP packet) or an ICMP destination-unreachable message (for a UDP packet) to the sender.<br>Select **Permit** to allow the passage of the packets.<br>The firewall rules for the WAN port with a higher route priority also apply to the dial backup connection. |
| Log | Select the check box next to a direction of packet travel to create a log when the configured action is taken for packets that are traveling in that direction and do not match any of your customized rules. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 13.4 The Firewall Default Rule (Bridge Mode) Screen

Click **SECURITY** > **FIREWALL** to open the **Default Rule** screen.

Use this screen to configure general firewall settings when the ZyWALL is in **Bridge** mode.

**Figure 146** SECURITY > FIREWALL > Default Rule (Bridge Mode)




The following table describes the labels in this screen.

**Table 70** SECURITY > FIREWALL > Default Rule (Bridge Mode)

| LABEL | DESCRIPTION |
|---|---|
| 0-100% | This bar displays the percentage of the ZyWALL's firewall rules storage space that is currently in use. When the storage space is almost full, you should consider deleting unnecessary firewall rules before adding more firewall rules. |
| Enable Firewall | Select this check box to activate the firewall. The ZyWALL performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.<br><br>Note: When you activate the firewall, all current connections through the ZyWALL are dropped when you apply your changes. |

**Table 70** SECURITY > FIREWALL > Default Rule (Bridge Mode) (continued)

| LABEL | DESCRIPTION |
|---|---|
| From, To | The firewall rules are grouped by the direction of packet travel. The number of rules for each packet direction displays. Click **Edit** to go to a summary screen of the rules for that packet direction.<br>Here are some example descriptions of the directions of travel.<br>**From LAN To LAN** means packets traveling from a computer on one LAN subnet to a computer on another LAN subnet on the LAN interface of the ZyWALL or the ZyWALL itself. The ZyWALL does not apply the firewall to packets traveling from a LAN computer to another LAN computer on the same subnet.<br>**From VPN** means traffic that came into the ZyWALL through a VPN tunnel and is going to the selected "to" interface. For example, **From VPN To LAN** specifies the VPN traffic that is going to the LAN. The ZyWALL applies the firewall to the traffic after decrypting it.<br>**To VPN** is traffic that comes in through the selected "from" interface and goes out through any VPN tunnel. For example, **From LAN To VPN** specifies the traffic that is coming from the LAN and going out through a VPN tunnel. The ZyWALL applies the firewall to the traffic before encrypting it.<br>**From VPN To VPN** means traffic that comes in through a VPN tunnel and goes out through (another) VPN tunnel or terminates at the ZyWALL. This is the case when the ZyWALL is the hub in a hub-and-spoke VPN. This is also the case if you allow someone to use a service (like Telnet or HTTP) through a VPN tunnel to manage the ZyWALL. The ZyWALL applies the firewall to the traffic after decrypting it.<br>Note: The VPN connection directions apply to the traffic going to or from the ZyWALL's VPN tunnels. They do not apply to other VPN traffic for which the ZyWALL is not one of the gateways (VPN pass-through traffic).<br>Use the drop-down list box to set the firewall's default actions based on the direction of travel of packets.<br>Select **Drop** to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender.<br>Select **Reject** to deny the packets and send a TCP reset packet (for a TCP packet) or an ICMP destination-unreachable message (for a UDP packet) to the sender.<br>Select **Permit** to allow the passage of the packets.<br>The firewall rules for the WAN port with a higher route priority also apply to the dial backup connection. |
| Log | Select the check box next to a direction of packet travel to create a log when the configured action is taken for packets that are traveling in that direction and do not match any of your customized rules. |
| Log Broadcast Frame (Bridge mode only) | Select this to create a log for any broadcast frames traveling in the selected direction. Many of these logs in a short time period could indicate a broadcast storm. A broadcast storm occurs when a packet triggers multiple responses from all hosts on a network or when computers attempt to respond to a host that never replies. As a result, duplicated packets are continuously created and circulated in the network, thus reducing network performance or even rendering it inoperable. A broadcast storm can be caused by an attack on the network, an incorrect network topology (such as a bridge loop) or a malfunctioning network device. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

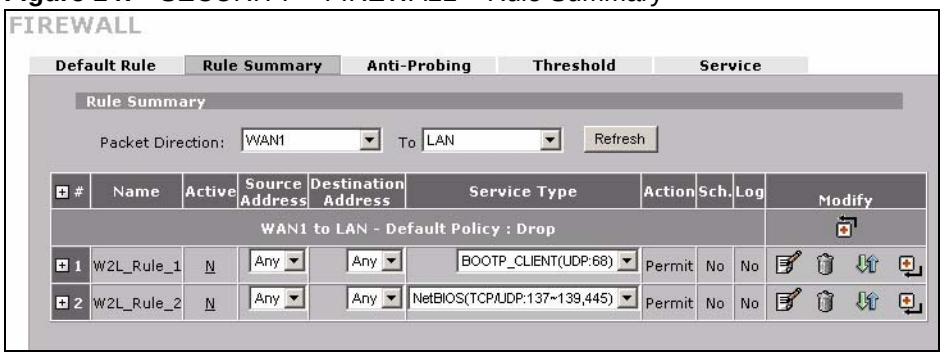
# 13.5 The Firewall Rule Summary Screen

Click **SECURITY** > **FIREWALL** > **Rule Summary** to open the screen. This screen displays a list of the configured firewall rules.

The ordering of your rules is very important as rules are applied in the order that they are listed.

See Section 13.1 on page 251 for more information about the firewall.

**Figure 147** SECURITY > FIREWALL > Rule Summary




The following table describes the labels in this screen.

**Table 71** SECURITY > FIREWALL > Rule Summary

| LABEL | DESCRIPTION |
|---|---|
| Packet Direction | Use the drop-down list boxes and click **Refresh** to select a direction of travel of packets for which you want to display firewall rules.<br><br>Note: The VPN connection directions apply to the traffic going to or from the ZyWALL's VPN tunnels. They do not apply to other VPN traffic for which the ZyWALL is not one of the gateways (VPN pass-through traffic). |
| +/- | In the heading row, click + to expand or - to collapse the **Source Address**, **Destination Address** and **Service Type** drop down lists for all of the displayed rules. |
| Default Policy | This field displays the default action you selected in the **Default Rule** screen for the packet direction displayed. |
| The following fields summarize the rules you have created that apply to traffic traveling in the selected packet direction. The firewall rules that you configure (summarized below) take priority over the general firewall action settings above. | |
| # | This is your firewall rule number. The ordering of your rules is important as rules are applied in turn. Click + to expand or - to collapse the **Source Address**, **Destination Address** and **Service Type** drop down lists. |
| Name | This is the name of the firewall rule. |
| Active | This field displays whether a firewall is turned on (**Y**) or not (**N**). Click the setting to change it. |

**Table 71** SECURITY > FIREWALL > Rule Summary

| LABEL | DESCRIPTION |
|---|---|
| Source Address | This drop-down list box displays the source addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to **Any**. |
| Destination Address | This drop-down list box displays the destination addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to **Any**. |
| Service Type | This drop-down list box displays the services to which this firewall rule applies. Custom services have an * before the name. See Appendix B on page 783 for a list of common services. |
| Action | This field displays whether the firewall silently discards packets (**Drop**), discards packets and sends a TCP reset packet or an ICMP destination-unreachable message to the sender (**Reject**) or allows the passage of packets (**Permit**). |
| Sch. | This field tells you whether a schedule is specified (**Yes**) or not (**No**). |
| Log | This field shows you whether a log is created when packets match this rule (**Yes**) or not (**No**). |
| Modify | Click the edit icon to go to the screen where you can edit the rule.<br>Click the delete icon to delete an existing firewall rule. A window displays asking you to confirm that you want to delete the firewall rule. Note that subsequent firewall rules move up by one when you take this action.<br>Click the move icon, type an index number, and press Enter to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering.<br>Click the insert icon to display the screen where you can configure a new firewall rule. The insert icon at the top of the row creates the new firewall rule before the others. The individual firewall rule insert icons create a new firewall rule after the row's firewall rule. |

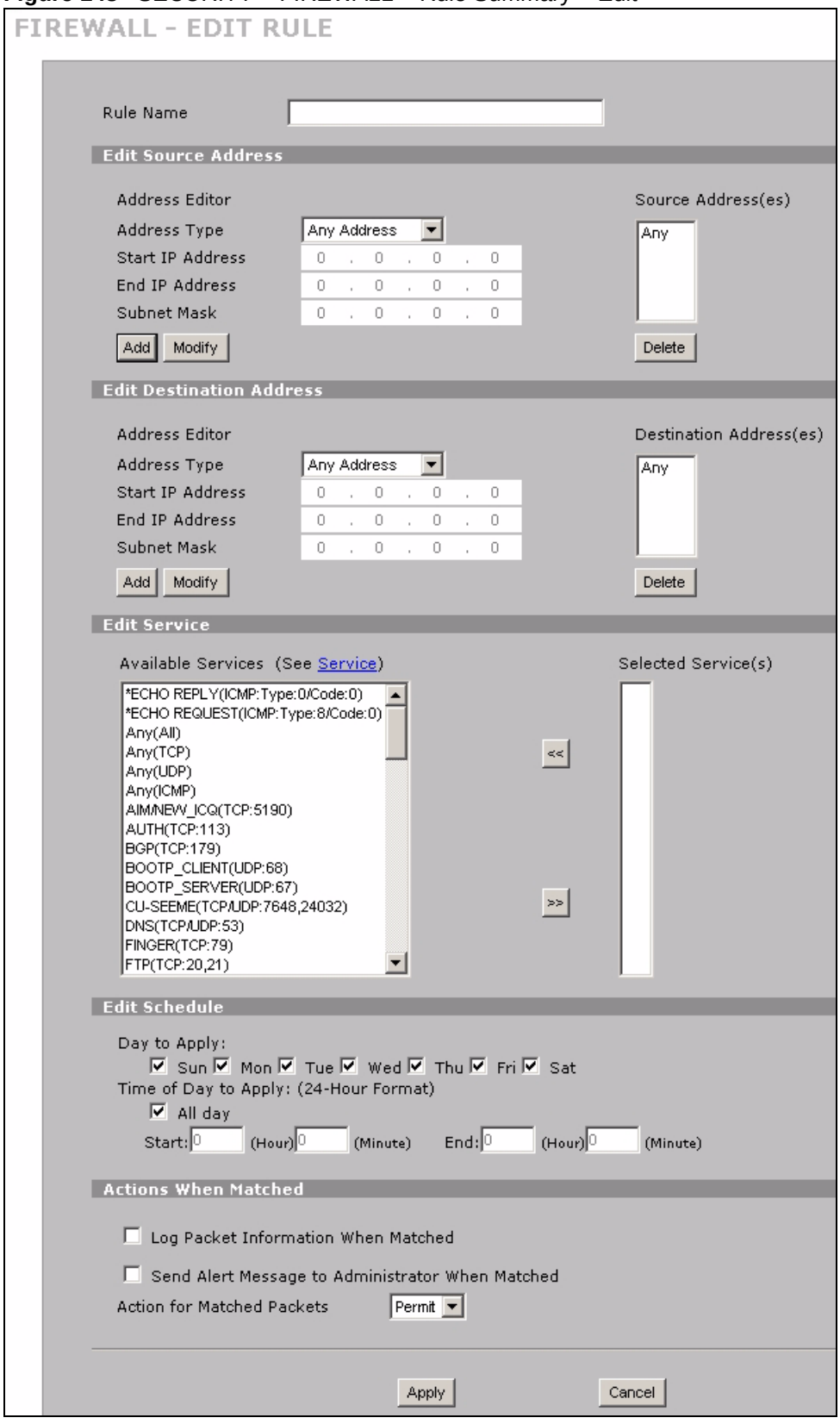
## 13.5.1 The Firewall Edit Rule Screen

In the **Rule Summary** screen, click the edit icon or the insert icon to display the **Firewall Edit Rule** screen.

Use this screen to create or edit a firewall rule. Refer to the following table for information on the labels.

See Section 13.1 on page 251 for more information about the firewall.

**Figure 148** SECURITY > FIREWALL > Rule Summary > Edit



The following table describes the labels in this screen.

**Table 72** SECURITY > FIREWALL > Rule Summary > Edit

| LABEL | DESCRIPTION |
|---|---|
| Rule Name | Enter a descriptive name of up to 31 printable ASCII characters (except Extended ASCII characters) for the firewall rule. Spaces are allowed. |
| Edit Source/ Destination Address | |
| Address Type | Do you want your rule to apply to packets with a particular (single) IP, a range of IP addresses (for example 192.168.1.10 to 192.169.1.50), a subnet or any IP address? Select an option from the drop-down list box that includes: **Single Address**, **Range Address**, **Subnet Address** and **Any Address**. |
| Start IP Address | Enter the single IP address or the starting IP address in a range here. |
| End IP Address | Enter the ending IP address in a range here. |
| Subnet Mask | Enter the subnet mask here, if applicable. |
| Add | Click **Add** to add a new address to the **Source** or **Destination Address(es)** box. You can add multiple addresses, ranges of addresses, and/or subnets. |
| Modify | To edit an existing source or destination address, select it from the box and click **Modify**. |
| Delete | Highlight an existing source or destination address from the **Source** or **Destination Address(es)** box and click **Delete** to remove it. |
| Edit Service | |
| Available/ Selected Services | Highlight a service from the **Available Services** box on the left, then click **>>** to add it to the **Selected Service(s)** box on the right. To remove a service, highlight it in the **Selected Service(s)** box on the right, then click **<<**.<br>Custom services have an * before the name.<br>Next to the name of a service, two fields appear in brackets. The first field indicates the IP protocol type (TCP, UDP, or ICMP). The second field indicates the IP port number that defines the service. (Note that there may be more than one IP protocol type). For example, look at the DNS entry, (UDP/TCP:53) means UDP port 53 and TCP port 53. Click the **Service** link to go to the **Service screen where you can** configure custom service ports. See Appendix B on page 783 for a list of commonly used services and port numbers.<br>You can use the [CTRL] key and select multiple services at once. |
| Edit Schedule | |
| Day to Apply | Select everyday or the day(s) of the week to apply the rule. |
| Time of Day to Apply (24-Hour Format) | Select **All Day** or enter the start and end times in the hour-minute format to apply the rule. |
| Actions When Matched | |
| Log Packet Information When Matched | This field determines if a log for packets that match the rule is created (**Yes**) or not (**No**). Go to the **Log Settings** page and select the **Access Control** logs category to have the ZyWALL record these logs. |
| Send Alert Message to Administrator When Matched | Select the check box to have the ZyWALL generate an alert when the rule is matched. |

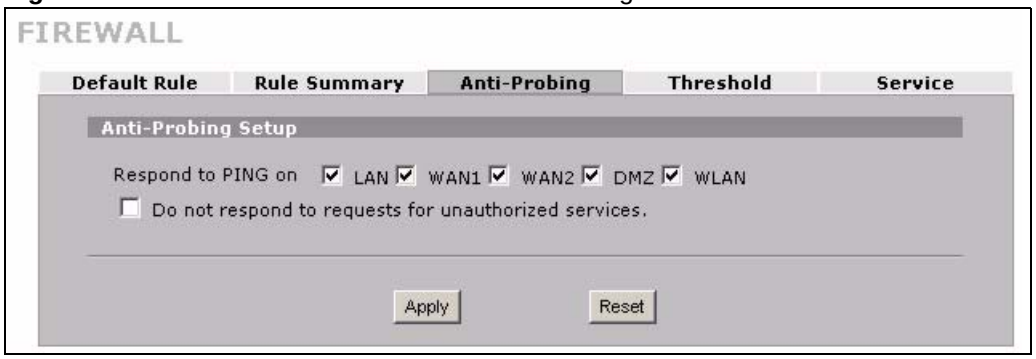
**Table 72** SECURITY > FIREWALL > Rule Summary > Edit

| LABEL | DESCRIPTION |
|---|---|
| Action for Matched Packets | Use the drop-down list box to select what the firewall is to do with packets that match this rule.<br>Select **Drop** to silently discard the packets without sending a TCP reset packet or an ICMP destination-unreachable message to the sender.<br>Select **Reject** to deny the packets and send a TCP reset packet (for a TCP packet) or an ICMP destination-unreachable message (for a UDP packet) to the sender.<br>Select **Permit** to allow the passage of the packets.<br><br>Note: You also need to configure NAT port forwarding (or full featured NAT address mapping rules) if you want to allow computers on the WAN to access devices on the LAN.<br><br>Note: You may also need to configure the remote management settings if you want to allow a WAN computer to manage the ZyWALL or restrict management from the LAN. |
| Apply | Click **Apply** to save your customized settings and exit this screen. |
| Cancel | Click **Cancel** to exit this screen without saving. |

## 13.6 The Anti-Probing Screen

Click **SECURITY** > **FIREWALL** > **Anti-Probing** to open the following screen. Configure this screen to help keep the ZyWALL hidden from probing attempts. You can specify which of the ZyWALL's interfaces will respond to Ping requests and whether or not the ZyWALL is to respond to probing for unused ports.

**Figure 149** SECURITY > FIREWALL > Anti-Probing



The following table describes the labels in this screen.

**Table 73** SECURITY > FIREWALL > Anti-Probing

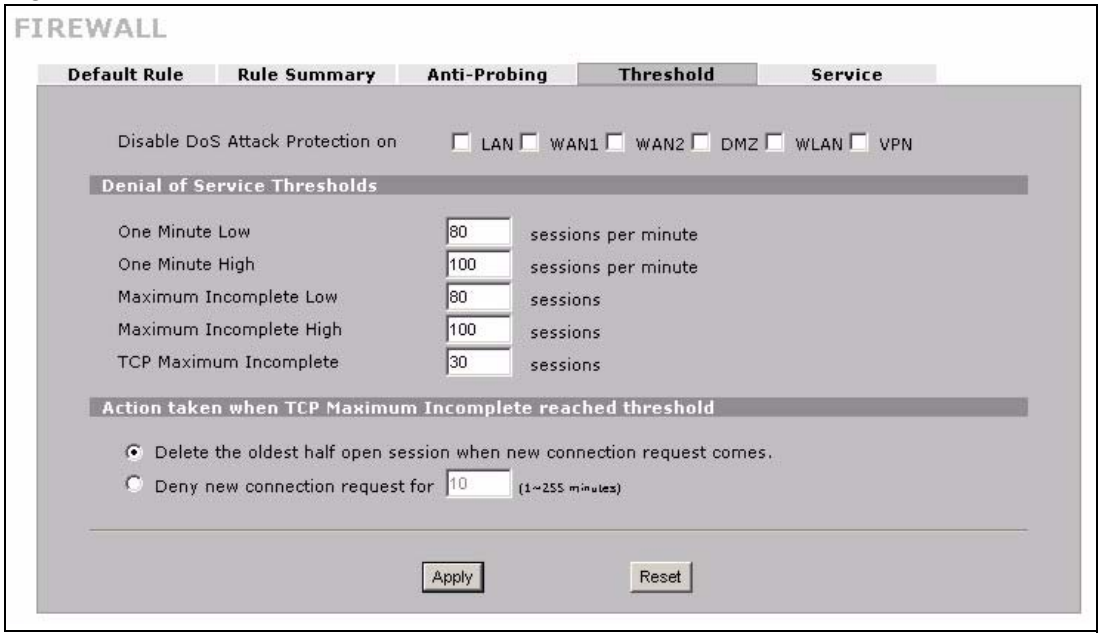
| LABEL | DESCRIPTION |
|---|---|
| Respond to PING on | Select the check boxes of the interfaces that you want to reply to incoming Ping requests.<br>Clear an interface's check box to have the ZyWALL not respond to any Ping requests that come into that interface. |
| Do not respond to requests for unauthorized services. | Select this option to prevent hackers from finding the ZyWALL by probing for unused ports. If you select this option, the ZyWALL will not respond to port request(s) for unused ports, thus leaving the unused ports and the ZyWALL unseen. If this option is not selected, the ZyWALL will reply with an ICMP port unreachable packet for a port probe on its unused UDP ports and a TCP reset packet for a port probe on its unused TCP ports.<br>Note that the probing packets must first traverse the ZyWALL's firewall rule checks before reaching this anti-probing mechanism. Therefore if a firewall rule stops a probing packet, the ZyWALL reacts based on the firewall rule to either send a TCP reset packet for a blocked TCP packet (or an ICMP port-unreachable packet for a blocked UDP packets) or just drop the packets without sending a response packet. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 13.7 The Firewall Thresholds Screen

For DoS attacks, the ZyWALL uses thresholds to determine when to start dropping sessions that do not become fully established (half-open sessions). These thresholds apply globally to all sessions. See Threshold Values on page 275 for more information on DoS thresholds.

Click **SECURITY** > **FIREWALL** > **Threshold** to bring up the next screen. The global values specified for the threshold and timeout apply to all TCP connections.

**Figure 150** SECURITY > FIREWALL > Threshold



The following table describes the labels in this screen.

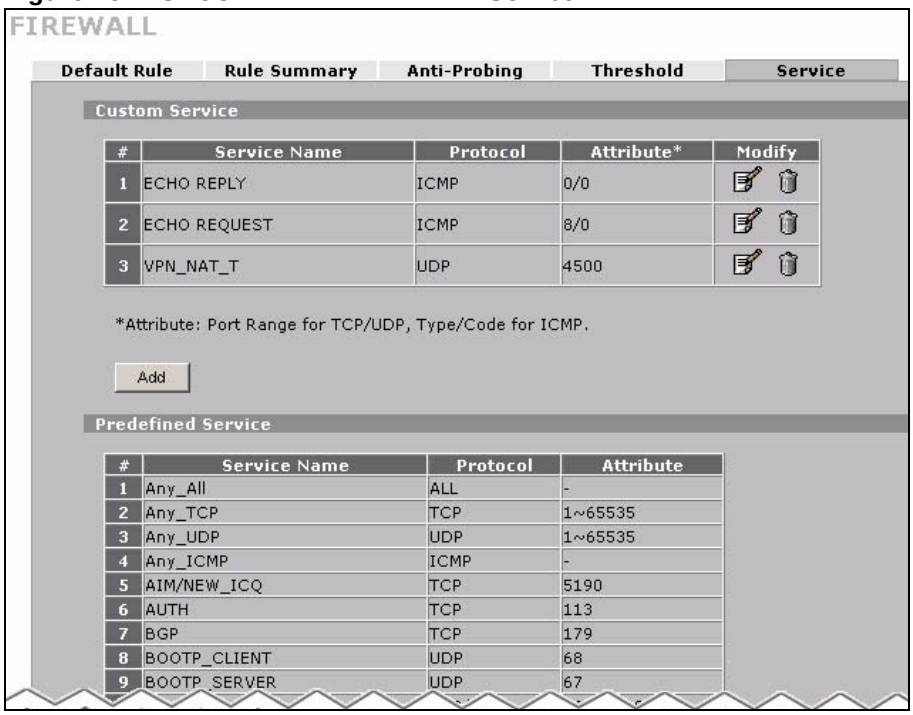
**Table 74** SECURITY > FIREWALL > Threshold

| LABEL | DESCRIPTION |
|---|---|
| Disable DoS Attack Protection on | Select the check boxes of any interfaces (or all VPN tunnels) for which you want the ZyWALL to not use the Denial of Service protection thresholds. This disables DoS protection on the selected interface (or all VPN tunnels).<br>You may want to disable DoS protection for an interface if the ZyWALL is treating valid traffic as DoS attacks. Another option would be to raise the thresholds. |
| Denial of Service Thresholds | The ZyWALL measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are counted in the total number and rate measurements. Measurements are made once a minute. |
| One Minute Low | This is the rate of new half-open sessions per minute that causes the firewall to stop deleting half-open sessions. The ZyWALL continues to delete half-open sessions as necessary, until the rate of new connection attempts drops below this number. |
| One Minute High | This is the rate of new half-open sessions per minute that causes the firewall to start deleting half-open sessions. When the rate of new connection attempts rises above this number, the ZyWALL deletes half-open sessions as required to accommodate new connection attempts.<br>For example, if you set the one minute high to 100, the ZyWALL starts deleting half-open sessions when more than 100 session establishment attempts have been detected in the last minute. It stops deleting half-open sessions when the number of session establishment attempts detected in a minute goes below the number set as the one minute low. |
| Maximum Incomplete Low | This is the number of existing half-open sessions that causes the firewall to stop deleting half-open sessions. The ZyWALL continues to delete half-open requests as necessary, until the number of existing half-open sessions drops below this number. |
| Maximum Incomplete High | This is the number of existing half-open sessions that causes the firewall to start deleting half-open sessions. When the number of existing half-open sessions rises above this number, the ZyWALL deletes half-open sessions as required to accommodate new connection requests. Do not set **Maximum Incomplete High** to lower than the current **Maximum Incomplete Low** number.<br>For example, if you set the maximum incomplete high to 100, the ZyWALL starts deleting half-open sessions when the number of existing half-open sessions rises above 100. It stops deleting half-open sessions when the number of existing half-open sessions drops below the number set as the maximum incomplete low. |
| TCP Maximum Incomplete | An unusually high number of half-open sessions with the same destination host address could indicate that a DoS attack is being launched against the host.<br>Specify the number of existing half-open TCP sessions with the same destination host IP address that causes the firewall to start dropping half-open sessions to that same destination host IP address. Enter a number between 1 and 256. As a general rule, you should choose a smaller number for a smaller network, a slower system or limited bandwidth. The ZyWALL sends alerts whenever the **TCP Maximum Incomplete** is exceeded. |
| Action taken when TCP Maximum Incomplete reached threshold | Select the action that ZyWALL should take when the TCP maximum incomplete threshold is reached. You can have the ZyWALL either:<br>Delete the oldest half open session when a new connection request comes.<br>or<br>Deny new connection requests for the number of minutes that you specify (between 1 and 256). |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# 13.8 The Firewall Services Screen

Click **SECURITY** > **FIREWALL** > **Service** to open the screen as shown next. Use this screen to configure custom services for use in firewall rules or view the services that are predefined in the ZyWALL.

**Figure 151** SECURITY > FIREWALL > Service




The following table describes the labels in this screen.

**Table 75** SECURITY > FIREWALL > Service

| LABEL | DESCRIPTION |
|---|---|
| Custom Service | This table shows all configured custom services. |
| # | This is the index number of the custom service. |
| Service Name | This is the name of the service. |
| Protocol | This is the IP protocol type.<br>If you selected **Custom**, this is the IP protocol value you entered. |
| Attribute | This is the IP port number or ICMP type and code that defines the service. |
| Modify | Click the edit icon to go to the screen where you can edit the service.<br>Click the delete icon to remove an existing service. A window displays asking you to confirm that you want to delete the service. Note that subsequent services move up by one when you take this action. |
| Add | Click this button to bring up the screen that you use to configure a new custom service that is not in the predefined list of services. |
| Predefined Service | This table shows all the services that are already configured for use in firewall rules. See Appendix B on page 783 for a list of common services. |
| # | This is the index number of the predefined service. |
| Service Name | This is the name of the service. |

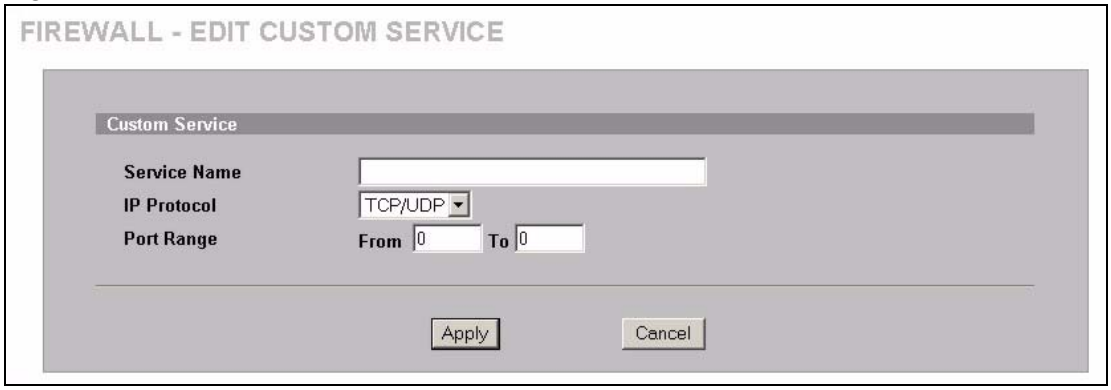
**Table 75** SECURITY > FIREWALL > Service (continued)

| LABEL | DESCRIPTION |
|---|---|
| Protocol | This is the IP protocol type. There may be more than one IP protocol type. |
| Attribute | This is the IP port number or ICMP type and code that defines the service. |

## 13.8.1 The Firewall Edit Custom Service Screen

Click **SECURITY** > **FIREWALL** > **Service** > **Add** to display the following screen. Use this screen to configure a custom service entry not is not predefined in the ZyWALL. See Appendix B on page 783 for a list of commonly used services and port numbers.

**Figure 152** SECURITY > FIREWALL > Service > Add




The following table describes the labels in this screen.

**Table 76** SECURITY > FIREWALL > Service > Add

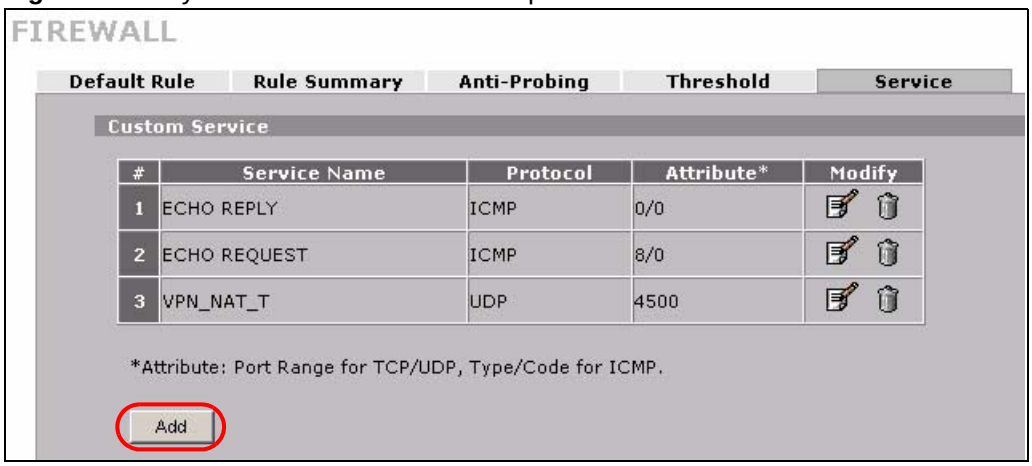
| LABEL | DESCRIPTION |
|---|---|
| Service Name | Enter a descriptive name of up to 31 printable ASCII characters (except Extended ASCII characters) for the custom service. You cannot use the “(“character. Spaces are allowed. |
| IP Protocol | Choose the IP protocol (**TCP**, **UDP**, **TCP/UDP**, **ICMP** or **Custom**) that defines your customized service from the drop down list box.<br>If you select **Custom**, specify the protocol’s number. For example, ICMP is 1, TCP is 6, UDP is 17 and so on. |
| Port Range | Enter the port number (from 1 to 255) that defines the customized service<br>To specify one port only, enter the port number in the **From** field and enter it again in the **To** field.<br>To specify a span of ports, enter the first port in the **From** field and enter the last port in the **To** field. |
| Type/Code | This field is available only when you select **ICMP** in the **IP Protocol** field.<br>The ICMP messages are identified by their types and in some cases codes.<br>Enter the type number in the **Type** field and select **Code** and enter the code number if any. |
| Apply | Click **Apply** to save your customized settings and exit this screen. |
| Cancel | Click **Cancel** to exit this screen without saving. |

## 13.8.2 My Service Firewall Rule Example

The following Internet firewall rule example allows a hypothetical My Service connection from the Internet.

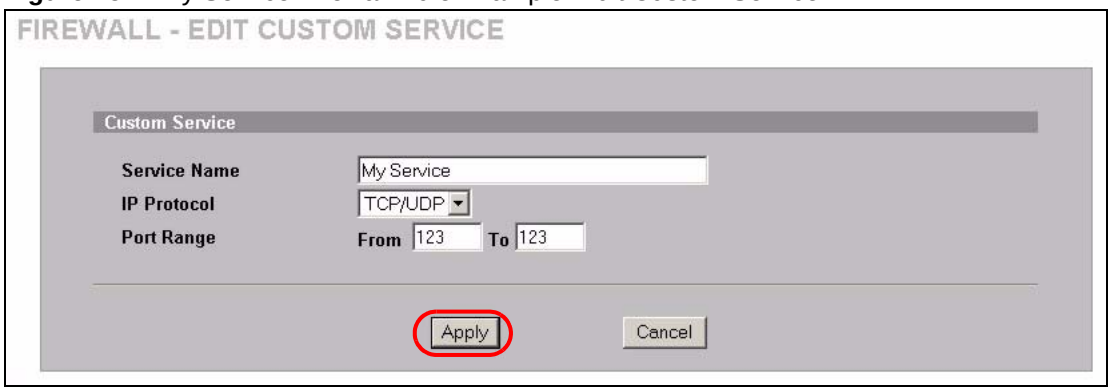
1 In the **Service** screen, click **Add** to open the **Edit Custom Service** screen.

**Figure 153** My Service Firewall Rule Example: Service




2 Configure it as follows and click **Apply**.

**Figure 154** My Service Firewall Rule Example: Edit Custom Service

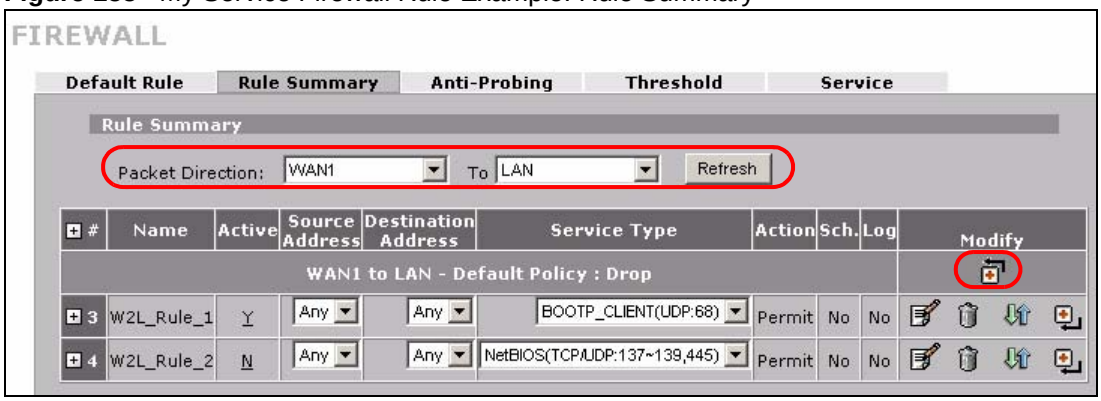



3 Click **Rule Summary**. Select **WAN1** to **LAN** from the **Packet Direction** drop-down list boxes and click **Refresh**.

4 In the **Rule Summary** screen, type the index number for where you want to put the rule. For example, if you type 6, your new rule becomes number 6 and the previous rule 6 (if there is one) becomes rule 7.

5 Click **Insert** at the top of the **Modify** column to display the firewall rule configuration screen.

**Figure 155** My Service Firewall Rule Example: Rule Summary

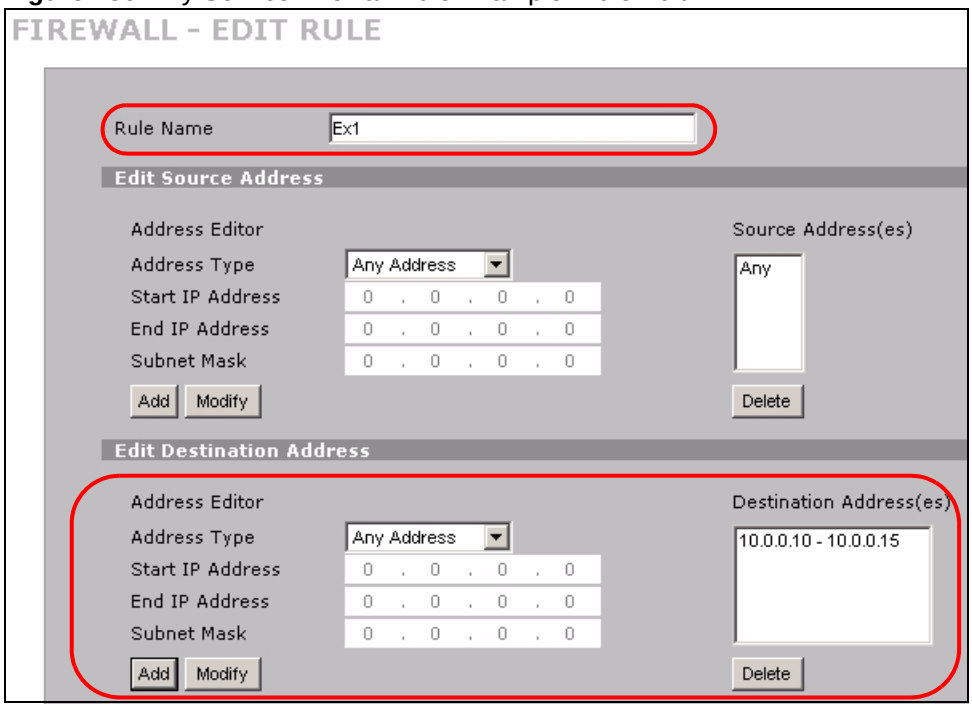



6 Enter the name of the firewall rule.

7 Select **Any** in the **Destination Address(es)** box and then click **Delete**.

8 Configure the destination address fields as follows and click **Add**.

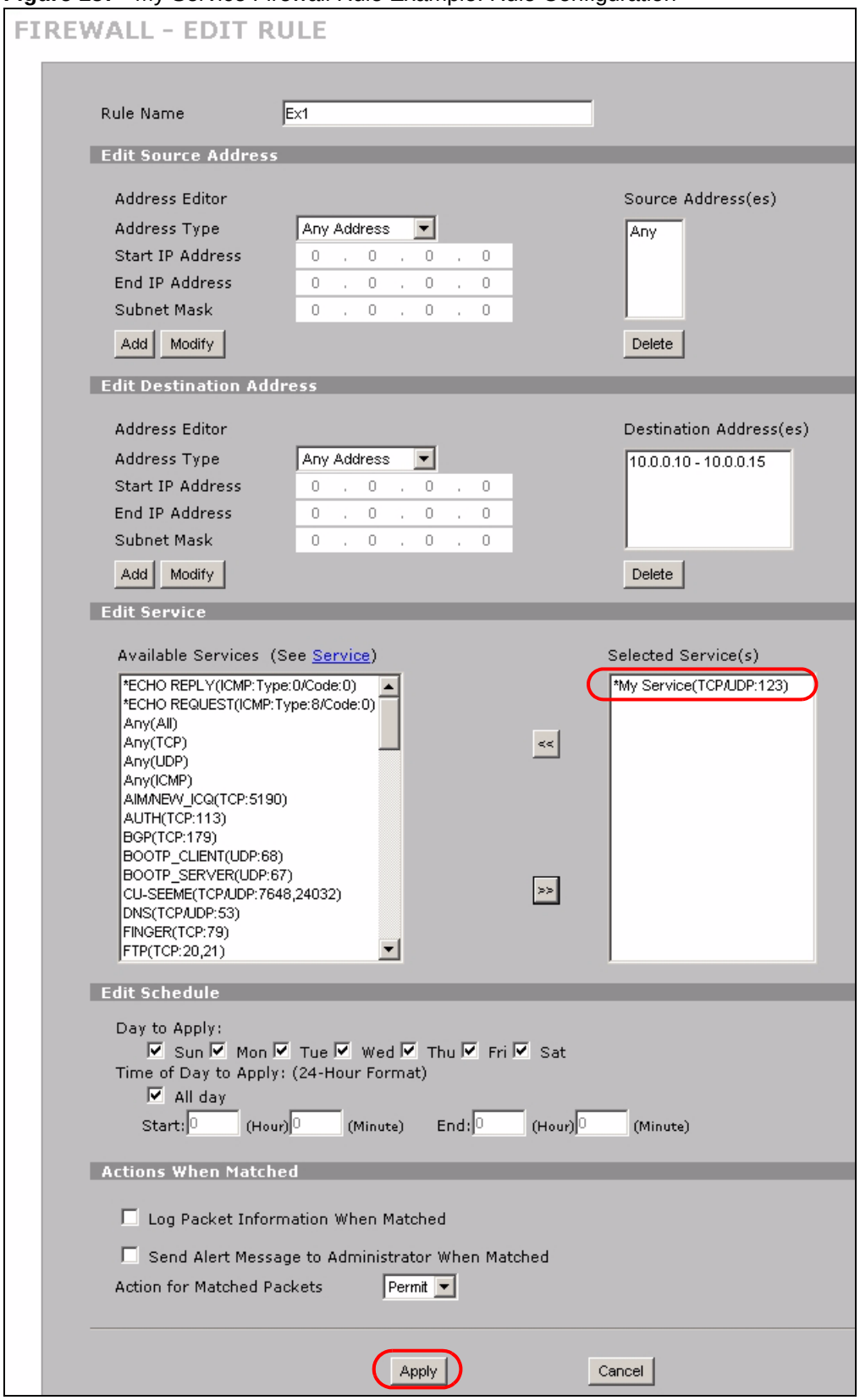
**Figure 156** My Service Firewall Rule Example: Rule Edit




9 In the **Edit Rule** screen, use the arrows between **Available Services** and **Selected Service(s)** to configure it as follows. Click **Apply** when you are done.

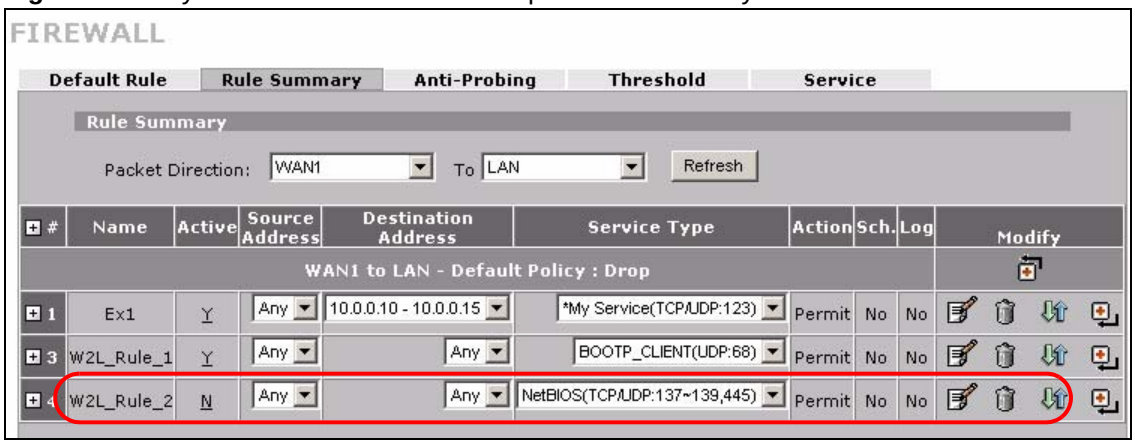
Custom services show up with an * before their names in the **Services** list box and the **Rule Summary** list box.

**Figure 157** My Service Firewall Rule Example: Rule Configuration



Rule 1 allows a My Service connection from the WAN to IP addresses 10.0.0.10 through 10.0.0.15 on the LAN.

**Figure 158** My Service Firewall Rule Example: Rule Summary




## 13.9 Technical Reference

This technical reference contains the following sections:

- Packet Direction Examples
- Asymmetrical Routes
- DoS Thresholds
- Security Considerations

## Packet Direction Examples

Firewall rules are grouped based on the direction of travel of packets to which they apply. This section gives some examples of why you might configure firewall rules for specific connection directions.

By default, the ZyWALL allows packets traveling in the following directions.:

- LAN to LAN — These rules specify which computers on the LAN can manage the ZyWALL (remote management) and communicate between networks or subnets connected to the LAN interface (IP alias).

  Note: You can also configure the remote management settings to allow only a specific computer to manage the ZyWALL.

- LAN to WAN 1 — These rules specify which computers on the LAN can access which computers or services connected to WAN 1. See Section 13.2 on page 252 for an example.

By default, the ZyWALL drops packets traveling in the following directions.

- WAN 1 to LAN These rules specify which computers connected to WAN 1 can access which computers or services on the LAN. For example, you may create rules to:
  - Allow certain types of traffic, such as Lotus Notes database synchronization, from specific hosts on the Internet to specific hosts on the LAN.
  - Allow public access to a Web server on your protected network. You could also block certain IP addresses from accessing it.

  Note: You also need to configure NAT port forwarding (or full featured NAT address mapping rules) to allow computers on the WAN to access devices on the LAN. See Section 22.4.3 on page 442 for an example.

- WAN to WAN By default the ZyWALL stops computers connected to WAN1 or WAN2 from managing the ZyWALL or using the ZyWALL as a gateway to communicate with other computers on the WAN. You could configure one of these rules to allow a WAN computer to manage the ZyWALL.

  Note: You also need to configure the remote management settings to allow a WAN computer to manage the ZyWALL.

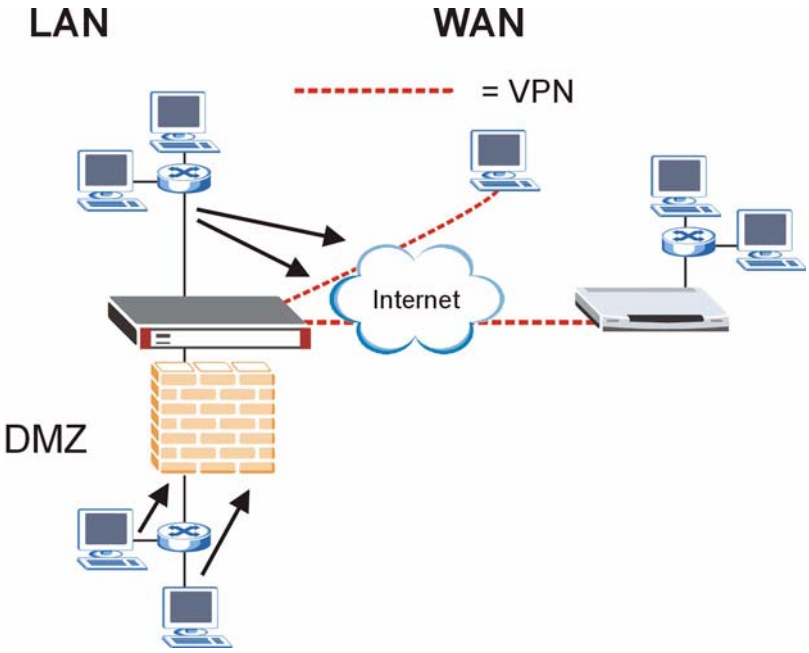
See Chapter 5 on page 109 for information about packets traveling to or from the VPN tunnels.

### To VPN Packet Direction

The ZyWALL can apply firewall rules to traffic before encrypting it to send through a VPN tunnel. **To VPN** means traffic that comes in through the selected “from” interface and goes out through any of the ZyWALL’s VPN tunnels. For example, **From LAN To VPN** specifies the traffic that is coming from the LAN and going out through any of the ZyWALL’s VPN tunnels.

For example, by default the **From LAN To VPN** default firewall rule allows traffic from the LAN computers to go out through any of the ZyWALL’s VPN tunnels. You could configure the **From DMZ To VPN** default rule to set the ZyWALL to silently block traffic from the DMZ computers from going out through any of the ZyWALL’s VPN tunnels.

**Figure 159** From LAN to VPN Example

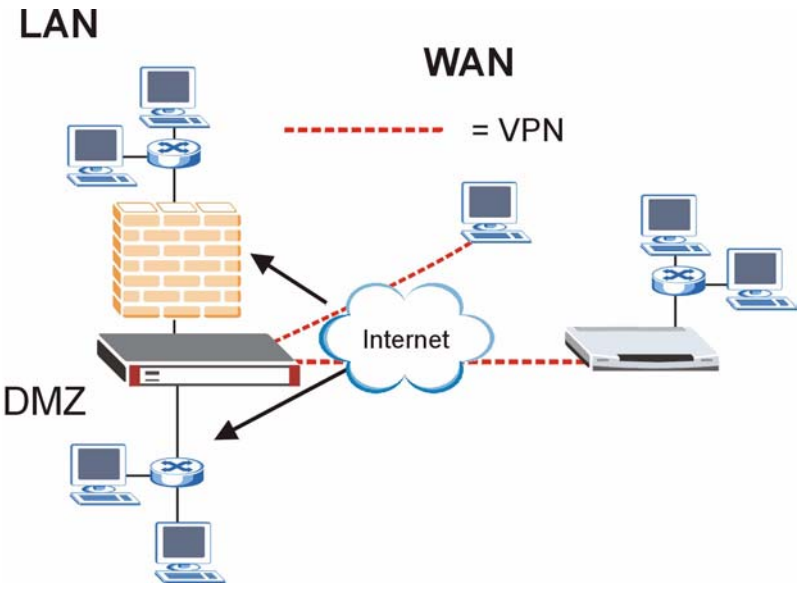



## From VPN Packet Direction

You can also apply firewall rules to traffic that comes in through the ZyWALL's VPN tunnels. The ZyWALL decrypts the VPN traffic and then applies the firewall rules. **From VPN** means traffic that came into the ZyWALL through a VPN tunnel and is going to the selected "to" interface.

For example, by default the firewall allows traffic from any VPN tunnel to go to any of the ZyWALL's interfaces, the ZyWALL itself and other VPN tunnels. You could edit the **From VPN To LAN** default firewall rule to silently block traffic from the VPN tunnels from going to the LAN computers.

**Figure 160** From VPN to LAN Example

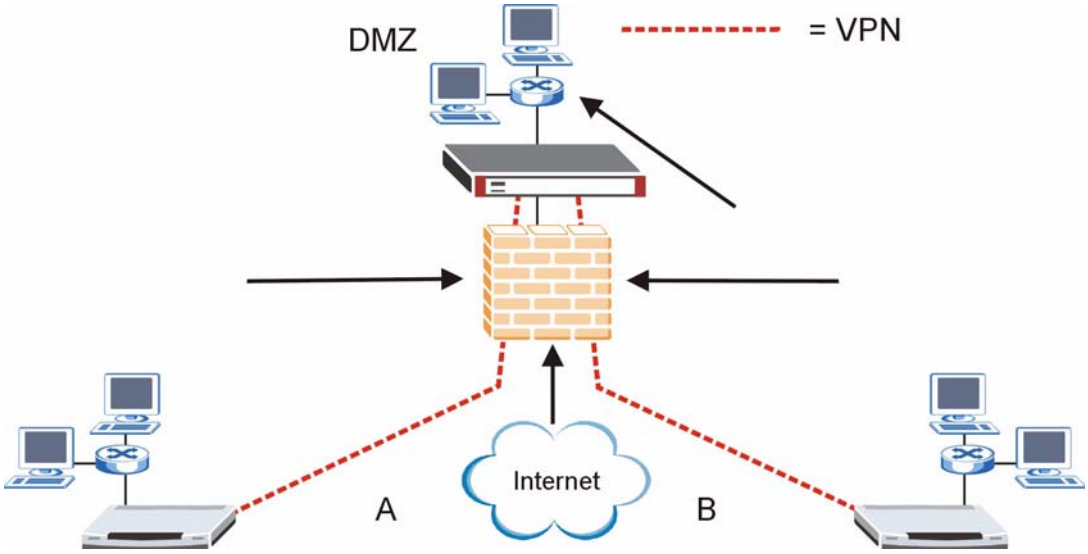


## From VPN To VPN Packet Direction

**From VPN To VPN** firewall rules apply to traffic that comes in through one of the ZyWALL's VPN tunnels and terminates at the ZyWALL (like for remote management) or goes out through another of the ZyWALL's VPN tunnels (this is called hub-and-spoke VPN, see Section 19.13 on page 385 for details). The ZyWALL decrypts the traffic and applies the firewall rules before re-encrypting it or allowing the traffic to terminate at the ZyWALL.

In the following example, the **From VPN To VPN** default firewall rule silently blocks the traffic that the ZyWALL receives from any VPN tunnel (either A or B) that is destined for the other VPN tunnel or the ZyWALL itself. VPN traffic destined for the DMZ is allowed through.

**Figure 161** From VPN to VPN Example




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).

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 IP alias to put the ZyWALL and the backup gateway on separate subnets.

## Asymmetrical Routes and IP Alias

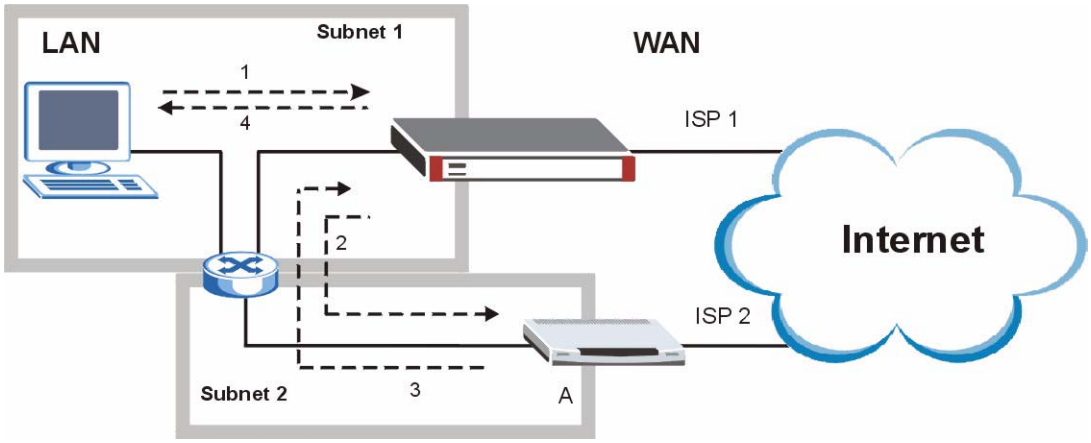
You can use IP alias instead of allowing asymmetrical routes. IP Alias allow you to partition your network into logical sections over the same interface.

By putting your LAN and Gateway **A** in different subnets, all returning network traffic must pass through the ZyWALL to your LAN. The following steps describe such a scenario.

1. A computer on the LAN 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 LAN in **Subnet 1**.

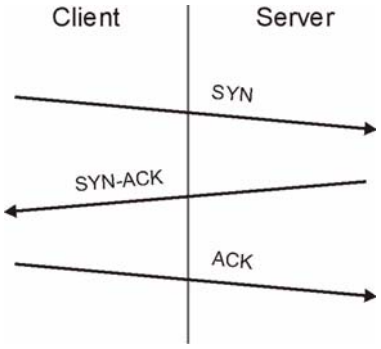
**Figure 162** Using IP Alias to Solve the Triangle Route Problem




# DoS Thresholds

For TCP, half-open means that the session has not reached the established state-the TCP three-way handshake has not yet been completed. Under normal circumstances, the application that initiates a session sends a SYN (synchronize) packet to the receiving server. The receiver sends back 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 163** Three-Way Handshake




For UDP, half-open means that the firewall has detected no return traffic. An unusually high number (or arrival rate) of half-open sessions could indicate a DOS attack.

## Threshold Values

If everything is working properly, you probably do not need to change the threshold settings as the default threshold values should work for most small offices. Tune these parameters when you believe the ZyWALL has been receiving DoS attacks that are not recorded in the logs or the logs show that the ZyWALL is classifying normal traffic as DoS attacks. Factors influencing choices for threshold values are:

1. The maximum number of opened sessions.
2. The minimum capacity of server backlog in your LAN network.
3. The CPU power of servers in your LAN network.
4. Network bandwidth.
5. Type of traffic for certain servers.

Reduce the threshold values if your network is slower than average for any of these factors (especially if you have servers that are slow or handle many tasks and are often busy).

If you often use P2P applications such as file sharing with eMule or eDonkey, it's recommended that you increase the threshold values since lots of sessions will be established during a small period of time and the ZyWALL may classify them as DoS attacks.

## Security Considerations

Incorrectly configuring the firewall may block valid access or introduce security risks to the ZyWALL and your protected network. Use caution when creating or deleting firewall rules and test your rules after you configure them.

Consider these security ramifications before creating a rule:

1. Does this rule stop LAN users from accessing critical resources on the Internet? For example, if IRC is blocked, are there users that require this service?
2. Is it possible to modify the rule to be more specific? For example, if IRC is blocked for all users, will a rule that blocks just certain users be more effective?
3. Does a rule that allows Internet users access to resources on the LAN create a security vulnerability? For example, if FTP ports (TCP 20, 21) are allowed from the Internet to the LAN, Internet users may be able to connect to computers with running FTP servers.
4. Does this rule conflict with any existing rules?

Once these questions have been answered, adding rules is simply a matter of entering the information into the correct fields in the web configurator screens.

# 14

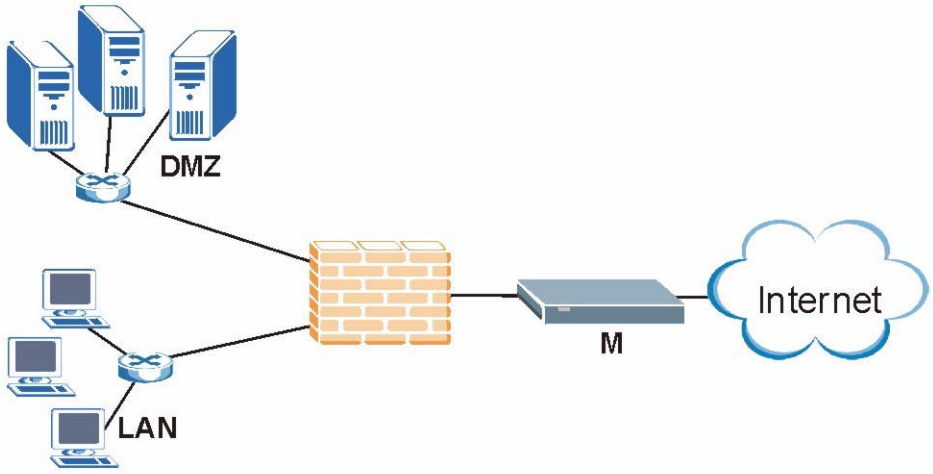
# Intrusion Detection and Prevention (IDP) Screens

## 14.1 Overview

An IDP system can detect malicious or suspicious packets and respond instantaneously. It can detect anomalies based on violations of protocol standards (RFCs – Requests for Comments) or traffic flows and abnormal flows such as port scans.

The following figure represents a typical business network consisting of a LAN, a DMZ (DeMilitarized Zone) containing the company web, FTP, mail servers etc., a firewall and/or NAT router connected to a broadband modem (M) for Internet access.

**Figure 164** Network Intrusions




### 14.1.1 What You Can Do Using the IDP Screens

- Use the **General** screen (Section 14.2 on page 279) to enable IDP on the ZyWALL and choose what traffic flows the ZyWALL checks for intrusions.
- Use the **Signatures** screens (Section 14.3 on page 281) to configure the ZyWALL's signatures. The rules that define how to identify and respond to intrusions are called signatures.
- Use the **Anomaly** screen (Section 14.4 on page 289) to configure the ADP (Anomaly Detection and Prevention) settings

- Use the **Update** screen (Section 14.5 on page 291) to immediately download or schedule new signature downloads.
- Use the **Backup & Restore** screen (Section 14.6 on page 293) to back up IDP signatures with your custom configured settings, restore previously saved IDP signatures (with your custom configured settings) or revert to the original ZSRT-defined signature Active, Log, Alert and/or Action settings.

## 14.1.2 What You Need To Know About the ZyWALL IDP

### Network Intrusions

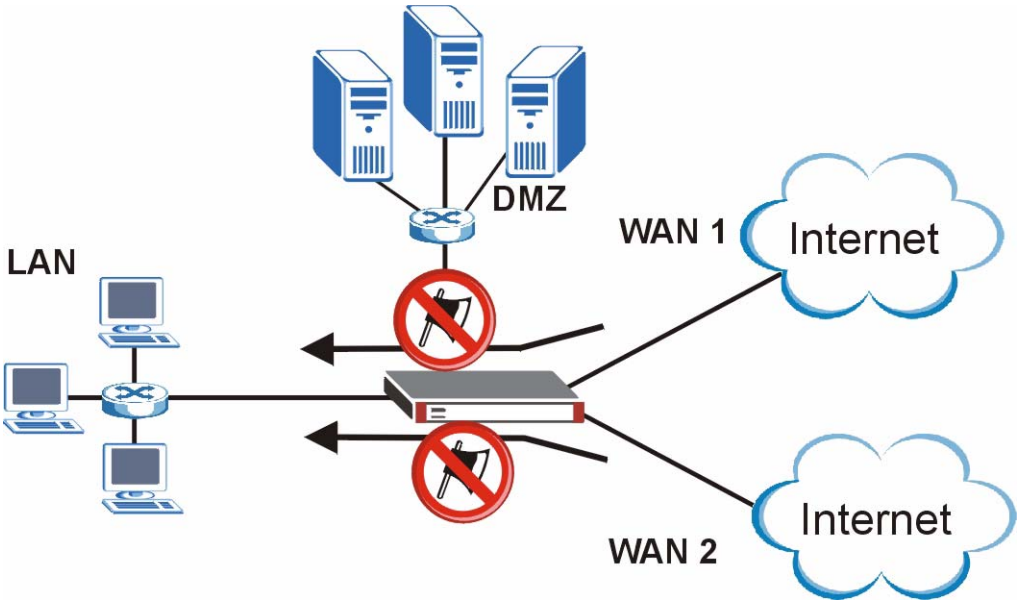
The ZyWALL Internet Security Appliance is designed to protect against network-based intrusions. Network-based intrusions have the goal of bringing down a network or networks by attacking computer(s), switch(es), router(s) or modem(s). If a LAN switch is compromised for example, then the whole LAN is compromised (see Figure 164 on page 277). Typical "network-based intrusions" are SQL slammer, Blaster, Nimda, MyDoom etc.

### IDP and Interfaces

As packets appear at an interface they are passed to the IDP detection engine, which determines whether they are malicious or not. If a malicious packet is detected, an action is taken. The remaining packets that make up that particular TCP session are also discarded.

You can change the default actions in the **Signature** and **Anomaly** screens (Figure 14.3 on page 281 and Figure 172 on page 290). In the following figure the ZyWALL is set to check traffic coming from either WAN interface to the LAN.

**Figure 165** Applying IDP to Interfaces




See Section 14.2 on page 279 for more information on how to apply IDP to ZyWALL interfaces.

### Finding out More

See Section 14.7 on page 294 for more detailed information on IDP.

## 14.1.3 Before You Begin

To use IDP on the ZyWALL, you need to insert the ZyWALL Turbo Card into the rear panel slot of the ZyWALL. See the ZyWALL Turbo Card guide for details.

Turn the ZyWALL off before you install or remove the ZyWALL Turbo card.

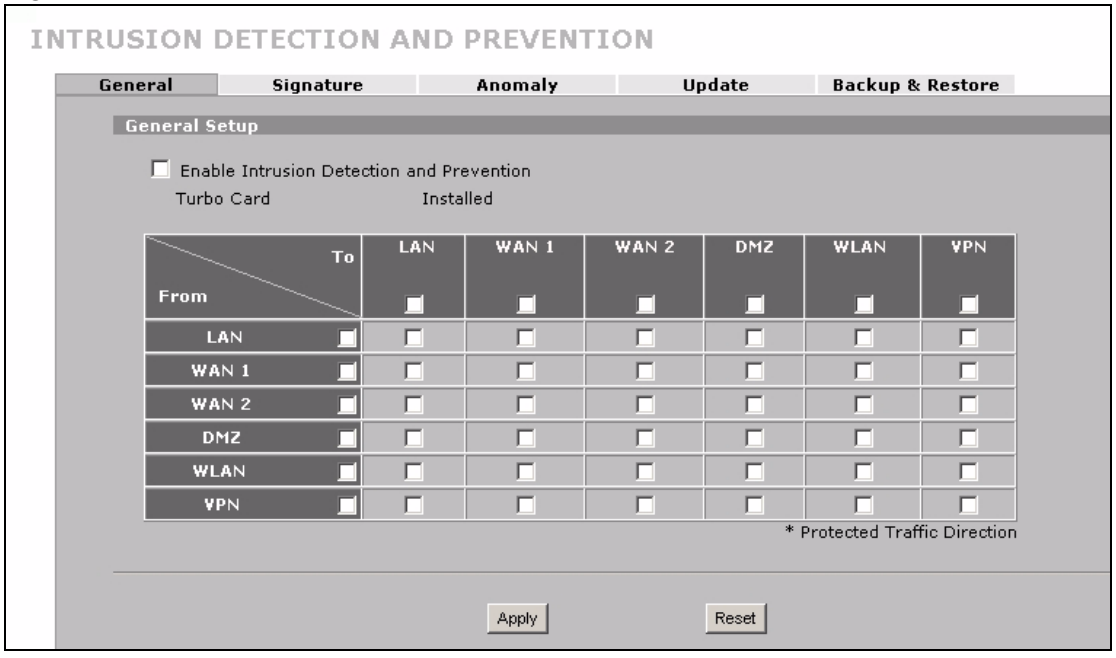
The ZyWALL Turbo Card does not have a MAC address.

# 14.2 The General Setup Screen

Use this screen to enable IDP on the ZyWALL and choose what traffic flows the ZyWALL checks for intrusions.

Click **SECURITY > IDP** from the navigation panel. **General** is the first screen as shown in the following figure.

**Figure 166** SECURITY > IDP > General



The following table describes the labels in this screen.

**Table 77** SECURITY > IDP > General Setup

| LABEL | DESCRIPTION |
|---|---|
| General Setup | |
| Enable Intrusion Detection and Protection | Select this check box to enable IDP on the ZyWALL. When this check box is cleared the ZyWALL is in IDP "bypass" mode and no IDP checking is done. |
| Turbo Card | This field displays whether or not a ZyWALL Turbo Card is installed.<br><br>Note: You cannot configure and save the IDP and Anti-Virus screens if the ZyWALL Turbo Card is not installed. |
| From, To | Select the directions of travel of packets that you want to check. Select or clear a row or column's first check box (with the interface label) to select or clear the interface's whole row or column.<br>You could for example have the ZyWALL check packets traveling between the LAN and the WAN interfaces (**From WAN1 to LAN**, **From WAN2 to LAN**, **From LAN To WAN1**, and **From LAN To WAN2**).<br><br>Note: Depending on your network topology and traffic load, selecting every packet direction may affect the ZyWALL's performance.<br><br>**From LAN To LAN** means packets traveling from a computer on one LAN subnet to a computer on another LAN subnet via the LAN interface of the ZyWALL. The ZyWALL does not check packets traveling from a LAN computer to another LAN computer on the same subnet.<br>**From WAN1 To WAN1** means packets that come in through the WAN 1 interface and the ZyWALL routes back out through the WAN 1 interface.<br>**From VPN** means traffic that came into the ZyWALL through a VPN tunnel and is going to the selected "to" interface. For example, **From VPN To LAN** specifies the VPN traffic that is going to the LAN or terminating at the ZyWALL's LAN interface. The ZyWALL checks the traffic after decrypting it.<br>**To VPN** is traffic that comes in through the selected "from" interface and goes out through any VPN tunnel. For example, **From LAN To VPN** specifies the traffic that is coming from the LAN and going out through a VPN tunnel. The ZyWALL checks the traffic before encrypting it.<br>**From VPN To VPN** means traffic that comes in through a VPN tunnel and goes out through (another) VPN tunnel. This is the case when the ZyWALL is the hub in a hub-and-spoke VPN. The ZyWALL checks the traffic after decrypting it (before encrypting it again).<br><br>Note: The VPN connection directions apply to the traffic going to or from the ZyWALL's VPN tunnels. They do not apply to other VPN traffic for which the ZyWALL is not one of the gateways (VPN pass-through traffic). |
| Apply | Click this button to save your changes back to the ZyWALL. |
| Reset | Click this button to begin configuring this screen afresh. |

# 14.3 The Signatures Screen

The rules that define how to identify and respond to intrusions are called “signatures”. Click **SECURITY** > **IDP** > **Signatures** to see the ZyWALL’s signatures.

## 14.3.1 Attack Types

Click **SECURITY** > **IDP** > **Signature**. The **Attack Type** list box displays all intrusion types supported by the ZyWALL. **Other** covers all intrusion types not covered by other types listed.

To see signatures listed by intrusion type supported by the ZyWALL, select that type from the **Attack Type** list box.

**Table 78** SECURITY > IDP > Signature: Attack Types

| TYPE | DESCRIPTION |
|---|---|
| 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. 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. |
| 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>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. |
| Access Control | Access control refers to procedures and controls that limit or detect access. Access control is used typically to control user access to network resources such as servers, directories, and files. |
| Scan | Scan refers to all port, IP or vulnerability scans. Hackers scan ports to find targets. They may use a TCP connect() call, SYN scanning (half-open scanning), Nmap etc. After a target has been found, a vulnerability scanner can be used to exploit exposures. |
| Trojan Horse | A Trojan horse is a harmful program that’s hidden inside apparently harmless programs or data. It could be used to steal information or remotely control a device. |
| 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 eMule, eDonkey, BitTorrent, iMesh etc. |
| IM | IM (Instant Messaging) refers to chat applications. Chat is real-time communication between two or more users via networks-connected computers. After you enter a chat (or chat room), any member can type a message that will appear on the monitors of all the other participants. |
| 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.<br>The IDP VirusWorm category refers to network-based viruses and worms. The Anti-Virus (AV) screen refers to file-based viruses and worms. Refer to the anti-virus chapter for additional information on file-based anti-virus scanning in the ZyWALL. |
| Porn | The ZyWALL can block web sites if their URLs contain certain pornographic words. It cannot block web pages containing those words if the associated URL does not. |

**Table 78** SECURITY > IDP > Signature: Attack Types (continued)

| TYPE | DESCRIPTION |
|---|---|
| Web Attack | Web attack signatures refer to attacks on web servers such as IIS (Internet Information Services). |
| SPAM | Spam is unsolicited "junk" e-mail sent to large numbers of people to promote products or services. Refer to the anti-spam chapter for more detailed information. |
| Other | This category refers to signatures for attacks that do not fall into the previously mentioned categories. |

## 14.3.2 Intrusion Severity

Intrusions are assigned a severity level based on the following table. The intrusion severity level then determines the default signature action.

**Table 79** SECURITY > IDP > Signature: Intrusion Severity

| SEVERITY | DESCRIPTION |
|---|---|
| Severe | These are intrusions that try to run arbitrary code or gain system privileges. |
| High | These are known serious vulnerabilities or intrusions that are probably not false alarms. |
| Medium | These are medium threats, access control intrusions or intrusions that could be false alarms. |
| Low | These are mild threats or intrusions that could be false alarms. |
| Very Low | These are possible intrusions caused by traffic such as Ping, trace route, ICMP queries etc. |

## 14.3.3 Signature Actions

You can enable/disable individual signatures. You can log and/or have an alert sent when traffic meets a signature criteria. You can also change the default action to be taken when a packet or stream matches a signature. The following figure and table describes these actions. Note that in addition to these actions, a log may be generated or an alert sent, if those check boxes are selected and the signature is enabled.

**Table 80** SECURITY > IDP > Signature: Actions

| ACTION | DESCRIPTION |
|---|---|
| No Action | The intrusion is detected but no action is taken. |
| Drop Packet | The packet is silently discarded. |
| Drop Session | When the firewall is enabled, subsequent TCP/IP packets belonging to the same connection are dropped. Neither sender nor receiver are sent TCP RST packets. If the firewall is not enabled only the packet that matched the signature is dropped. |
| Reset Sender | When the firewall is enabled, the TCP/IP connection is silently torn down. Just the sender is sent TCP RST packets. If the firewall is not enabled only the packet that matched the signature is dropped. |
| Reset Receiver | When the firewall is enabled, the TCP/IP connection is silently torn down. Just the receiver is sent TCP RST packets. If the firewall is not enabled only the packet that matched the signature is dropped. |
| Reset Both | When the firewall is enabled, the TCP/IP connection is silently torn down. Both sender and receiver are sent TCP RST packets. If the firewall is not enabled only the packet that matched the signature is dropped. |

## 14.3.4 Configuring The IDP Signatures Screen

Click **SECURITY** >**IDP** > **Signature** to see the ZyWALL's "group view" signature screen where you can view signatures by attack type. To search for signatures based on other criteria such as signature name or ID, then click the **Switch to query view** link to go to the "query view" screen.

You can take actions on these signatures as described in Section 14.3.3 on page 282. To revert to the default actions or to save sets of actions, go to the **Backup & Restore** screen.

**Figure 167** SECURITY > IDP > Signature: Group View


The following table describes the labels in this screen.

**Table 81** SECURITY > IDP > Signature: Group View

| LABEL | DESCRIPTION |
|---|---|
| Signature Groups | |
| Switch to query view | Click this hyperlink to go to a screen where you can search for signatures based on criteria other than attack type. |
| Attack Type | Select the type of signatures you want to view from the list box. See Section 14.3.1 on page 281 for information on types of signatures.<br>The table displays the signatures of the type that you selected. Click a column's header to sort the entries by that attribute. |
| Go To | Navigate between signatures found. This field is available only if there are more signatures than that can be displayed on one screen. |
| Name | The (read-only) signature name identifies a specific signature targeted at a specific intrusion. Click the hyperlink for more detailed information on the intrusion. |
| ID | Each intrusion has a unique identification number. This number may be searched at myZyXEL.com for more detailed information. |
| Severity | This field displays the level of threat that the intrusion may pose. See Table 79 on page 282 for more information on intrusion severity. |
| Platform | This field displays the computer or network device operating system that the intrusion targets or is vulnerable to the intrusion. These icons represent a Windows operating system, a UNIX-based operating system and a network device respectively.<br>  |

**Table 81** SECURITY > IDP > Signature: Group View (continued)

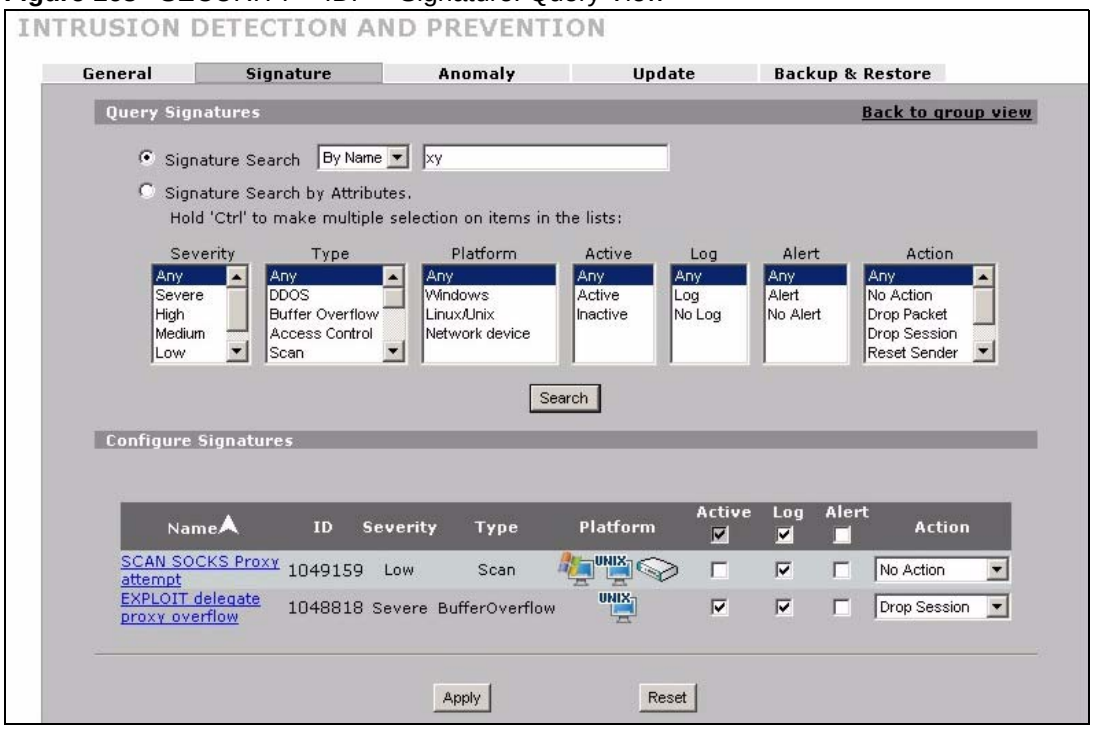
| LABEL | DESCRIPTION |
|---|---|
| Active | Select the check box in the heading row to automatically select all check boxes and enable all signatures.<br>Clear it to clear all entries and disable all signatures on the current page. For example, you could clear all check boxes for signatures that targets operating systems not in your network. This would speed up the IDP signature checking process.<br>Alternatively, you may select or clear individual entries. The check box becomes gray when you select the check box.<br>If you edited any of the check boxes in this column on the current page, use the check box in the heading row to switch between the settings (last partial edited, all selected and all cleared). |
| Log | Select this check box to have a log generated when a match is found for a signature.<br>Select the check box in the heading row to automatically select all check boxes or clear it to clear all entries on the current page.<br>Alternatively, you may select or clear individual entries. The check box becomes gray when you select the check box.<br>If you edited any of the check boxes in this column on the current page, use the check box in the heading row to switch between the settings (last partial edited, all selected and all cleared). |
| Alert | You can only edit the **Alert** check box when the corresponding **Log** check box is selected.<br>Select this check box to have an e-mail sent when a match is found for a signature.<br>Select the check box in the heading row to automatically select all check boxes or clear it to clear all entries on the current page.<br>Alternatively, you may select or clear individual entries. The check box becomes gray when you select the check box.<br>If you edited any of the check boxes in this column on the current page, use the check box in the heading row to switch between the settings (last partial edited, all selected and all cleared). |
| Action | You can change the default signature action here. See Table 80 on page 282 for more details on actions. |
| Apply | Click this button to save your changes back to the ZyWALL. |
| Reset | Click this button to begin configuring this screen afresh. |

## 14.3.5 The Query View Screen

Click **SECURITY** > **IDP** > **Signature** to see the ZyWALL's "group view" signature screen, then click the **Switch to query view** link to go to this 'query view" screen.

Use this screen to search for signatures by criteria such as name, ID, severity, attack type, vulnerable attack platforms, whether or not they are active, log options, alert options or actions.

**Figure 168** SECURITY > IDP > Signature: Query View




The following table describes the fields in this screen.

**Table 82** SECURITY > IDP > Signature: Query View

| LABEL | DESCRIPTION |
|---|---|
| Back to group view | Click this button to go to the IDP group view screen where IDP signatures are grouped by attack type. |
| Signature Search | Select this to search for a specific signature name or ID (that you already know). Then select whether to search the signatures by name or ID. Then enter the name (or part of the name) or the complete ID number of the signature(s) that you want to find. |
| Signature Search by Attributes | Select this to search for signatures that match the criteria that you specify. Then select the criteria to search for. Hold down the [Ctrl] key if you want to make multiple selections from a list of attributes. |
| Severity | Search for signatures by severity level(s) (see Table 79 on page 282). |
| Type | Search for signatures by attack type(s) (see Table 78 on page 281). Attack types are known as policy types in the group view screen. |
| Platform | Search for signatures created to prevent intrusions targeting specific operating system(s). |
| Active | Search for enabled and/or disabled signatures here. |
| Log | Search for signatures by log option here. |
| Alert | Search for signatures by alert option here. |
| Action | Search for signatures by the response the ZyWALL takes when a packet matches a signature. See Table 80 on page 282 for action 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. |

**Table 82** SECURITY > IDP > Signature: Query View (continued)

| LABEL | DESCRIPTION |
|---|---|
| Configure Signatures | The results display in a table showing the criteria as selected in the search. Click a column's header to sort the entries by that attribute. |
| Go To | Navigate between signatures found. This field is available only if there are more signatures than that can be displayed on one screen. |
| Name | The (read-only) signature name identifies a specific signature targeted at a specific intrusion. Click the hyperlink for more detailed information on the intrusion. |
| ID | Each intrusion has a unique identification number. This number may be searched at myZyXEL.com for more detailed information. |
| Severity | This field displays the level of threat that the intrusion may pose. See Table 79 on page 282 for more information on intrusion severity. |
| Platform | This field displays the computer or network device operating system that the intrusion targets or is vulnerable to the intrusion. These icons represent a Windows operating system, a UNIX-based operating system and a network device respectively.   |
| Active | Select the check box in the heading row to automatically select all check boxes and enable all signatures.<br>Clear it to clear all entries and disable all signatures on the current page. For example, you could clear all check boxes for signatures that targets operating systems not in your network. This would speed up the IDP signature checking process.<br>Alternatively, you may select or clear individual entries. The check box becomes gray when you select the check box.<br>If you edited any of the check boxes in this column on the current page, use the check box in the heading row to switch between the settings (last partial edited, all selected and all cleared). |
| Log | Select this check box to have a log generated when a match is found for a signature.<br>Select the check box in the heading row to automatically select all check boxes or clear it to clear all entries on the current page.<br>Alternatively, you may select or clear individual entries. The check box becomes gray when you select the check box.<br>If you edited any of the check boxes in this column on the current page, use the check box in the heading row to switch between the settings (last partial edited, all selected and all cleared). |
| Alert | You can only edit the **Alert** check box when the corresponding **Log** check box is selected.<br>Select this check box to have an e-mail sent when a match is found for a signature.<br>Select the check box in the heading row to automatically select all check boxes or clear it to clear all entries on the current page.<br>Alternatively, you may select or clear individual entries. The check box becomes gray when you select the check box.<br>If you edited any of the check boxes in this column on the current page, use the check box in the heading row to switch between the settings (last partial edited, all selected and all cleared). |
| Action | You can change the default signature action here. See Table 80 on page 282 for more details on actions. |
| Apply | Click this button to save your changes back to the ZyWALL. |
| Reset | Click this button to begin configuring this screen afresh. |

#### 14.3.5.1 Query Example 1

1. From the “group view” signature screen, click the **Switch to query view** link.
1. Select **Signature Search**.
2. Select **By Name** or **By ID** from the list box.
3. Enter a name (complete or partial) or complete ID to display all relevant signatures in the signature database.

A partial name may be searched but a complete ID number must be entered before a match can be found. For example, a search by name for “w” (in the first example) finds all intrusions that contain this letter in the name field. However a search by ID for “1” would return no match. You must enter the complete ID as shown in the second example.

4. Click **Search**. If the search finds more signatures than can be displayed on one page, use the **Go to Page** list box to view other pages of signatures found in the search.
5. If you change the **Active**, **Log**, **Alert** and/or **Action** signature fields in the signatures found, then click **Apply** to save the changes to the ZyWALL.

**Figure 169** SECURITY > IDP > Signature: Query by Partial Name

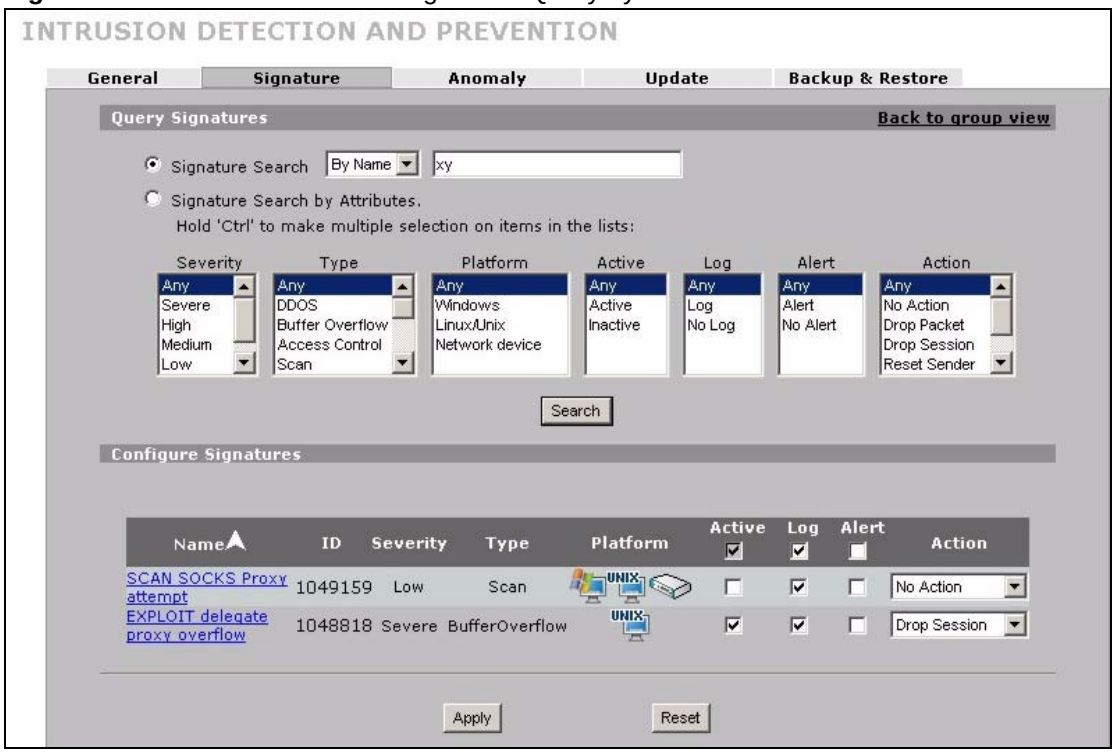


**Figure 170** SECURITY > IDP > Signature: Query by Complete ID


### 14.3.5.2 Query Example 2

1. From the "group view" signature screen, click the **Switch to query view** link.
1. Select **Signature Search By Attributes**.
2. Select the **Severity**, **Type**, **Platform**, **Active**, **Log**, **Alert** and/or **Action** items. In this example all severe **DDoS** type signatures that target the Windows operating system are displayed.
3. Click **Search**.

If you change the **Active**, **Log**, **Alert** and/or **Action** signature fields in the signatures found, then click **Apply** to save the changes to the ZyWALL.

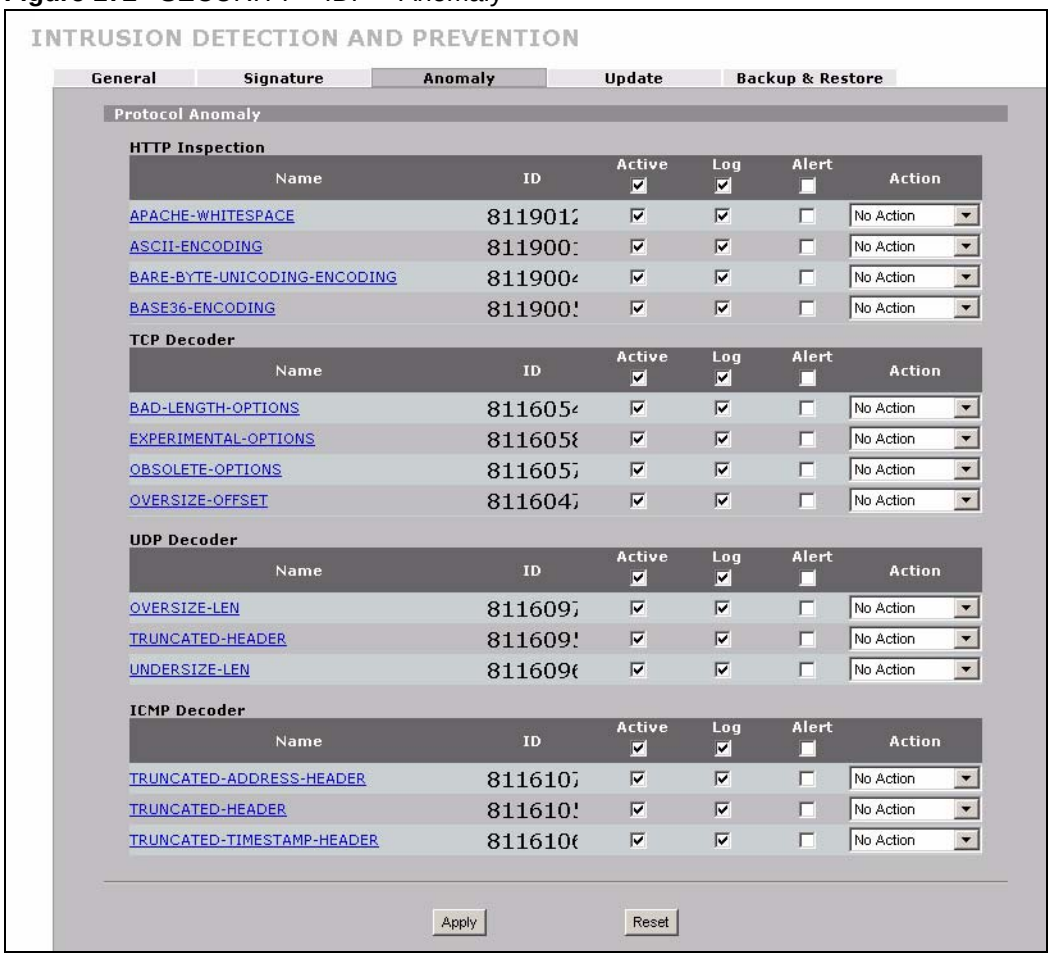
**Figure 171** Signature Query by Attribute.


## 14.4 The Anomaly Screen

This section introduces ADP (Anomaly Detection and Prevention). An ADP system protects against anomalies based on violations of protocol standards (RFCs – Requests for Comments) and abnormal flows such as port scans. Protocol anomaly detection includes HTTP Inspection, TCP Decoder, UDP Decoder and ICMP Decoder. Protocol anomaly rules may be updated when you upload new firmware.

Click **SECURITY** > **IDP** > **Anomaly** to display the following screen.

**Figure 172** SECURITY > IDP > Anomaly




The following table describes the labels in this screen.

**Table 83** SECURITY > IDP > Anomaly

| LABEL | DESCRIPTION |
|---|---|
| Protocol Anomaly | |
| HTTP Inspection/TCP Decoder/UDP Decoder/ICMP Decoder | |
| Name | This is the name of the protocol anomaly rule. Click a name to display more detailed information on a rule. |
| ID | This is the unique identifying number for the anomaly rule. |
| Active | Select the head of the **Active** column to activate all rules for an anomaly detection method, or select **Active** for an individual rule to make it active. |
| Log | Select the head of the **Log** column to generate logs for all rules included in an anomaly detection method. Select **Log** to generate a log when a match is found for the corresponding rule.<br>See Chapter 32 on page 555 for more information on logs. |
| Alert | Select the head of the **Alert** column to activate the alert for all rules in an anomaly detection method. Select **Alert** to generate an alert log when a match is found for the corresponding rule.<br>See Chapter 32 on page 555 for more information on alerts. |

**Table 83** SECURITY > IDP > Anomaly (continued)

| LABEL | DESCRIPTION |
|---|---|
| Action | Select what the ZyWALL should do when a packet matches a rule.<br>**No Action**: The ZyWALL takes no action when a packet matches the signature(s).<br>**Drop Packet**: The packet is silently discarded.<br>**Drop Session**: When the firewall is enabled, subsequent TCP/IP packets belonging to the same connection are dropped. Neither sender nor receiver are sent TCP RST packets. If the firewall is not enabled only the packet that matched the signature is dropped.<br>**Reset Sender**: When the firewall is enabled, the TCP/IP connection is silently torn down. Just the sender is sent TCP RST packets. If the firewall is not enabled only the packet that matched the signature is dropped.<br>**Reset Receiver**: When the firewall is enabled, the TCP/IP connection is silently torn down. Just the receiver is sent TCP RST packets. If the firewall is not enabled only the packet that matched the signature is dropped.<br>**Reset Both**: When the firewall is enabled, the TCP/IP connection is silently torn down. Both sender and receiver are sent TCP RST packets. If the firewall is not enabled only the packet that matched the signature is dropped. |
| Apply | Click this button to save your changes. |
| Reset | Click this button to begin configuring this screen afresh. |

## 14.5 The Update Screen

The ZyWALL comes with built-in signatures. These are updated as new intrusions evolve. Use the **Update** screen to immediately download or schedule new signature downloads.

You should have already registered the ZyWALL at myZyXEL.com (http://www.myzyxel.com/myzyxel/) and also have either activated the trial license or standard license (iCard). If your license has expired, you will have to renew it before updates are allowed.

### 14.5.1 mySecurityZone

mySecurityZone is a web portal that provides all security-related information such as intrusion and anti-virus information for ZyXEL security products.

Click the intrusion **ID** hyperlink to go directly to information on that signature or enter https://mysecurity.zyxel.com/mysecurity/ as the URL in your web browser.

You should have already registered your ZyWALL on myZyXEL.com at:

http://www.myzyxel.com/myzyxel/.

You can use your myZyXEL.com username and password to log into mySecurityZone.

## 14.5.2 Configuring The IDP Update Screen

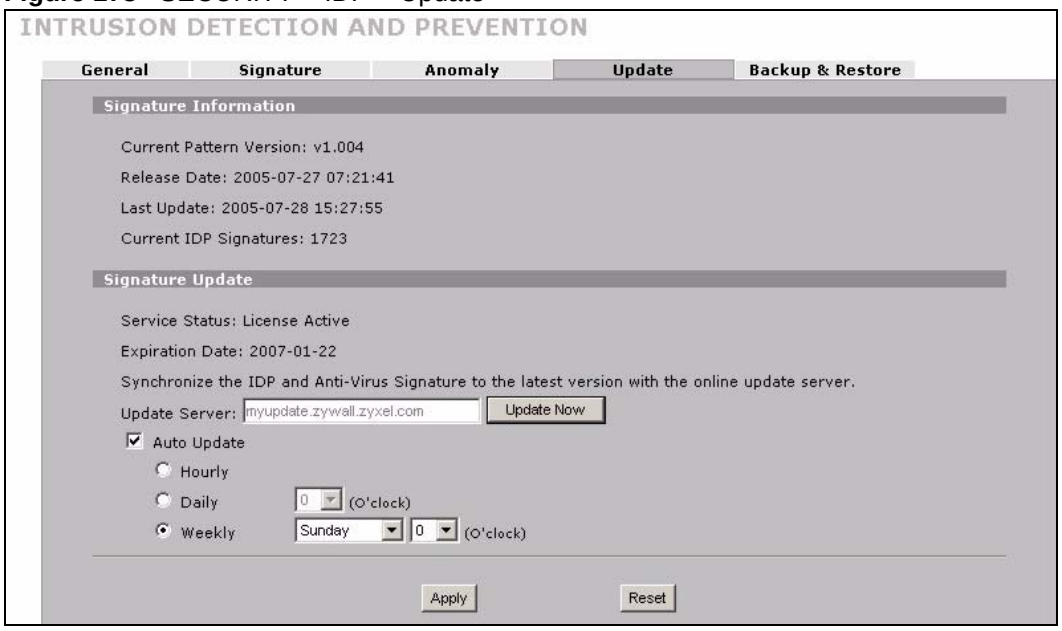
When scheduling signature updates, you should choose a day and time when your network is least busy so as to minimize disruption to your network. Your custom signature configurations are not over-written when you download new signatures.

File-based anti-virus signatures (see the anti-virus chapter) are included with IDP signatures. When you download new signatures using the anti-virus **Update** screen, IDP signatures are also downloaded. The version number changes both in the anti-virus **Update** screen and this screen. Both screens also share the same **Auto-Update** schedule. Changes made to the schedule in one screen are reflected in the other.

You do not have to reboot the ZyWALL when you upload new signatures.

Click **SECURITY** > **IDP** > **Update**.

**Figure 173** SECURITY > IDP > Update




The following table describes the labels in this screen.

**Table 84** SECURITY > IDP > Update

| LABEL | DESCRIPTION |
|---|---|
| Signature Information | |
| Current Pattern Version | This field displays the 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>This number increments 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. |

**Table 84** SECURITY > IDP > Update (continued)

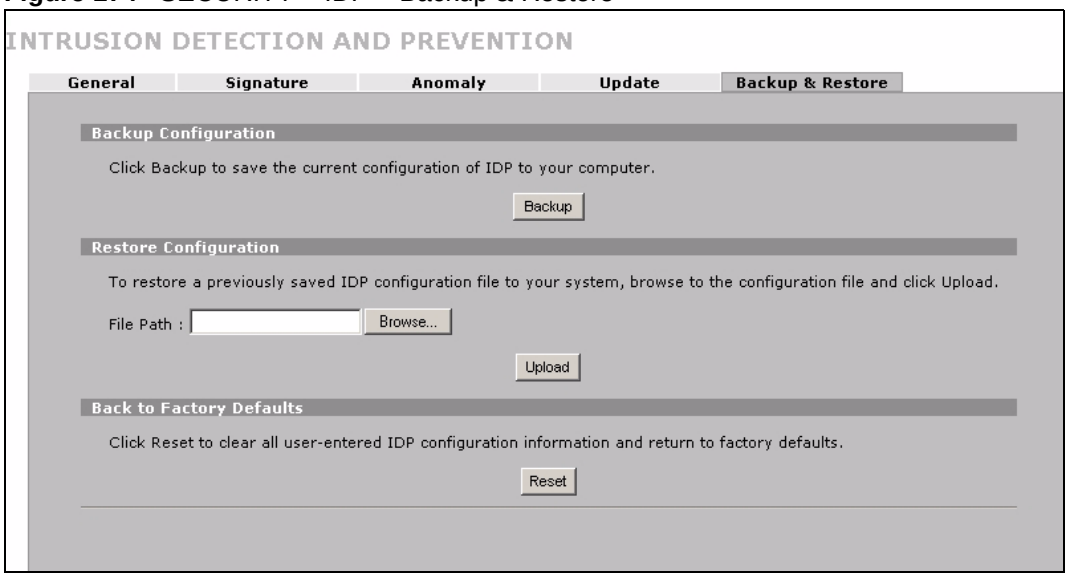
| LABEL | DESCRIPTION |
|---|---|
| Release Date | This field displays the time (hour, minutes second) and date (month, date, year) that the above signature set was created. |
| Last Update | This field displays the last date and time you downloaded new signatures to the ZyWALL. It displays **N/A** if you have not downloaded any new signatures yet. |
| Current IDP Signatures | This field displays the number of IDP-related signatures. |
| Signature Update | |
| Service Status | This field displays **License Inactive** if you have not yet activated your trial or iCard license at myZyXEL.com.<br>It displays **License Inactive** and an expiration date if your trial or iCard license has expired (the expiration date is the date it expired).<br>It displays **Trial Active** and an expiration date when you have activated your trial license.<br>It displays **License Active** and an expiration date when you have activated your iCard license (the expiration date is the date it will expire). |
| Update Server | This is the URL of the signature server from which you download signatures. |
| Update Now | Click this button to begin downloading signatures from the **Update Server** immediately. |
| Auto Update | Select the check box to configure a schedule for automatic signature updates. The **Hourly**, **Daily** and **Weekly** fields display when the check box is selected. The ZyWALL then automatically downloads signatures from the **Update Server** regularly at the time and/or day you specify. |
| Hourly | Select this option to have the ZyWALL check the update server for new signatures every hour. This may be advisable when new intrusions are currently spreading throughout the Internet. |
| Daily | Select this option to have the ZyWALL check the update server for new signatures every day at the hour you select from the list box. The ZyWALL uses a 24-hour clock. For example, choose 15 from the **O'clock** list box to have the ZyWALL check the update server for new signatures at 3 PM every day. |
| Weekly | Select this option to have the ZyWALL check the update server for new signatures once a week on the day and hour you select from the list boxes. The ZyWALL uses a 24-hour clock, so for example, choose **Wednesday** and 15 from the respective list boxes to have the ZyWALL check the update server for new signatures at 3PM every Wednesday. |
| Apply | Click this button to save your changes back to the ZyWALL. |
| Reset | Click this button to close this screen without saving any changes. |

## 14.6 The Backup and Restore Screen

Use the **Backup & Restore** screen to:

- Back up IDP signatures with your custom configured settings.
- Restore previously saved IDP signatures (with your custom configured settings).
- Revert to the factory-default signature (**Active**, **Log**, **Alert** and/or **Action)** settings.

**Figure 174** SECURITY > IDP > Backup & Restore




To back up IDP signatures, click **Backup** and then choose a location and filename for the IDP configuration set.

To restore previously saved IDP signatures, type in the location where the previously saved file resides on your computer or click **Browse ...** to find it, then click **Upload**.

To revert to the factory-default signature (**Active**, **Log**, **Alert** and/or **Action)** settings, click **Reset**.

## 14.7 Technical Reference

This technical reference contains the following sections:

- Firewalls and Intrusions
- IDS and IDP
- Host IDP
- Network IDP
- Example Intrusions

## Firewalls and Intrusions

Firewalls are designed to block clearly suspicious traffic and forward other traffic through. Many exploits take advantage of weaknesses in the protocols that are allowed through the firewall, so that once an inside server has been compromised it can be used as a backdoor to launch attacks on other servers.

Firewalls are usually deployed at the network edge. However, many attacks (inadvertently) are launched from within an organization. Virtual private networks (VPN), removable storage devices and wireless networks may all provide access to the internal network without going through the firewall.

## IDS and IDP

An Intrusion Detection System (IDS) can detect suspicious activity, but does not take action against attacks. On the other hand an IDP is a proactive defense mechanisms designed to detect malicious packets within normal network traffic and take an action (block, drop, log, send an alert) against the offending traffic automatically before it does any damage. An IDS only raises an alert after the malicious payload has been delivered. Worms such as Slammer and Blaster have such fast proliferation speeds that by the time an alert is generated, the damage is already done and spreading fast.

There are two main categories of IDP; Host IDP and Network IDP.

## Host IDP

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 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 IDP

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, resulting in the equivalent of a LAN Denial of Service (DoS) attack. 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.

A Network IDP has at least two network interfaces, one internal and one external. As packets appear at an interface they are passed to the detection engine, which determines whether they are malicious or not. If a malicious packet is detected, an action is taken. The remaining packets that make up that particular TCP session are also discarded.

## Example Intrusions

The following are some examples of intrusions.

### SQL Slammer Worm

W32.SQLExp.Worm is a worm that targets the systems running Microsoft SQL Server 2000, as well as Microsoft Desktop Engine (MSDE) 2000. The worm sends 376 bytes to UDP port 1434, the SQL Server Resolution Service Port. The worm has the unintended payload of performing a Denial of Service attack due to the large number of packets it sends. Refer to Microsoft SQL Server 2000 or MSDE 2000 vulnerabilities in *Microsoft Security Bulletin MS02-039* and *Microsoft Security Bulletin MS02-061*.

### Blaster W32.Worm

This is a worm that exploits the DCOM RPC vulnerability (see *Microsoft Security Bulletin MS03-026* and *Microsoft Security Bulletin MS03-039*) using TCP port 135. The worm targets only Windows 2000 and Windows XP machines. While Windows NT and Windows 2003 Server machines are vulnerable (if not properly patched), the worm is not coded to replicate on those systems. This worm attempts to download the msblast.exe file to the %WinDir%\system32 directory and then execute it. W32.Blaster.Worm does not mass mail to other devices.

### Nimda

Its name (backwards for "admin") refers to an "admin.DLL" file that, when run, continues to propagate the virus. Nimda probes each IP address within a randomly selected range of IP addresses, attempting to exploit weaknesses that, unless already patched, are known to exist in computers with Microsoft's Internet Information Server. A system with an exposed IIS Web server will read a Web page containing an embedded JavaScript that automatically executes, causing the same JavaScript code to propagate to all Web pages on that server. As Microsoft Internet Explorer browsers version 5.01 or earlier visit sites at the infected Web server, they unwittingly download pages with the JavaScript code that automatically executes, causing the virus to be sent to other computers on the Internet in a somewhat random fashion. Nimda also can infect users within the Web server's own internal network that have been given a network share (a portion of file space). Finally, one of the things that Nimda has an infected system do is to send an e-mail with a "readme.exe" attachment to the addresses in the local Windows address book. A user who opens or previews this attachment (which is a Web page with the JavaScript) propagates the virus further.

Server administrators should get and apply the cumulative IIS patch that Microsoft has provided for previous viruses and ensure that no one at the server opens e-mail. You should update your Internet Explorer version to IE 5.5 SP2 or later. Scan and cleanse your system with anti-virus software.

### MyDoom

MyDoom W32.Mydoom.A@mm (also known as W32.Novarg.A) is a mass-mailing worm that arrives as an attachment with an bat, cmd, exe, pif, scr, or zip file extension. When a computer is infected, the worm sets up a backdoor into the system by opening TCP ports 3127 through 3198, which can potentially allow an attacker to connect to the computer and use it as a proxy to gain access to its network resources. In addition, the backdoor can download and execute arbitrary files. Systems affected are Windows 95, Windows 98, Windows Me, Windows NT, Windows 2000, Windows XP and Windows Server 2003.

W32/MyDoom-A is a worm that is spread by email. When the infected attachment is launched, the worm gathers e-mail addresses from address books and from files with the following extensions: WAB, TXT, HTM, SHT, PHP, ASP, DBX, TBB, ADB and PL. W32/MyDoom-A creates a file called Message in the temp folder and runs Notepad to display the contents, which displays random characters. W32/MyDoom-A creates randomly chosen email addresses in the "To:" and "From:" fields as well as a randomly chosen subject line. Attached files will have an extension of BAT, CMD, EXE, PIF, SCR or ZIP.

# 15

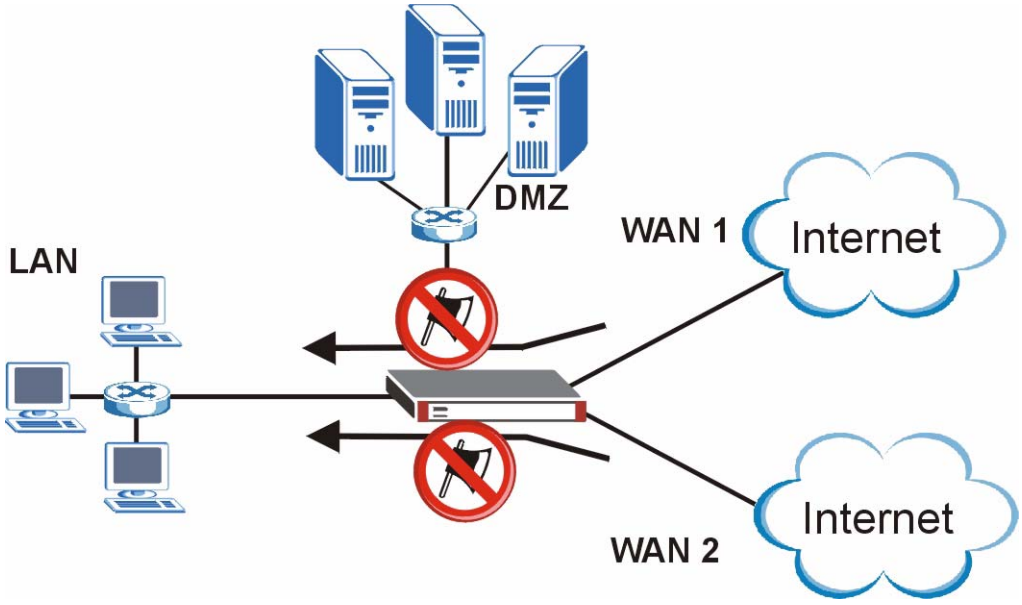
# Anti-Virus Screens

## 15.1 Overview

This section shows you how to configure the ZyWALL to scan files transmitted 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.

The following figure shows the ZyWALL virus-scanning files going to the LAN from WAN1 and WAN2.

**Figure 175** ZyWALL Anti-virus Overview




### 15.1.1 What You Can Do in the Antivirus Screens

- Use the **General** screen (Section 15.2 on page 301) to enable the antivirus service and configure to which interface(s) it applies.
- Use the **Signature** screen (Section 15.3 on page 303) to locate signatures and manage how the ZyWALL uses them.
- Use the **Update** screen (Section 15.4 on page 306) to immediately download or schedule new signature downloads.
- Use the **Backup and Restore** screen (Section 15.5 on page 309) to backup or restore antivirus signatures, or return antivirus signatures to their original settings.

## 15.1.2 What You Need to Know About Antivirus

### Virus

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.

### Signature

This is the pattern of code used by a particular virus. The virus-scanner compares files with a database of signatures to identify possible viruses.

### The ZyWALL Anti-Virus Scanner

The ZyWALL checks traffic going in the direction(s) you specify for signature matches.

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)

The following describes the virus scanning process on the ZyWALL.

1. The ZyWALL first identifies SMTP, POP3, 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 viruses.
4. If a virus pattern is matched, the ZyWALL “destroys” the file by removing the infected portion of the file.
5. If the send alert message function is enabled, the ZyWALL sends an alert to the file’s intended destination computer(s).

Since the ZyWALL erases the infected portion of the file before sending it, you may not be able to open the file.

The following lists important notes about the anti-virus scanner:

1. The ZyWALL anti-virus scanner cannot detect polymorphic viruses.
2. When a virus is detected, an alert message is displayed in Microsoft Windows computers.[2]
3. The ZyWALL does not scan the following file/traffic types:

2. For Windows 98/Me, refer to the Appendix D on page 801 for requirements.

- Simultaneous downloads of a file using multiple connections. For example, when you use FlashGet to download sections of a file simultaneously.
- Encrypted traffic (such as on a VPN) or password-protected files.
- Traffic through custom (non-standard) ports.
- ZIP file(s) within a ZIP file.

### ZyWALL Turbo Card

To use the anti-virus scanner on the ZyWALL, you need to insert the ZyWALL Turbo Card into the rear panel slot of the ZyWALL. See the ZyWALL Turbo Card guide for details.

Turn the ZyWALL off before you install or remove the ZyWALL Turbo card.

The ZyWALL Turbo Card does not have a MAC address.

### Finding Out More

- See Section 15.6 on page 310 for more information on viruses and virus scanners.

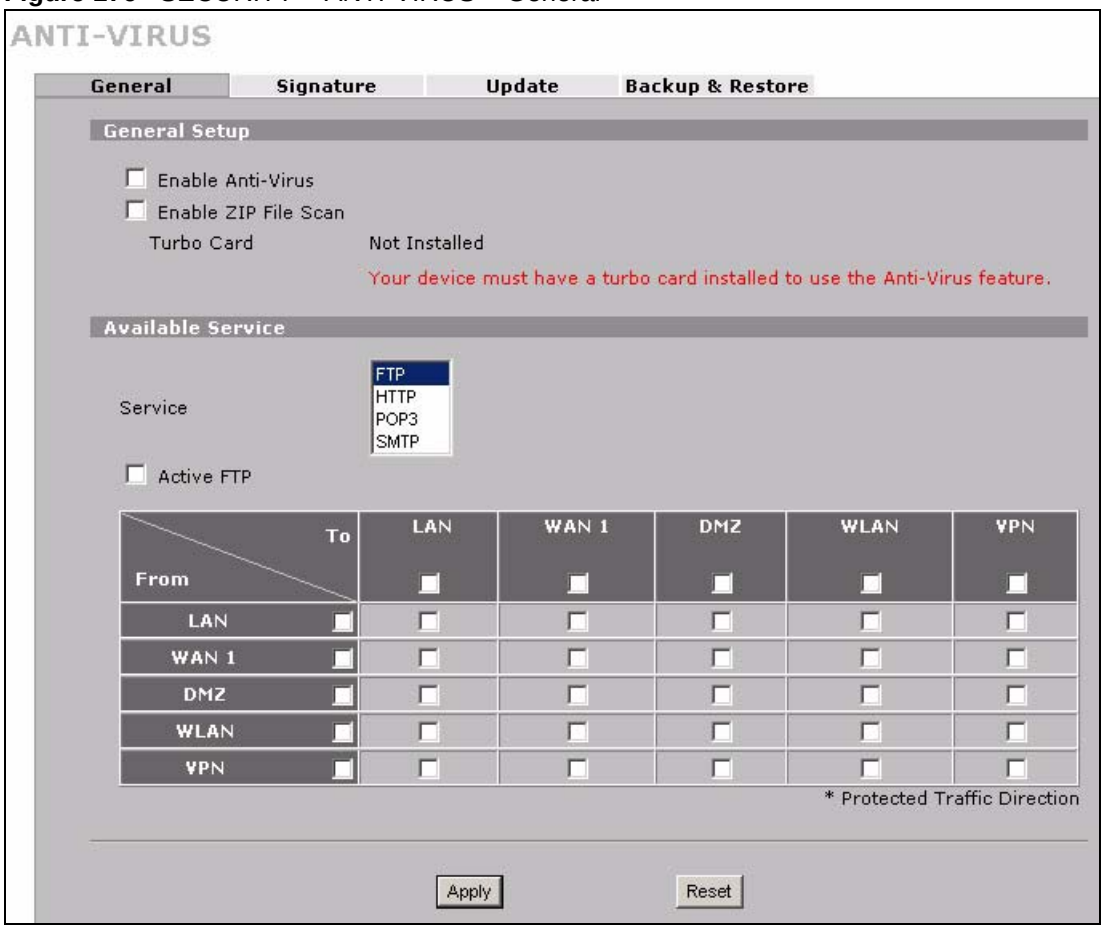
## 15.2 The General Screen

Use this screen to enable the antivirus service and configure to which interfaces the service applies.

Click **SECURITY** > **ANTI-VIRUS** to display the **General** screen as shown next.

Before you use the anti-virus feature, you must register for the service (refer to the chapter on registration for more information).

**Figure 176** SECURITY > ANTI-VIRUS > General




The following table describes the labels in this screen.

**Table 85** SECURITY > ANTI-VIRUS > General

| LABEL | DESCRIPTION |
|---|---|
| General Setup | |
| Enable Anti-Virus | Select this check box to check traffic for viruses. |
| Enable ZIP File Scan | Select this check box to have the ZyWALL scan a ZIP file (with the “zip”, “gzip” or “gz” 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 the ZIP file. |
| Turbo Card | This field displays whether or not a ZyWALL Turbo Card is installed.<br><br>Note: You cannot configure and save the IDP and Anti-Virus screens if the ZyWALL Turbo Card is not installed. |
| Available Service | |

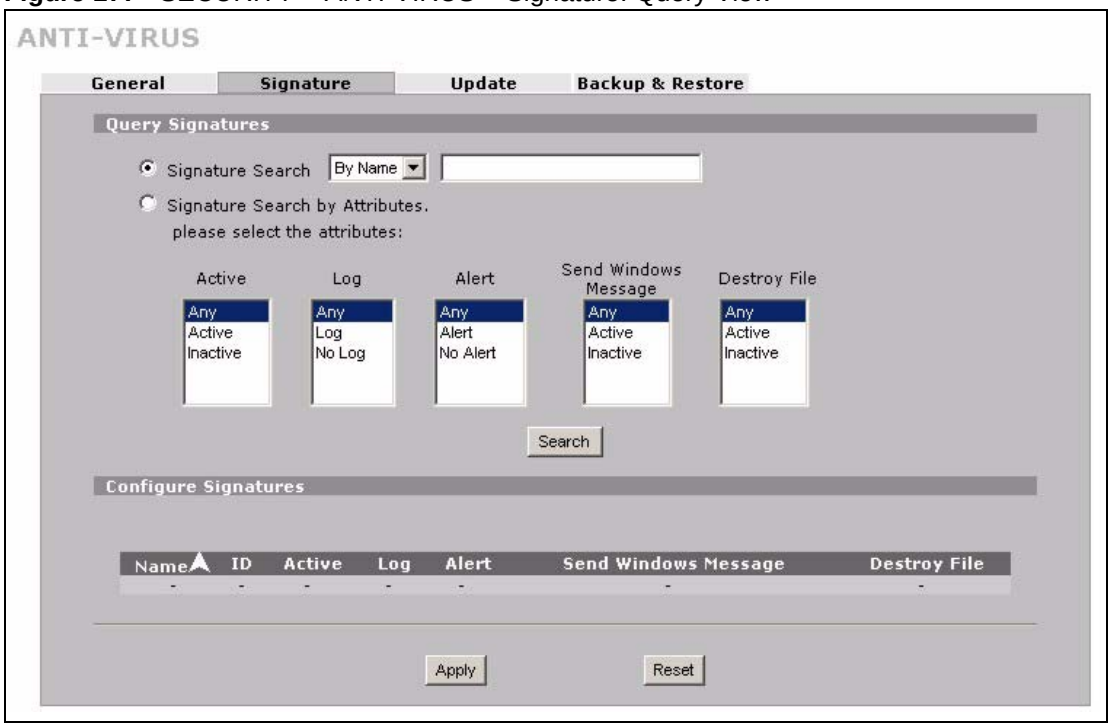
**Table 85** SECURITY > ANTI-VIRUS > General (continued)

| LABEL | DESCRIPTION |
|---|---|
| Service | This field displays the services for which the ZyWALL can scan traffic for viruses. Select a service to be able to enable or disable anti-virus scanning on it's traffic. Here are the services and default port numbers.<br>FTP traffic using TCP ports 20 and 21<br>HTTP traffic using TCP ports 80, 8080 and 3128<br>POP3 traffic using TCP port 110<br>SMTP traffic using TCP port 25<br>See Section 29.2 on page 529 if you need to use the anti-virus scanner for FTP, HTTP, POP3 or SMTP traffic on custom ports. |
| Active | Select **Active** to enable the anti-virus scanner for the selected service. |
| From, To | Select the directions of travel of packets that you want to check. Select or clear a row or column's first check box (with the interface label) to select or clear the interface's whole row or column.<br>You could for example have the ZyWALL check packets traveling in from the WAN to the DMZ. For example, **From WAN1 to DMZ** and **From WAN2 to DMZ**.<br>**From LAN To LAN** means packets traveling from a computer on one LAN subnet to a computer on another LAN subnet via the LAN interface of the ZyWALL. The ZyWALL does not check packets traveling from a LAN computer to another LAN computer on the same subnet.<br>**From WAN1 To WAN1** means packets that come in through the WAN 1 interface and the ZyWALL routes back out through the WAN 1 interface.<br>**From VPN** means traffic that came into the ZyWALL through a VPN tunnel and is going to the selected "to" interface. For example, **From VPN To LAN** specifies the VPN traffic that is going to the LAN or terminating at the ZyWALL's LAN interface. The ZyWALL checks the traffic after decrypting it.<br>**To VPN** is traffic that comes in through the selected "from" interface and goes out through any VPN tunnel. For example, **From LAN To VPN** specifies the traffic that is coming from the LAN and going out through a VPN tunnel. The ZyWALL checks the traffic before encrypting it.<br>**From VPN To VPN** means traffic that comes in through a VPN tunnel and goes out through (another) VPN tunnel. This is the case when the ZyWALL is the hub in a hub-and-spoke VPN. The ZyWALL checks the traffic after decrypting it (before encrypting it again).<br>Note: The VPN connection directions apply to the traffic going to or from the ZyWALL's VPN tunnels. They do not apply to other VPN traffic for which the ZyWALL is not one of the gateways (VPN pass-through traffic). |
| Apply | Click **Apply** to save your changes. |
| Reset | Click **Reset** to start configuring this screen again. |

## 15.3 The Signature Screen

Click **SECURITY** > **ANTI-VIRUS** > **Signature** to display this screen. Use this screen to locate signatures and manage how the ZyWALL uses them.

**Figure 177** SECURITY > ANTI-VIRUS > Signature: Query View




The following table describes the labels in this screen.

**Table 86** SECURITY > ANTI-VIRUS > Signature: Query View

| LABEL | DESCRIPTION |
|---|---|
| Query Signatures | Select the criteria on which to perform the search. |
| Signature Search | Select this radio button if you would like to search the signatures by name or ID. Select this check box to only select the signatures you created or imported in the **Custom Signature** screen by name or ID.<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.<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. |
| Signature Search by Attributes | Select this radio button if you would like to search the signatures by the general attributes listed next. |
| Active | Use this field to search for active (enabled) and/or inactive (disabled) signatures here. |
| Log | Search for signatures by log option here (whether or not the ZyWALL is set to log packets that match the signature). |
| Alert | Search for signatures by whether or not the ZyWALL is set to generate an alert mail when packets match the signature). |
| Send Windows Message | Search for signatures by whether or not the ZyWALL is set to send a message alert to files' intended user(s) using Microsoft Windows computer connected to the protected interface. |
| Destroy File | Search for signatures by whether or not the ZyWALL is set to erase the infected portion of the file before sending it. |
| Search | Click this button to begin the search. The results display in the table 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 (relevant) signatures returned. |

**Table 86** SECURITY > ANTI-VIRUS > Signature: Query View (continued)

| LABEL | DESCRIPTION |
|---|---|
| Configure Signatures | The signature search results display 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 SID. |
| Go to Page | Navigate between the pages of signature search results. |
| 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 rule name. |
| ID | This is the IDentification number of the anti-virus signature. Click the ID column header to sort your search results by ID. |
| Active | Select **Active** to enable the anti-virus scanner for the selected signature. Select or clear the check box in the column heading to select or clear the column's check boxes for all of the displayed anti-virus signatures. |
| Log | Select **Log** to create a log when packets match the signature. Select or clear the check box in the column heading to select or clear the column's check boxes for all of the displayed anti-virus signatures. |
| Alert | This field is applicable only when you select **Log**.<br>Select **Alert** to create an alert when a virus is detected. Select or clear the check box in the column heading to select or clear the column's check boxes for all of the displayed anti-virus signatures. |
| Send Windows Message | Select this check box to set the ZyWALL to send a message alert to files' intended user(s) using Microsoft Windows computer connected to the protected interface. Select or clear the check box in the column heading to select or clear the column's check boxes for all of the displayed anti-virus signatures. |
| Destroy File | Select this check box to set the ZyWALL to erase the infected portion of the file before sending it. Once destroyed, you may not be able to open the file. Select or clear the check box in the column heading to select or clear the column's check boxes for all of the displayed anti-virus signatures. |
| Apply | Click **Apply** to save your settings to the ZyWALL. |
| Reset | Click **Reset** to return to discard any unsaved changes that you have made in this screen and return to the previously saved settings. |

## 15.3.1 Signature Search Example

This example shows a search for signatures that are enabled, set to generate logs and alerts, send Windows messages and destroy the infected portion of the file.

**Figure 178** Query Example Search Criteria

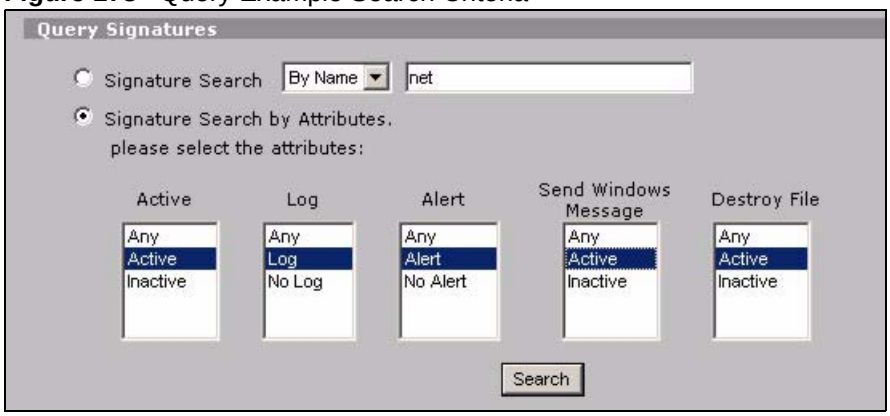
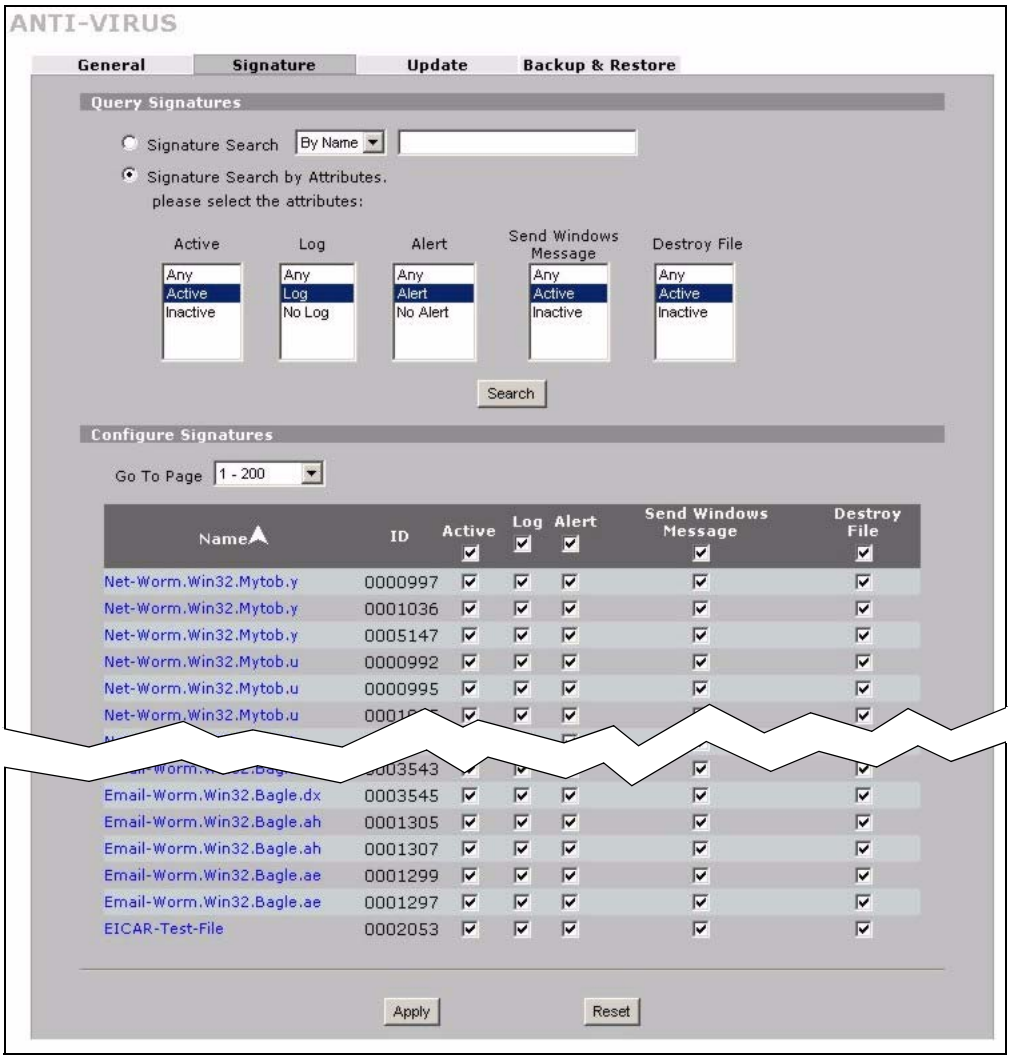


**Figure 179** Query Example Search Results




## 15.4 The Update Screen

The ZyWALL comes with built-in signatures created by the ZyXEL Security Response Team (ZSRT). These are regularly updated as new intrusions evolve. Use the **Update** screen to immediately download or schedule new signature downloads.

You should have already registered the ZyWALL at myZyXEL.com (http://www.myzyxel.com/myzyxel/) and also have either activated the trial license or standard license (iCard). If your license has expired, you will have to renew it before updates are allowed.

### 15.4.1 mySecurityZone

mySecurityZone is a web portal that provides all security-related information such as intrusion and anti-virus information for ZyXEL security products.

You should have already registered your ZyWALL on myZyXEL.com at:

http://www.myzyxel.com/myzyxel/.

You can use your myZyXEL.com username and password to log into mySecurityZone.

### 15.4.2 Configuring Anti-virus Update

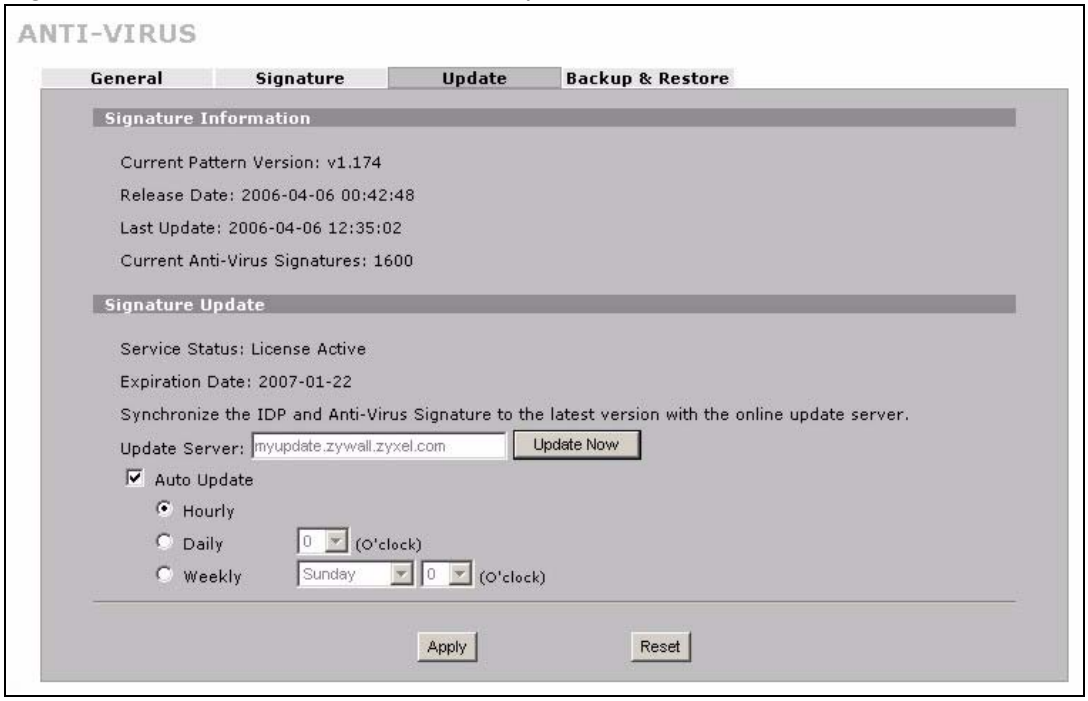
When scheduling signature updates, you should choose a day and time when your network is least busy so as to minimize disruption to your network. Your custom signature configurations are not over-written when you download new signatures.

IDP signatures (see the chapters on IDP) are included with file-based anti-virus signatures. When you download new signatures using the IDP **Update** screen, anti-virus signatures are also downloaded. The version number changes both in the IDP **Update** screen and this screen. Both screens also share the same **Auto-Update** schedule. Changes made to the schedule in one screen are reflected in the other.

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

Click **SECURITY** > **ANTI-VIRUS** > **Update**.

**Figure 180** SECURITY > ANTI-VIRUS > Update



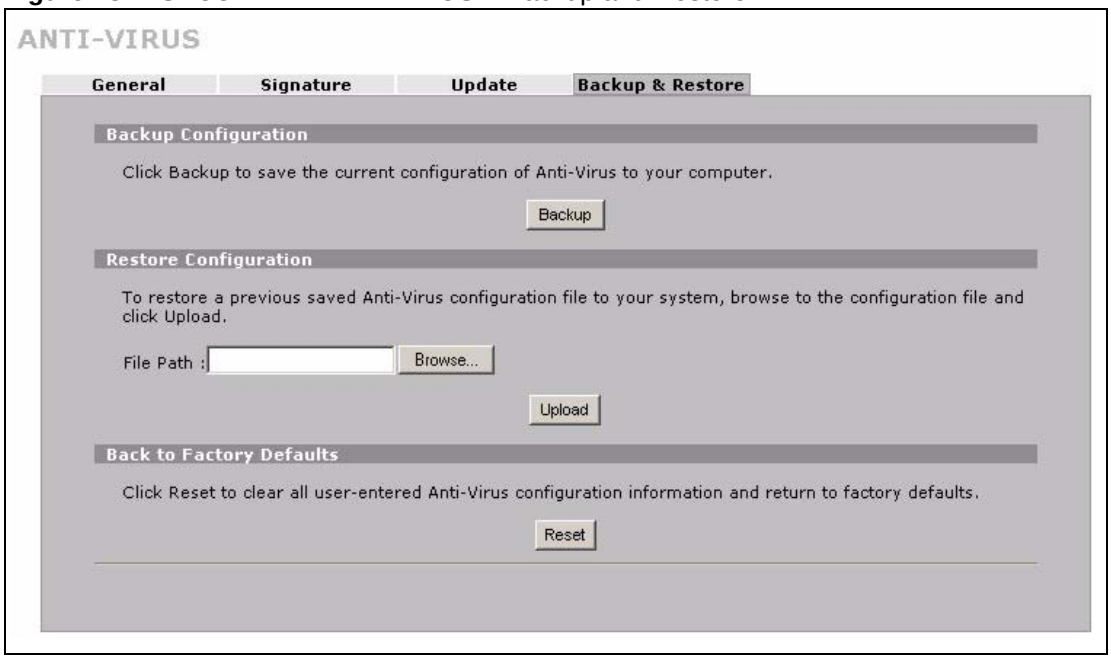
The following table describes the labels in this screen.

| LABEL | DESCRIPTION |
|---|---|
| Signature Information | |
| Current Pattern Version | This field displays the 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>This number increments 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. |
| Release Date | This field displays the time (hour, minutes second) and date (month, date, year) that the above signature set was created. |
| Last Update | This field displays the last date and time you downloaded new signatures to the ZyWALL. It displays **N/A** if you have not downloaded any new signatures yet. |
| Current Anti-Virus Signatures | This field displays the number of Anti-Virus-related signatures. |
| Signature Update | |
| Service Status | This field displays **License Inactive** if you have not yet activated your trial or iCard license at myZyXEL.com.<br>It displays **License Inactive** and an expiration date if your trial or iCard license has expired (the expiration date is the date it expired).<br>It displays **Trial Active** and an expiration date when you have activated your trial license.<br>It displays **License Active** and an expiration date when you have activated your iCard license (the expiration date is the date it will expire). |
| Update Server | This is the URL of the signature server from which you download signatures. |
| Update Now | Click this button to begin downloading signatures from the **Update Server** immediately. |
| Auto Update | Select the check box to configure a schedule for automatic signature updates. The **Hourly**, **Daily** and **Weekly** fields display when the check box is selected. The ZyWALL then automatically downloads signatures from the **Update Server** regularly at the time and/or day you specify. |
| Hourly | Select this option to have the ZyWALL check the update server for new signatures every hour. This may be advisable when new viruses are currently spreading throughout the Internet. |
| Daily | Select this option to have the ZyWALL check the update server for new signatures every day at the hour you select from the list box. The ZyWALL uses a 24-hour clock. For example, choose 15 from the **O'clock** list box to have the ZyWALL check the update server for new signatures at 3 PM every day. |
| Weekly | Select this option to have the ZyWALL check the update server for new signatures once a week on the day and hour you select from the list boxes. The ZyWALL uses a 24-hour clock, so for example, choose **Wednesday** and **15** from the respective list boxes to have the ZyWALL check the update server for new signatures at 3PM every Wednesday. |
| Apply | Click this button to save your changes back to the ZyWALL. |
| Reset | Click this button to close this screen without saving any changes. |

## 15.5 The Backup and Restore Screen

Click **ANTI-VIRUS** > **Backup & Restore**. The screen displays as shown next. You can change the pre-defined **Active**, **Log**, **Alert**, **Send Windows Message** and/or **Destroy File** settings of individual signatures.

**Figure 181** SECURITY > ANTI-VIRUS > Backup and Restore




Use the **Backup & Restore** screen to:

- Back up anti-virus signatures with your custom configured settings to a computer. Click **Backup** and then choose a location and filename for the anti-virus configuration set.
- Restore previously saved anti-virus signatures (with your custom configured settings). Type in the location where the previously saved file resides on your computer or click **Browse ...** to find it. Click **Upload**.
- Revert to the original ZSRT-defined signature **Active**, **Log**, **Alert**, **Send Windows Message** and/or **Destroy File** settings. Click **Reset**.

# 15.6 Technical Reference

## Types of Computer Viruses

The following table describes some of the common computer viruses.

**Table 87** 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. |
| E-mail Virus | E-mail viruses are malicious programs that spread through e-mail. |
| Polyrmorphic 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.

# 16

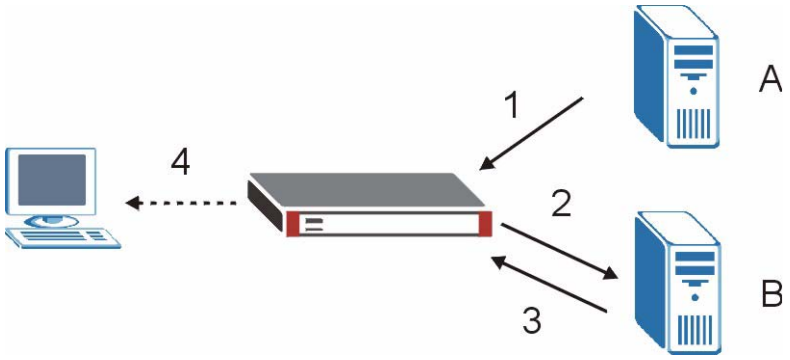
# Anti-Spam Screens

## 16.1 Overview

The ZyWALL's anti-spam feature identifies unsolicited commercial or junk e-mail (spam). You can set the ZyWALL to mark or discard spam. The ZyWALL can use an anti-spam external database to help identify spam. Use the whitelist to identify legitimate e-mail. Use the blacklist to identify spam e-mail.

The following is an figure showing the ZyWALL checking e-mail with the external database.

**Figure 182** Anti-spam Overview




1. E-mail comes into the ZyWALL from an e-mail server (A in the figure).
2. The ZyWALL calculates a digest of the e-mail and sends it to the anti-spam external database.
3. The anti-spam external database calculates a spam score for the e-mail and sends the score back to the ZyWALL.
4. The ZyWALL forwards the e-mail if the spam score is at or below the ZyWALL's spam threshold. If the spam score is higher than the spam threshold, the ZyWALL takes the action that you configured for dealing with spam.

### 16.1.1 What You Can Do in the Antispam Screens

- Use the **General** screen (Section 16.2 on page 315) to configure interfaces to scan for spam mail and actions to be taken when spam is identified.
- Use the **External DB** screen (Section 16.3 on page 318) to enable or disable external database services and configure the spam threshold.
- Use the **Anti-Spam Lists** screen (Section 16.4 on page 320) to configure whitelist and blacklist settings.

## 16.1.2 What You Need to Know About Antispam

### MIME Headers

MIME (Multipurpose Internet Mail Extensions) allows varied media types to be used in e-mail. MIME headers describe an e-mail's content encoding and type. For example, it may show which program generated the e-mail and what type of text is used in the e-mail body. Here are some examples of MIME headers:

- X-Priority: 3 (Normal)
- X-MSMail-Priority: Normal

In an MIME header, the part that comes before the colon (:) is the header. The part that comes after the colon is the value. Spam often has blank header values or comments in them that are part of an attempt to bypass spam filters.

### Whitelist

Configure whitelist entries to identify legitimate e-mail. The whitelist entries have the ZyWALL classify any e-mail that is from a specified sender or uses a specified MIME header or MIME header value as being legitimate. The anti-spam feature checks an e-mail against the whitelist entries before doing any other anti-spam checking. If the e-mail matches a whitelist 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 whitelist helps keep important e-mail from being incorrectly classified as spam. The whitelist 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.

### Blacklist

Configure blacklist entries to identify spam. The blacklist entries have the ZyWALL classify any e-mail that is from a specified sender or uses a specified MIME header or MIME header value as being spam. If an e-mail does not match any of the whitelist entries, the ZyWALL checks it against the blacklist entries. The ZyWALL classifies an e-mail that matches a blacklist entry as spam and immediately takes the action that you configured for dealing with spam. The ZyWALL does not perform any more anti-spam checking on that individual e-mail. A properly configured blacklist helps catch spam e-mail and increases the ZyWALL's anti-spam speed and efficiency.

### Anti-Spam External Database

If an e-mail does not match any of the whitelist or blacklist entries, the ZyWALL calculates a digest (fingerprint ID) of the e-mail and sends it to the anti-spam external database. The anti-spam external database checks the digest against (more than a million) known spam patterns.

The anti-spam external database then uses a proprietary Bayesian[3] statistical formula to combine the results into one score of how likely the e-mail is to be spam and sends it to the ZyWALL. The possible range for the spam score is 0~100. The closer the score is to 100, the more likely the e-mail is to be spam. You must subscribe to and activate the anti-spam external database service in order to use it (see Section  on page 314 for details).

3. Bayesian analysis interprets probabilities as degrees of belief rather than as proportions, frequencies and such. Bayesian analysis frequently uses Bayes' theorem, hence the name.

### SpamBulk Engine

The e-mail fingerprint ID that the ZyWALL generates and sends to the anti-spam external database only includes the parts of the e-mail that are the most difficult for spammers (senders of spam) to change or fake. The anti-spam external database maintains a database of e-mail fingerprint IDs. The anti-spam external database SpamBulk engine then queries the database in analyzing later e-mails.

The SpamBulk Engine also uses Bayesian statistical analysis to detect whether an e-mail is fundamentally the same as a known spam message in spite of a spammer's attempt to disguise it.

### Spam Threshold

You can configure the threshold for what spam score is classified as spam. The ZyWALL considers any e-mail with a spam score higher than the spam threshold to be spam. Any e-mail with a score less than or equal to the spam threshold is treated as legitimate.

### 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.

### Finding Out More

See Section 16.6 on page 324 for more information on antispam.

## 16.2 The General Screen

Use this screen to turn the anti-spam feature on or off, choose what traffic flows the ZyWALL checks for spam, and set how the ZyWALL treats spam.

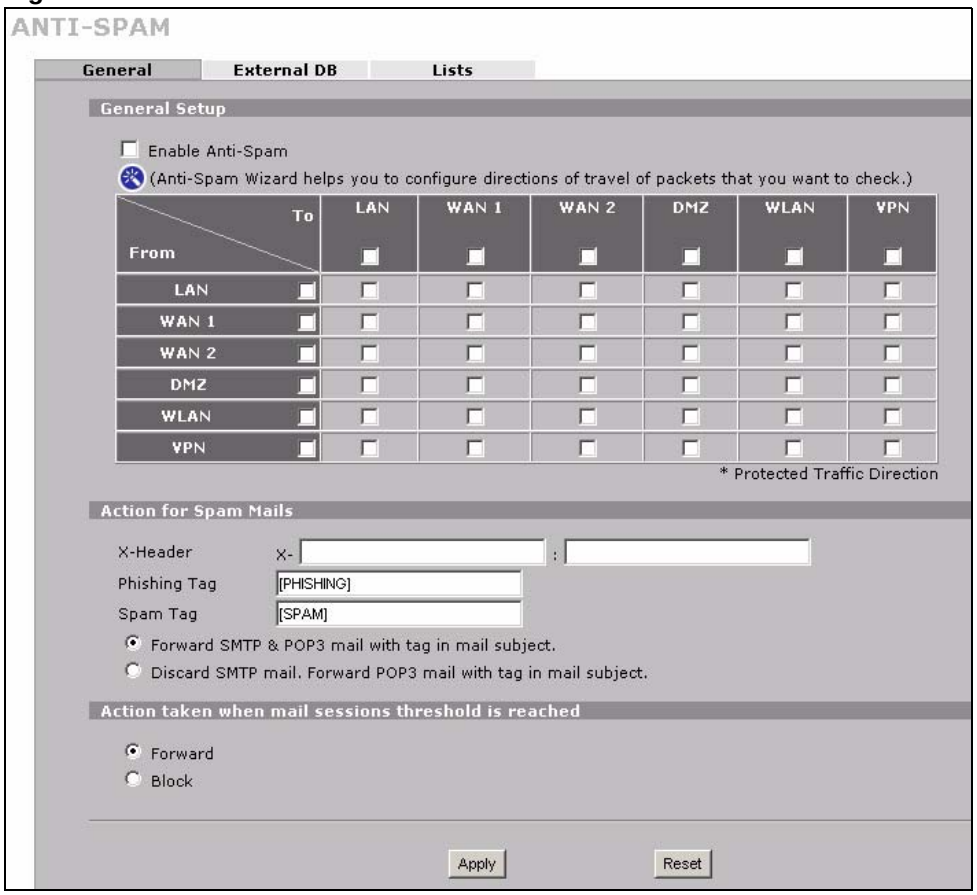
### Phishing

Phishing is a scam where fraudsters send e-mail claiming to be from a well-known enterprise in an attempt to steal private information. For example, the e-mail might appear to be from a bank, online payment service, or even a government agency. It generally tells you to click a link and update your identity information in order for the business or organization to verify your account. The link directs you to a phony website that mimics the business or organization's website. The fraudsters then use your personal information to pretend to be you and commit crimes like running up bills in your name (identity theft).

The anti-spam external database checks for spoofing of e-mail attributes (like the IP address) and uses statistical analysis to detect phishing.

Click **SECURITY** > **ANTI-SPAM** to open the **Anti-Spam General** screen. The following screen appears.

**Figure 183** SECURITY > ANTI-SPAM > General




The following table describes the labels in this screen.

**Table 88** SECURITY > ANTI-SPAM > General

| LABEL | DESCRIPTION |
|---|---|
| General Setup | |
| Enable Anti-Spam | Select this check box to check traffic for spam SMTP (TCP port 25 and POP3 (TCP port 110) e-mail.<br>See Section 29.2 on page 529 if you need to use anti-spam for SMTP and POP3 traffic on custom ports. |
| Anti-Spam Wizard | Click the icon to open wizard that helps you choose which packet directions to check for spam. |

**Table 88** SECURITY > ANTI-SPAM > General

| LABEL | DESCRIPTION |
|---|---|
| From, To | Select the directions of travel of packets that you want to check. Select or clear a row or column's first check box (with the interface label) to select or clear the interface's whole row or column.<br>You could for example have the ZyWALL check packets traveling in from the WAN to the interface your e-mail server is on. For example, **From WAN1 To DMZ**, or **From WAN2 To DMZ**.<br>**From LAN To LAN** means packets traveling from a computer on one LAN subnet to a computer on another LAN subnet via the LAN interface of the ZyWALL. The ZyWALL does not check packets traveling from a LAN computer to another LAN computer on the same subnet.<br>**From WAN1 To WAN1** means packets that come in through the WAN 1 interface and the ZyWALL routes back out through the WAN 1 interface.<br>**From VPN** means traffic that came into the ZyWALL through a VPN tunnel and is going to the selected "to" interface. For example, **From VPN To LAN** specifies the VPN traffic that is going to the LAN or terminating at the ZyWALL's LAN interface. The ZyWALL checks the traffic after decrypting it.<br>**To VPN** is traffic that comes in through the selected "from" interface and goes out through any VPN tunnel. For example, **From LAN To VPN** specifies the traffic that is coming from the LAN and going out through a VPN tunnel. The ZyWALL checks the traffic before encrypting it.<br>**From VPN To VPN** means traffic that comes in through a VPN tunnel and goes out through (another) VPN tunnel. This is the case when the ZyWALL is the hub in a hub-and-spoke VPN. The ZyWALL checks the traffic after decrypting it (before encrypting it again).<br>Note: The VPN connection directions apply to the traffic going to or from the ZyWALL's VPN tunnels. They do not apply to other VPN traffic for which the ZyWALL is not one of the gateways (VPN pass-through traffic). |
| Action for Spam Mails | Use this section to set how the ZyWALL is to handle spam mail. |
| X-Header | An X-Header is a line (preceded by "X-") in the SMTP mail header.<br>Enter an X-tag to insert into the X-header of mails that match a black list or are identified as spam by the anti-spam external database. You can enter up to 30 ASCII characters before the colon (:) and up to 47 ASCII characters after the colon (:).<br>You can put any information as an X-tag or use "%status" and/or "%score".<br>For example, if you enter "Mail status: %status %score", you may see "Mail status: SPAM 25" in the mail header. That means the mail is classified as spam and the spam score is 25. |
| Phishing Tag | Enter a message or label (up to 16 ASCII characters) to add to the mail subject of e-mails that the anti-spam external database classifies as phishing.<br>Note: You must register for and enable the anti-spam external database feature in order for the ZyWALL to use this tag (see Chapter 6 on page 141 for details). |
| Spam Tag | Enter a message or label (up to 16 ASCII characters) to add to the mail subject of e-mails that the ZyWALL classifies as spam. |

**Table 88** SECURITY > ANTI-SPAM > General

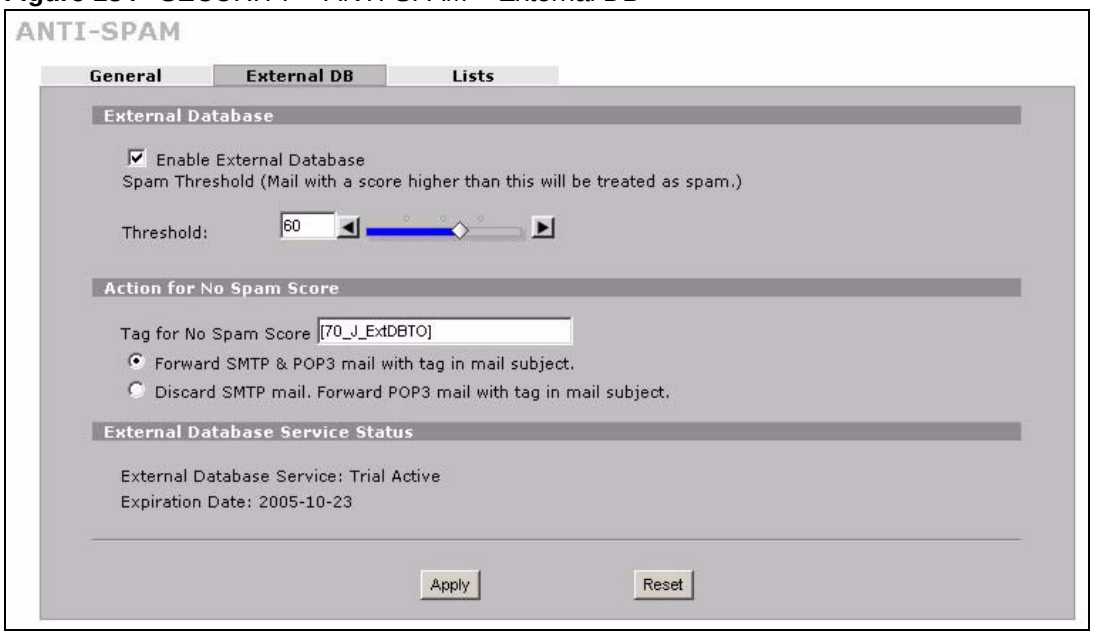
| LABEL | DESCRIPTION |
|---|---|
| Forward SMTP & POP3 mail with tag in mail subject | Select this radio button to have the ZyWALL forward spam e-mail with the tag that you define.<br>Even if you plan to use the discard option, you may want to use this initially as a test to check how accurate your anti-spam settings are. Check the e-mail the ZyWALL forwards to you to make sure that unwanted e-mail is marked as spam and legitimate e-mail is not marked as spam. |
| Discard SMTP mail. Forward POP3 mail with tag in mail subject | Select this radio button to have the ZyWALL discard spam SMTP e-mail. The ZyWALL will still forward spam POP3 e-mail with the tag that you define. |
| Action taken when mail sessions threshold is reached | The anti-spam feature limits the number of concurrent e-mail sessions. An e-mail session is when an e-mail client and e-mail server (or two e-mail servers) connect through the ZyWALL. Use this section to configure what the ZyWALL does when the number of concurrent e-mail sessions goes over the threshold (see the chapter of product specifications for the threshold).<br>Select **Forward** to have the ZyWALL allow the excess e-mail sessions without any spam filtering.<br>Select **Block** to have the ZyWALL drop mail connections to stop the excess e-mail sessions. The e-mail client or server will have to attempt to send or receive e-mail later when the number of e-mail sessions is under the threshold. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 16.3 The External DB Screen

Click **SECURITY** > **ANTI-SPAM** > **External DB** to display the **Anti-Spam External DB** screen.

Use this screen to enable or disable the use of the anti-spam external database. You can also configure the spam threshold and what to do when no valid spam score is received. You must register for this service before you can use it (see Chapter 6 on page 141 for details).

**Figure 184** SECURITY > ANTI-SPAM > External DB




The following table describes the labels in this screen.

**Table 89** SECURITY > ANTI-SPAM > External DB

| LABEL | DESCRIPTION |
|---|---|
| External Database | |
| Enable External Database | Enable the anti-spam external database feature to have the ZyWALL calculate a digest of an e-mail and send it to an anti-spam external database.<br>The anti-spam external database sends a spam score for the e-mail back to the ZyWALL. |
| Spam Threshold | The anti-spam external database checks an e-mail's digest and sends back a score that rates how likely the e-mail is to be spam. The possible range for the spam score is 0~100. The closer the score is to 100, the more likely the e-mail is to be spam.<br>Set the spam threshold (from 0 to 100) for considering an e-mail to be spam. The ZyWALL classifies any e-mail with a spam score greater than or equal to the threshold as spam. It classifies any e-mail with a spam score less than the threshold as not being spam.<br>A lower threshold catches more spam e-mails, but may also classify more legitimate e-mail as spam.<br>A higher threshold lessens the chance of classifying legitimate e-mail as spam, but may allow more spam to get through. |

**Table 89** SECURITY > ANTI-SPAM > External DB (continued)

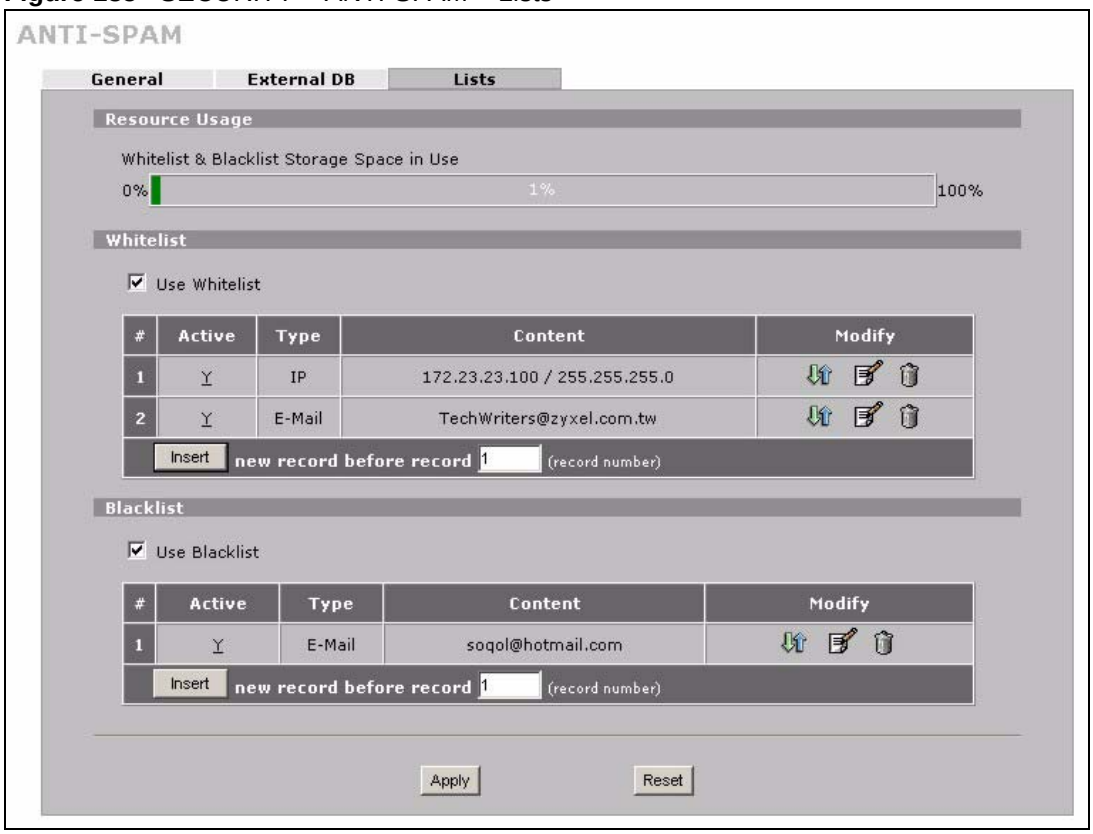
| LABEL | DESCRIPTION |
|---|---|
| Action for No Spam Score | Use this field to configure what the ZyWALL does if it does not receive a valid response from the anti-spam external database.<br>If the ZyWALL does not receive a response within seven seconds, it sends the e-mail digest a second time. If the ZyWALL still does not receive a response after another seven seconds, it takes the action that you configure here. The ZyWALL also takes this action if it receives an invalid response.<br>Here are possible reasons that would cause the ZyWALL to take this action:<br>1. The ZyWALL was not able to connect to the anti-spam external database.<br>2. The ZyWALL connected to the anti-spam external database, but there was no HTTP response within seven seconds.<br>3. The ZyWALL received an error code from the anti-spam external database.<br>4. The ZyWALL received an invalid spam score (for example a number higher than 100).<br>5. The ZyWALL received an unknown response to the anti-spam query. |
| Tag for No Spam Score | Enter a message or label (up to 16 ASCII characters) to add to the mail subject of e-mails that it forwards if a valid spam score was not received within ten seconds. |
| Forward SMTP & POP3 mail with tag in mail subject | Select this radio button to have the ZyWALL forward mail with the tag that you define. |
| Discard SMTP mail. Forward POP3 mail with tag in mail subject | Select this radio button to have the ZyWALL discard SMTP mail. The ZyWALL will still forward POP3 mail with the tag that you define. |
| External Database Service Status | This read-only field displays the status of your anti-spam external database service registration and activation.<br>**License Inactive** displays if you have not successfully registered and activated the anti-spam external database service.<br>**License Inactive** and the date your subscription expired display if your subscription to the anti-spam external database service has expired.<br>**License Active** and the subscription expiration date display if you have successfully registered the ZyWALL and activated the anti-spam external database service.<br>**Trial Active** and the trial subscription expiration date display if you have successfully registered the ZyWALL and activated the anti-spam external database service trial subscription. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 16.4 The Lists Screen

Click **SECURITY** > **ANTI-SPAM** > **Lists** to display the **Anti-Spam Lists** screen.

Configure the whitelist to identify legitimate e-mail. Configure the blacklist to identify spam e-mail. You can create whitelist or blacklist entries based on the sender's IP address or e-mail address. You can also create entries that check for particular MIME headers, MIME header values or specific subject text.

**Figure 185** SECURITY > ANTI-SPAM > Lists




The following table describes the labels in this screen.

**Table 90** SECURITY > ANTI-SPAM > Lists

| LABEL | DESCRIPTION |
|---|---|
| Resource Usage | |
| Whitelist & Blacklist Storage Space in Use | This bar displays the percentage of the ZyWALL's anti-spam whitelist and blacklist storage space that is currently in use. The bar turns from green to red when the maximum is being approached. When the bar is red, you should consider deleting unnecessary entries before adding more. |
| Whitelist | |
| Use Whitelist | Select this check box to have the ZyWALL forward e-mail that matches a whitelist entry without doing any more anti-spam checking on that individual e-mail. |
| Active | This field shows whether or not an entry is turned on. |
| Type | This field displays whether the entry is based on the e-mail's source IP address, source e-mail address, an MIME header or the e-mail's subject. |
| Content | This field displays the source IP address, source e-mail address, MIME header or subject content for which the entry checks. |
| Modify | Click the edit icon to change the entry. Click the remove icon to delete the entry. Click the move icon to change the entry's position in the list. |
| Insert | Type the index number where you want to put an entry. For example, if you type 6, your new entry becomes number 6 and the previous entry 6 (if there is one) becomes entry 7.<br>Click **Insert** to display the screen where you edit an entry. |
| Blacklist | |

**Table 90** SECURITY > ANTI-SPAM > Lists (continued)

| LABEL | DESCRIPTION |
|---|---|
| Use Blacklist | Select this check box to have the ZyWALL treat e-mail that matches a blacklist entry as spam. |
| Active | This field shows whether or not an entry is turned on. |
| Type | This field displays whether the entry is based on the e-mail's source IP address, source e-mail address, an MIME header or the e-mail's subject. |
| Content | This field displays the source IP address, source e-mail address, MIME header or subject content for which the entry checks. |
| Modify | Click the edit icon to change the entry. Click the remove icon to delete the entry. Click the move icon to change the entry's position in the list. |
| Insert | Type the index number where you want to put an entry. For example, if you type 6, your new entry becomes number 6 and the previous entry 6 (if there is one) becomes entry 7.<br>Click **Insert** to display the screen where you edit an entry. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

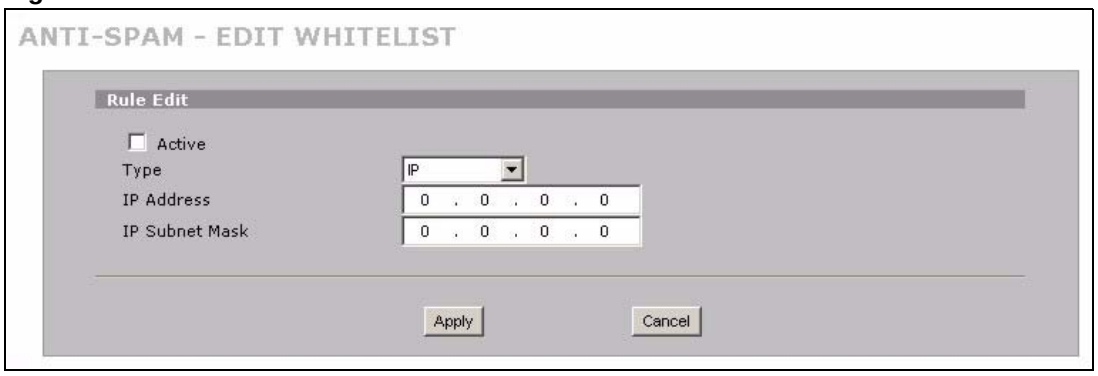
## 16.5 Anti-Spam Lists Edit Screen

Click **SECURITY** > **ANTI-SPAM** > **Lists** to display the **Anti-Spam Lists** screen. Use this screen to configure an anti-spam whitelist entry to identify legitimate e-mail or a blacklist entry to identify spam e-mail. You can create entries based on the sender's IP address or e-mail address. You can also create entries that check for particular MIME headers, MIME header values or specific subject text.

To create a new anti-spam whitelist or blacklist entry, type the index number where you want to put the entry and click **Insert** to display the **ANTI-SPAM Rule Edit** screen.

If you have already configured an anti-spam whitelist or blacklist entry, you can click the edit icon to display the **ANTI-SPAM Rule Edit** screen.

**Figure 186** SECURITY > ANTI-SPAM > Lists > Edit



The following table describes the labels in this screen.

**Table 91** SECURITY > ANTI-SPAM > Lists > Edit

| LABEL | DESCRIPTION |
|---|---|
| Rule Edit | |
| Active | Turn this entry on to have the ZyWALL use it as part of the whitelist or blacklist. You must also turn on the use of the corresponding list (in the **Anti-Spam Customization** screen) and the anti-spam feature (in the **Anti-Spam General** screen). |
| Type | Use this field to base the entry on the e-mail's source IP address, source e-mail address or an MIME header.<br>Select **IP** to have the ZyWALL check e-mail for a specific source IP address.<br>You can create whitelist IP address entries for e-mail servers on your LAN or DMZ to speed up the ZyWALL's processing of your outgoing e-mail.<br>Select **E-Mail** to have the ZyWALL check e-mail for a specific source e-mail address or domain name.<br>You can create a whitelist entry for your company's domain name (or e-mail accounts) to speed up the ZyWALL's processing of e-mail sent by your company's employees.<br>Select **MIME Header** to have the ZyWALL check e-mail for specific MIME headers or values.<br>Configure blacklist MIME header entries to check for e-mail from bulk mail programs or that have content that are commonly used in spam. You can also configure whitelist MIME header entries to allow certain MIME headers or values that identify the e-mail as being from a trusted source.<br>Select **Subject** to have the ZyWALL check e-mail for specific content in the subject line. |
| IP Address | This field displays when you select the **IP** type. Enter an IP address in dotted decimal notation. |
| IP Subnet Mask | This field displays when you select the **IP** type. Enter the subnet mask here, if applicable. |
| E-Mail Address | This field displays when you select the **E-Mail** type. Enter an e-mail address or domain name (up to 63 ASCII characters).<br>You can enter an individual e-mail address like abc@def.com.<br>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.<br>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.<br>The ZyWALL can check up to the first 63 characters of an e-mail's address. The whitelist or blacklist check fails for addresses over 63 characters. However, a whitelist or blacklist entry that uses some text followed by a wildcard only requires the ZyWALL to check the number of characters before the wildcard. So the check would still work for addresses longer than 63 characters. For example, if you used "abc*", the ZyWALL would only check up to the first three characters of the e-mail address. |
| Header | This field displays when you select the **MIME Header** type.<br>Type the header part (beginning with "X-") of an MIME header (up to 63 ASCII characters).<br>In an MIME header, the header is the part that comes before the colon (:).<br>For example, if you want the whitelist or blacklist entry to check for the MIME header "X-MSMail-Priority: Normal", enter "X-MSMail-Priority" here as the MIME header. |

**Table 91** SECURITY > ANTI-SPAM > Lists > Edit

| LABEL | DESCRIPTION |
|---|---|
| Value | This field displays when you select the **MIME Header** type.<br>Type the value part of an MIME header (up to 63 ASCII characters).<br>In an MIME header, the part that comes after the colon is the value.<br>For example, if you want the whitelist or blacklist entry to check for the MIME header “X-MSMail-Priority: Normal”, enter “Normal” here as the MIME value. |
| Subject | This field displays when you select the **Subject** type. Enter up to 63 ASCII characters of text to check for in the e-mail headers. Spaces are allowed.<br>You can use a wildcard (*). For example, if you configure “*good”, any e-mail subject that ends in “good” matches. So “this is very good” and “this is not so good” both match.<br>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.<br>The ZyWALL can check up to the first 63 characters of an e-mail’s subject. The whitelist or blacklist check fails for subjects over 63 characters. However, a whitelist or blacklist entry that uses some text followed by a wildcard only requires the ZyWALL to check the number of characters before the wildcard. So the check would still work for subjects longer than 63 characters. For example, if you used “abc*”, the ZyWALL would only check up to the first three characters of the e-mail subject. |
| Apply | Click **Apply** to save your settings and exit this screen. |
| Cancel | Click **Cancel** to exit this screen without saving. |

## 16.6 Technical Reference

The anti-spam external database uses the following spam detection engines in checking each e-mail.

- SpamBulk: This engine identifies e-mail that has been sent in bulk or is similar to e-mail that is sent in bulk.
- SpamRepute: This engine checks to see if most people want the e-mail.
- SpamContent: This engine checks to see if the message would generally be considered offensive.
- SpamTricks: This engine checks to see if the e-mail is formatted to be economical for spammers or to circumvent anti-spam rules.

## SpamRepute Engine

The SpamRepute engine calculates the reputation of the sender (whether or not most people want to receive the e-mail from this sender).

The SpamRepute engine checks proprietary and third-party databases of known spammer email addresses, domains and IP addresses. The SpamRepute engine also uses Bayesian statistical analysis to detect whether an e-mail is sent from a known in spite of a spammer’s attempt to disguise the sender’s identity. The anti-spam external database combines all of this data into a SpamRepute Index for calculating the reputation of the sender in order to guard against foreign language spam, fraud and phishing.

## SpamContent Engine

The SpamContent engine examines the e-mail's content to decide if it would generally be considered offensive. The vocabulary design, format and layout are considered as part of thousands of checks on message attributes that include the following.

- To Field
- Subject Field
- Header Fields
- Email Format, Design, and Layout
- Vocabulary, Word Formatting and Word Patterns
- Foreign Language Detection
- SMTP Envelope Content and Analysis
- Country Trace
- Image Layout Classification
- Hyperlink Analysis and Comparison
- Contact Verification

The SpamContent engine parses words into pieces to detect similar vocabulary even if the words do not match exactly. The anti-spam external database also performs Bayesian statistical analysis on the e-mail's content. The engine uses artificial intelligence technology to 'learn' over time, as spam changes.

## SpamTricks Engine

The SpamTricks engine checks for the tactics that spammers use to minimize the expense of sending lots of e-mail and tactics that they use to bypass spam filters.

Use of relays, image-only e-mails, manipulation of mail formats and HTML obfuscation are common tricks for which the SpamTricks engine checks. The SpamTricks engine also checks for "phishing" (see Section 16.2 on page 315 for more on phishing).

# 17

# Content Filtering Screens

## 17.1 Overview

Content filtering allows you to block certain web features, such as cookies, and/or block access to specific websites. With content filtering, you can do the following:

- Restrict web features. The ZyWALL can block web features such as ActiveX controls, Java applets, cookies and disable web proxies.
- Create a filter list. You can select categories, such as pornography or racial intolerance, to block from a pre-defined list.
- 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 key words that you specify.

### 17.1.1 What You Can Do in the Content Filtering Screens

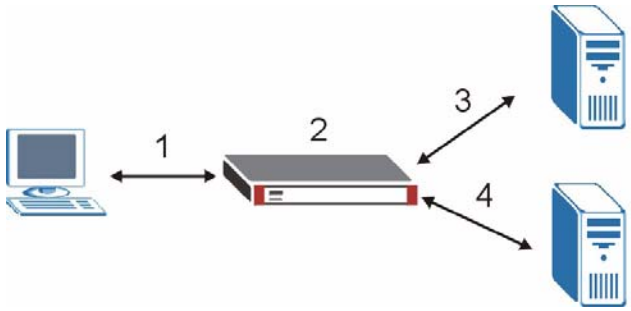
- Use the **General** screen (Section 17.2 on page 328) to enable content filtering and configure external database settings.
- Use the **Policy** screen (Section 17.2 on page 328) to configure content filtering policies on your ZyWALL.
- Use the **Object** screen (Section 17.2 on page 328) to configure lists of allowed and restricted web sites, and to block web sites based on keywords
- Use the **Cache** screen (Section 17.2 on page 328) to view and configure caching of URLs and their categorization.

### 17.1.2 What You Need to Know About Content Filtering

#### Content Filtering with an External Database

When you register for and enable external database content filtering, 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. The content filtering lookup process is described below.

**Figure 187** Content Filtering 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 17.9 on page 346). 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 will query the external content filtering database and simultaneously send the request to the web server.

   The external content filtering database may change a web site's category or categorize a previously uncategorized web site.
5. The external content filtering server sends the category information back to the ZyWALL, which then blocks and/or logs access to the web site. The web site's address and category are then stored in the ZyWALL's content filtering cache.

### Policies

Content filtering policies allow you to have different content filtering settings for different users or groups of users. For example, you may want to block most employees from accessing finance or stock websites, but allow the finance department to access these. You can set the ZyWALL to use external database content filtering and select which web site categories to block and/or log.

### Finding Out More

- See Section 5.6 on page 133 for a tutorial on content filtering.

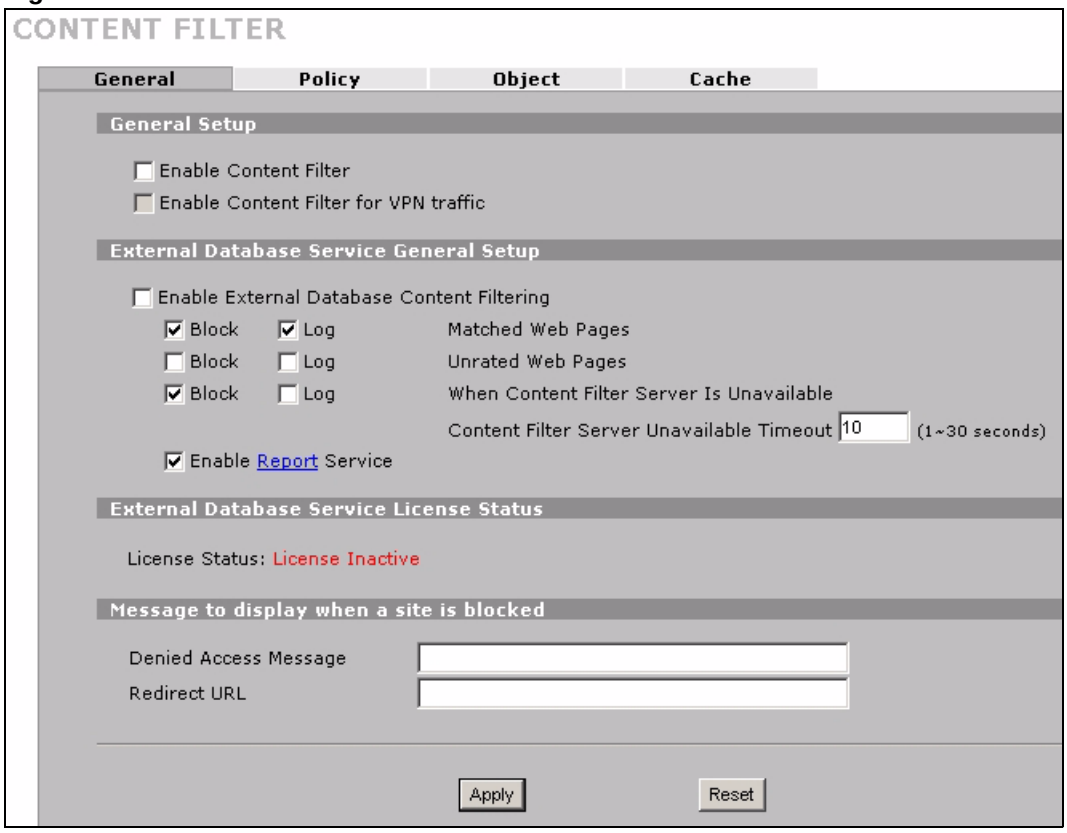
## 17.2 General Screen

Click **SECURITY** > **CONTENT FILTER** to open the **General** screen. Use this screen to enable content filtering and configure general settings.

You must register for external content filtering before you can use it.

Use the **REGISTRATION** screens (see Chapter 6 on page 141) to create a myZyXEL.com account, register your device and activate the external content filtering service.

**Figure 188** SECURITY > CONTENT FILTER > General




The following table describes the labels in this screen.

**Table 92** SECURITY > CONTENT FILTER > General

| LABEL | DESCRIPTION |
|---|---|
| General Setup | |
| Enable Content Filter | Select this check box to enable the content filter. Content filtering works on HTTP traffic that is using TCP ports 80, 119, 3128 or 8080.<br>See Section 29.2 on page 529 if you need to use content filtering for traffic on custom ports. |
| Enable Content Filter for VPN traffic | Select this check box to have the content filter apply to traffic that the ZyWALL sends out through a VPN tunnel or receives through a VPN tunnel. The ZyWALL applies the content filter to the traffic before encrypting it or after decrypting it.<br>Note: The ZyWALL can apply content filtering on the traffic going to or from the ZyWALL's VPN tunnels. It does not apply to other VPN traffic for which the ZyWALL is not one of the gateways (VPN pass-through traffic). |
| External Database Service General Setup | The external database content filtering service has the ZyWALL check an external database to find to which category a requested web page belongs. |
| Enable External Database Content Filtering | Turn on external database content filtering to have the ZyWALL block or forward access to web pages depending on the ZyWALL's external database content filtering settings. |

**Table 92** SECURITY > CONTENT FILTER > General

| LABEL | DESCRIPTION |
|---|---|
| Matched Web Pages | Select **Block** to prevent users from accessing web pages that match the categories that you select below.<br>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>Select **Log** to record attempts to access prohibited web pages. |
| Unrated Web Pages | Select **Block** to prevent users from accessing web pages that the external database content filtering has not categorized.<br>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>Select **Log** to record attempts to access web pages that are not categorized. |
| When Content Filter Server Is Unavailable | Select **Block** to block access to any requested web page if the external content filtering database is unavailable. The following are possible causes:<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>Select **Log** to record attempts to access web pages that occur when the external content filtering database is unavailable. |
| Content Filter Server Unavailable Timeout | Specify a number of seconds (1 to 30) 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. |
| Enable Report Service | Select this option to record content filtering reports on myZyXEL.com. These reports consist of generated statistics and charts of access attempts to web sites belonging to the categories you selected in your content filter configuration. Click **Report** to go to myZyXEL.com. Then do the following to view the content filtering reports (see Chapter 18 on page 349 for details).<br>1. Log into myZyXEL.com to view a list of registered devices.<br>2. Click your device's link to show content filtering reports for your ZyWALL. |
| License Status | This read-only field displays the status of your category-based content filtering (using an external database) service subscription.<br>**License Inactive** displays if you have not registered and activated the category-based content filtering service.<br>**License Active** and the subscription expiration date display if you have registered the ZyWALL and activated the category-based content filtering service.<br>**Trial Active** and the trial subscription expiration date display if you have registered the ZyWALL and activated the category-based content filtering service.<br>**License Inactive** and the date your subscription expired display if your subscription to the category-based content filtering service has expired.<br><br>Note: After you register for content filtering, you need to wait up to five minutes for content filtering to be activated. See Section 18.2 on page 349 for how to check the content filtering activation. |

**Table 92** SECURITY > CONTENT FILTER > General

| LABEL | DESCRIPTION |
|---|---|
| Message to display when a site is blocked | |
| Denied Access Message | Enter a message to be displayed when a user tries to access a restricted web site. The default message is Please contact your 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 filtering. The web page you specify here opens in a new frame below the denied access message.<br>Use "http://" followed by up to 120 ASCII characters. For example, http://192.168.1.17/blocked access.<br>If you do not specify a URL and a user tries to access a web page containing a forbidden object, a blocking page displays on the forbidden object. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

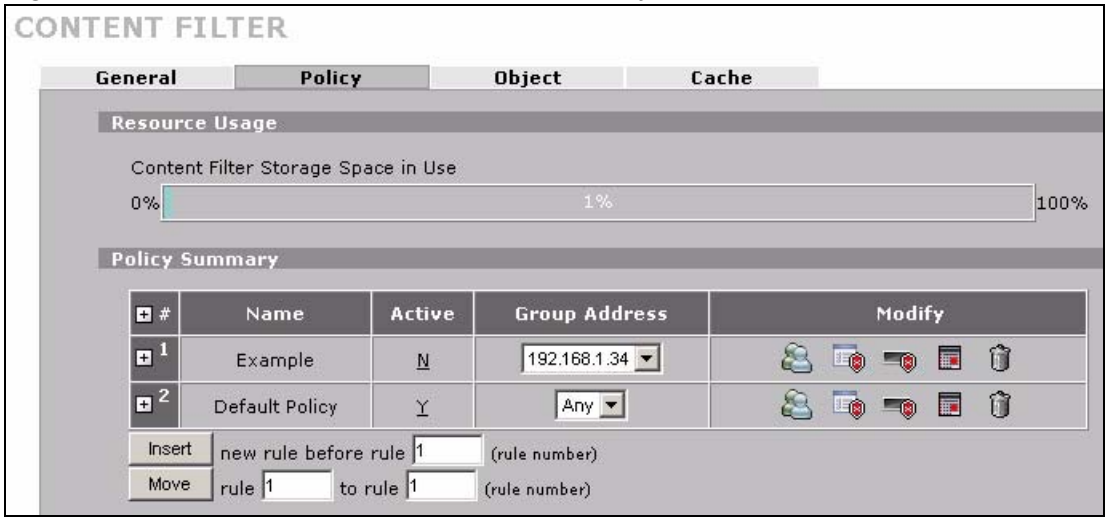
## 17.3 The Policy Screen

Click **SECURITY** >**CONTENT FILTER** > **Policy** to display the following screen. Use this screen to configure content filtering policies on your ZyWALL.

You may find that a web site has not been accurately categorized or that a web site's contents have changed and the content filtering category needs to be updated. See Section 18.4 on page 354 for how to submit the web site for review.

The ordering of your policies is very important as the ZyWALL applies policies in the order they are listed.

**Figure 189** SECURITY > CONTENT FILTER > Policy



The following table describes the labels in this screen.

**Table 93** SECURITY > CONTENT FILTER > Policy

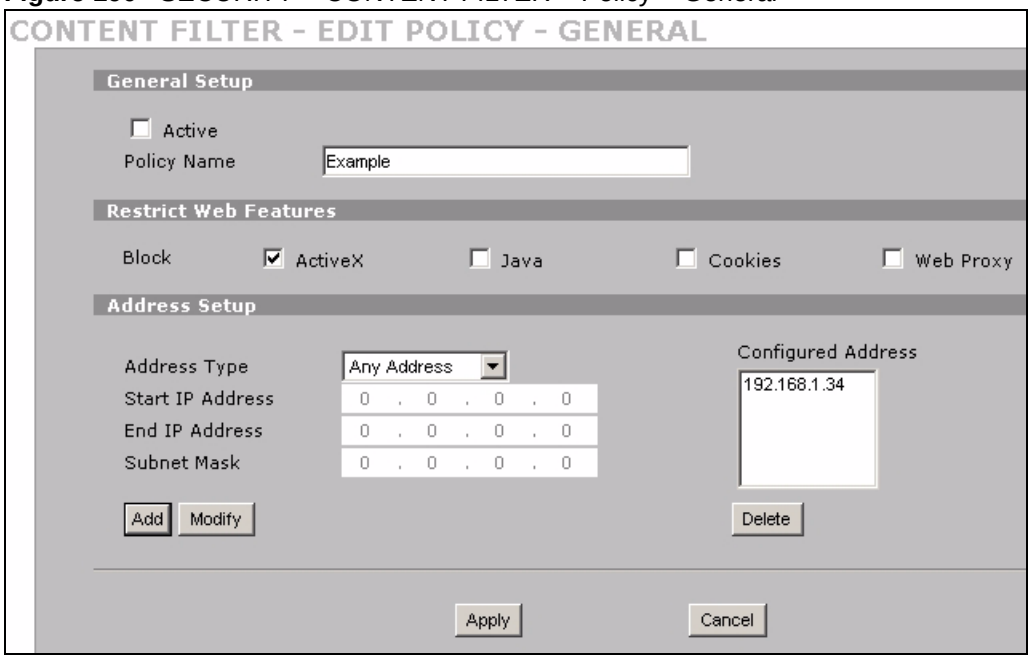
| LABEL | DESCRIPTION |
|---|---|
| Content Filter Storage Space in Use | This bar displays the percentage of the ZyWALL's content filter policies storage space that is currently in use. When the storage space is almost full, you should consider deleting unnecessary content filter policies before adding more. |
| The following fields summarize the content filter policies you have created. | |
| +/- | In the heading row, click + to expand or - to collapse the **Group Address** drop down lists for all of the displayed rules. |
| # | This is the content filter policy number. The ordering of your policies is important as rules are applied in turn. Click + to expand or - to collapse the **Group Address** drop down list. |
| Name | This is the name of the content filter policy. |
| Active | This field displays whether a content filter policy is turned on (**Y**) or not (**N**). Click the setting to change it. |
| Group Address | This drop-down list box displays the source (user) addresses or ranges of addresses to which the content filter policy applies. Please note that a blank source or destination address is equivalent to **Any**. |
| Modify | Click the general icon to restrict web features and edit the source (user) addresses or ranges of addresses to which the content filter policy applies.<br>Click the external database icon to edit which web features and content categories the content filter policy blocks.<br>Click the customization icon to configure the policy's 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.<br>Click the schedule icon to set for which days and times the policy applies.<br>Click the delete icon to remove the content filter policy. You cannot delete the default policy. A window display asking you to confirm that you want to delete the policy. Note that subsequent policies move up by one when you take this action. |
| Insert | Type the index number for where you want to put a content filter policy. For example, if you type 6, your new content filter policy becomes number 6 and the previous content filter policy 6 (if there is one) becomes content filter policy 7.<br>Click **Insert** to display the screens where you configure the content filter policy. |
| Move | Type a content filter policy's index number and the number for where you want to put that policy. Click **Move** to move the policy to the number that you typed. The ordering of your policies is important as they are applied in order of their numbering. |

## 17.4 Content Filter Policy: General

Click **SECURITY** > **CONTENT FILTER** > **Policy** and use the **Insert** button or a policy's general icon to display the following screen.

Use this screen to restrict web features and edit the source (user) addresses or ranges of addresses to which the content filter policy applies.

**Figure 190** SECURITY > CONTENT FILTER > Policy > General




The following table describes the labels in this screen.

**Table 94** SECURITY > CONTENT FILTER > Policy > General

| LABEL | DESCRIPTION |
|---|---|
| Active | Select this option to turn on the content filter policy. |
| Policy Name | Enter a descriptive name of up to 31 printable ASCII characters (except Extended ASCII characters) for the content filter policy. Spaces are allowed. |
| Restrict Web Features | Select the check box(es) to restrict a feature. When you try to access a page containing a restricted feature, the whole page will be blocked or the restricted feature part of the web page will appear blank or grayed out. You will also see the message and URL you configured in the **Denied Access Message** and **Redirect URL** fields.<br>**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.<br>**Java** is a programming language and development environment for building downloadable Web components or Internet and intranet business applications of all kinds.<br>**Cookies** are files stored on a computer's hard drive. Some web servers use them to track usage and provide service based on ID.<br>**Web Proxy** is 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. |
| Address Setup | |
| Address Type | Do you want the policy to apply to packets from a particular (single) IP, a range of IP addresses (for example 192.168.1.10 to 192.169.1.50), a subnet or any IP address? Select an option from the drop-down list box that includes: **Single Address**, **Range Address**, **Subnet Address** and **Any Address**. |

**Table 94** SECURITY > CONTENT FILTER > Policy > General (continued)

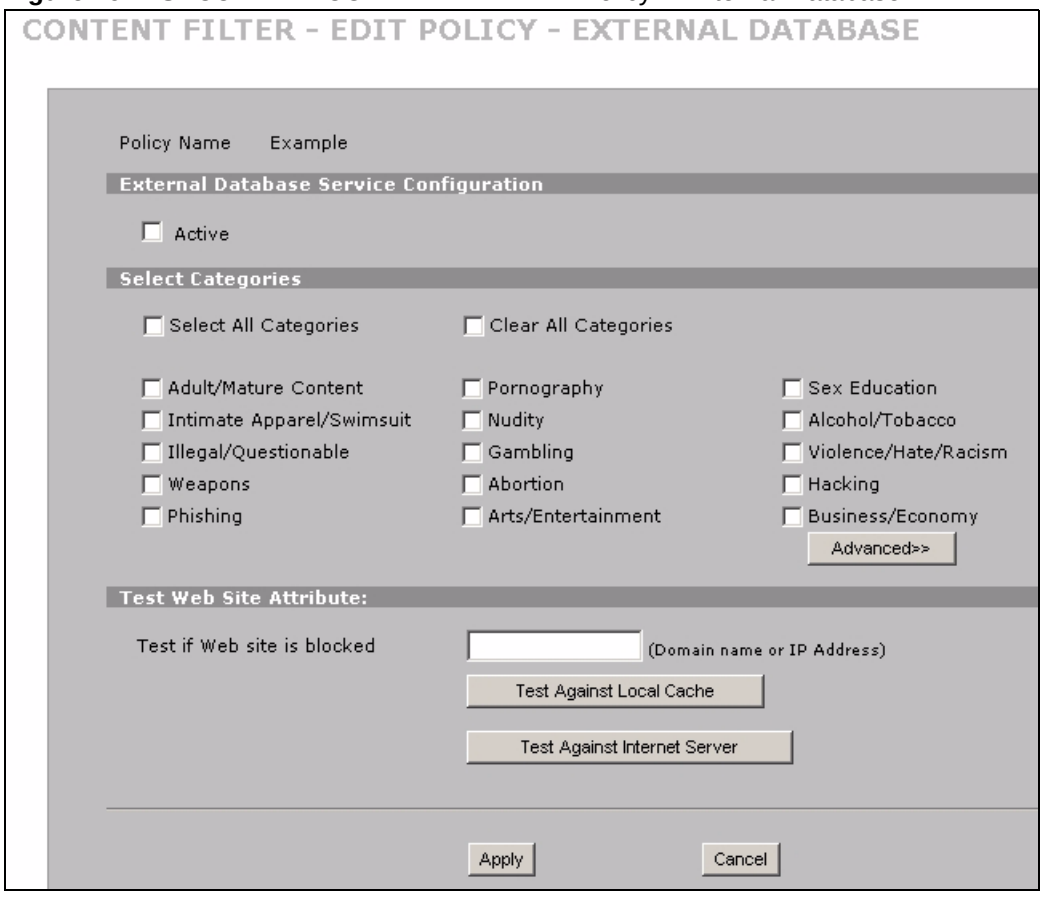
| LABEL | DESCRIPTION |
|---|---|
| Start IP Address | Enter the single IP address or the starting IP address in a range here. |
| End IP Address | Enter the ending IP address in a range here. |
| Subnet Mask | Enter the subnet mask here, if applicable. |
| Add | Click **Add** to add a new address to the **Configured Address** box. You can add multiple addresses, ranges of addresses, and/or subnets. |
| Modify | To edit an existing source or destination address, select it from the box and click **Modify**. |
| Delete | Highlight an existing source or destination address from the **Configured Address** box and click **Delete** to remove it. |
| Apply | Click **Apply** to save your customized settings and exit this screen. |
| Cancel | Click **Cancel** to exit this screen without saving. |

## 17.5 Content Filter Policy: External Database

Click **SECURITY** > **CONTENT FILTER** > **Policy** and then a policy's external database icon to display the following screen.

Use this screen to edit which content categories the content filter policy blocks.

**Figure 191** SECURITY > CONTENT FILTER > Policy > External Database



The following table describes the labels in this screen.

**Table 95** SECURITY > CONTENT FILTER > Policy > External Database

| LABEL | DESCRIPTION |
|---|---|
| Policy Name | This is the name of the content filter policy that you are configuring. |
| Active | Select this option to apply category based content filtering for this policy. |
| Select Categories | These are the categories available at the time of writing.<br><br>Note: If you chose to record attempts to access the restricted pages and a web page matches more than one category you selected, you will see a log showing this page matches one category (the first matched one) only. |
| 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. |
| Adult/Mature Content | Selecting this category excludes 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 | Selecting this category excludes pages that contain sexually explicit material for the purpose of arousing a sexual or prurient interest. |
| Sex Education | Selecting this category excludes 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 | Selecting this category excludes 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. |
| Nudity | Selecting this category excludes 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 | Selecting this category excludes 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 | Selecting this category excludes 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.). |

**Table 95** SECURITY > CONTENT FILTER > Policy > External Database (continued)

| LABEL | DESCRIPTION |
|---|---|
| Gambling | Selecting this category excludes 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 | Selecting this category excludes 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 | Selecting this category excludes 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 | Selecting this category excludes 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 | Selecting this category excludes 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. |
| Phishing | Selecting this category excludes 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). |
| Arts/Entertainment | Selecting this category excludes 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 | Selecting this category excludes 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 | Selecting this category excludes 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 | Selecting this category excludes 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. |

**Table 95** SECURITY > CONTENT FILTER > Policy > External Database (continued)

| LABEL | DESCRIPTION |
|---|---|
| Education | Selecting this category excludes 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 | Selecting this category excludes 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 | Selecting this category excludes 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 | Selecting this category excludes 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 | Selecting this category excludes 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. |
| Government/Legal | Selecting this category excludes 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 | Selecting this category excludes pages that promote or provide information on military branches or armed services. |
| Political/Activist Groups | Selecting this category excludes 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 | Selecting this category excludes 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 | Selecting this category excludes pages that sponsor or provide information on computers, technology, the Internet and technology-related organizations and companies. |
| Search Engines/Portals | Selecting this category excludes pages that support searching the Internet, indices, and directories. |

**Table 95** SECURITY > CONTENT FILTER > Policy > External Database (continued)

| LABEL | DESCRIPTION |
|---|---|
| Spyware/Malware Sources | Selecting this category excludes 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 | Selecting this category excludes 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. |
| Job Search/Careers | Selecting this category excludes pages that provide assistance in finding employment, and tools for locating prospective employers. |
| News/Media | Selecting this category excludes 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 | Selecting this category excludes pages that promote interpersonal relationships. |
| Reference | Selecting this category excludes 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 | Selecting this category excludes 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 | Selecting this category excludes pages that provide chat or instant messaging capabilities or client downloads. |
| Email | Selecting this category excludes pages offering web-based e-mail services, such as online e-mail reading, e-cards, and mailing list services. |
| Blogs/Newsgroups | Selecting this category excludes 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 95** SECURITY > CONTENT FILTER > Policy > External Database (continued)

| LABEL | DESCRIPTION |
|---|---|
| Religion | Selecting this category excludes 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 (Cult/Occult) or atheist beliefs (Political/Activist Groups). |
| Social Networking | Selecting this category excludes pages that enable people to connect with others to form an online community. Typically members describe themselves in personal web page policies 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 | Selecting this category excludes 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 | Selecting this category excludes 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 | Selecting this category excludes 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 | Selecting this category excludes pages that support the offering and purchasing of goods between individuals. This does not include classified advertisements. |
| Real Estate | Selecting this category excludes pages that provide information on renting, buying, or selling real estate or properties. |
| Society/Lifestyle | Selecting this category excludes 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 | Selecting this category excludes 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 | Selecting this category excludes pages that list, review, discuss, advertise and promote food, catering, dining services, cooking and recipes. |
| Sports/Recreation/Hobbies | Selecting this category excludes pages that promote or provide information about spectator sports, recreational activities, or hobbies. This includes pages that discuss or promote camping, gardening, and collecting. |

**Table 95** SECURITY > CONTENT FILTER > Policy > External Database (continued)

| LABEL | DESCRIPTION |
|---|---|
| Travel | Selecting this category excludes 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 | Selecting this category excludes pages that provide information on or promote vehicles, boats, or aircraft, including pages that support online purchase of vehicles or parts. |
| Humor/Jokes | Selecting this category excludes 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 | Selecting this category excludes pages that are dedicated to the electronic download of software packages, whether for payment or at no charge. |
| Pay to Surf | Selecting this category excludes pages that pay users in the form of cash or prizes, for clicking on or reading specific links, e-mail, or web pages. |
| Peer-to-Peer | Selecting this category excludes 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 | Selecting this category excludes pages that sell, deliver, or stream music or video content in any format, including sites that provide downloads for such viewers. |
| Proxy Avoidance | Selecting this category excludes 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 | Selecting this category excludes pages designed specifically for children. |
| Web Advertisements | Selecting this category excludes pages that provide online advertisements or banners. This does not include advertising servers that serve adult-oriented advertisements. |
| Web Hosting | Selecting this category excludes pages of organizations that provide top-level domain pages, as well as web communities or hosting services. |
| Advanced/Basic | Click **Advanced** to see an expanded list of categories, or click **Basic** to see a smaller list. |
| Test Web Site Attribute | |
| Test if Web site is blocked | You can check whether or not the content filter policy currently blocks any given web page. Enter a web site URL in the text box. |
| Test Against Local Cache | Click this button to test whether or not the web site above is saved in the ZyWALL's database of restricted web pages. |
| Test Against Internet Server | Click this button to test whether or not the web site above is saved in the external content filter server's database of restricted web pages. |
| Apply | Click **Apply** to save your settings and exit this screen. |
| Cancel | Click **Cancel** to exit this screen without saving. |

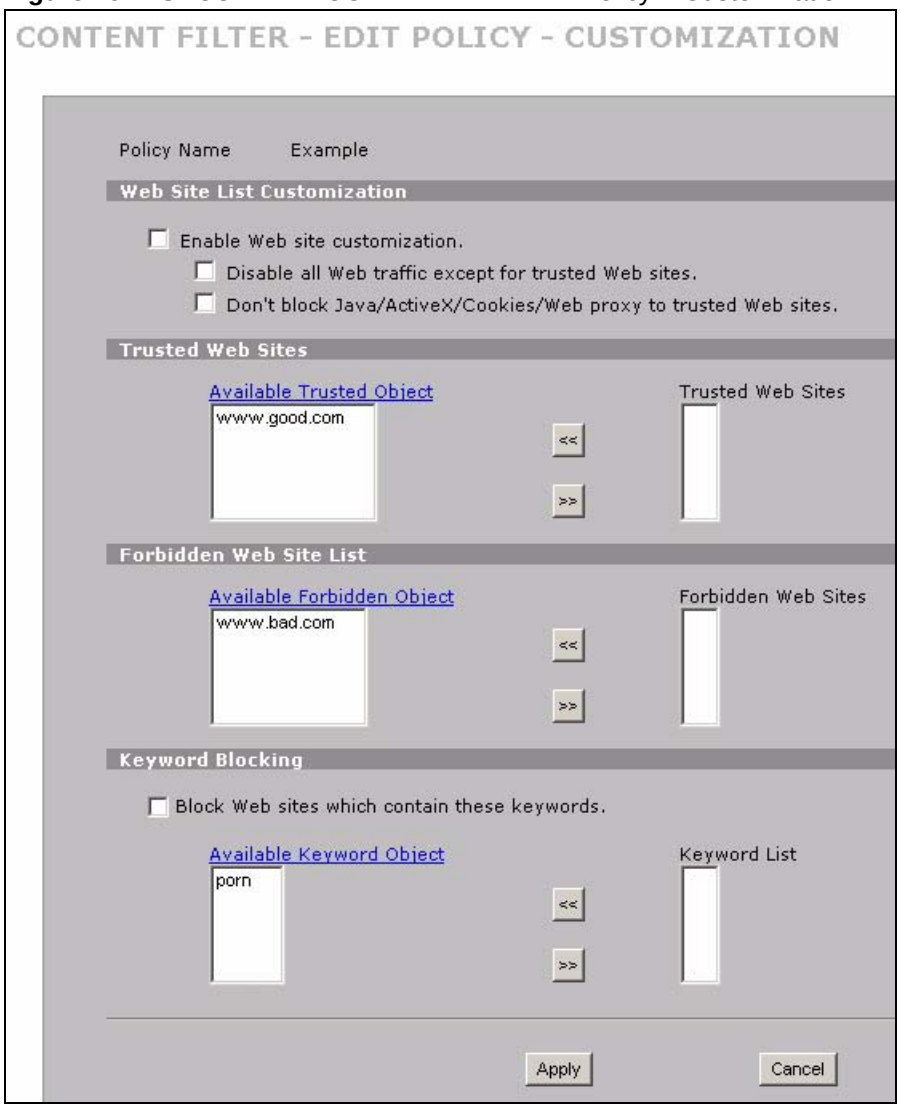
## 17.6 Content Filter Policy: Customization

Click **SECURITY** > **CONTENT FILTER** > **Policy** and then a policy's customization icon to display the following screen.

Use this screen to select good (allowed) web site addresses for this policy and 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.

Use the **SECURITY** > **CONTENT FILTER** > **Object** screen (see Section 17.8 on page 343) first to configure the master lists of trusted (allowed) web sites, forbidden (blocked) web sites, and keywords.

**Figure 192** SECURITY > CONTENT FILTER > Policy > Customization



The following table describes the labels in this screen.

**Table 96** SECURITY > CONTENT FILTER > Policy > Customization

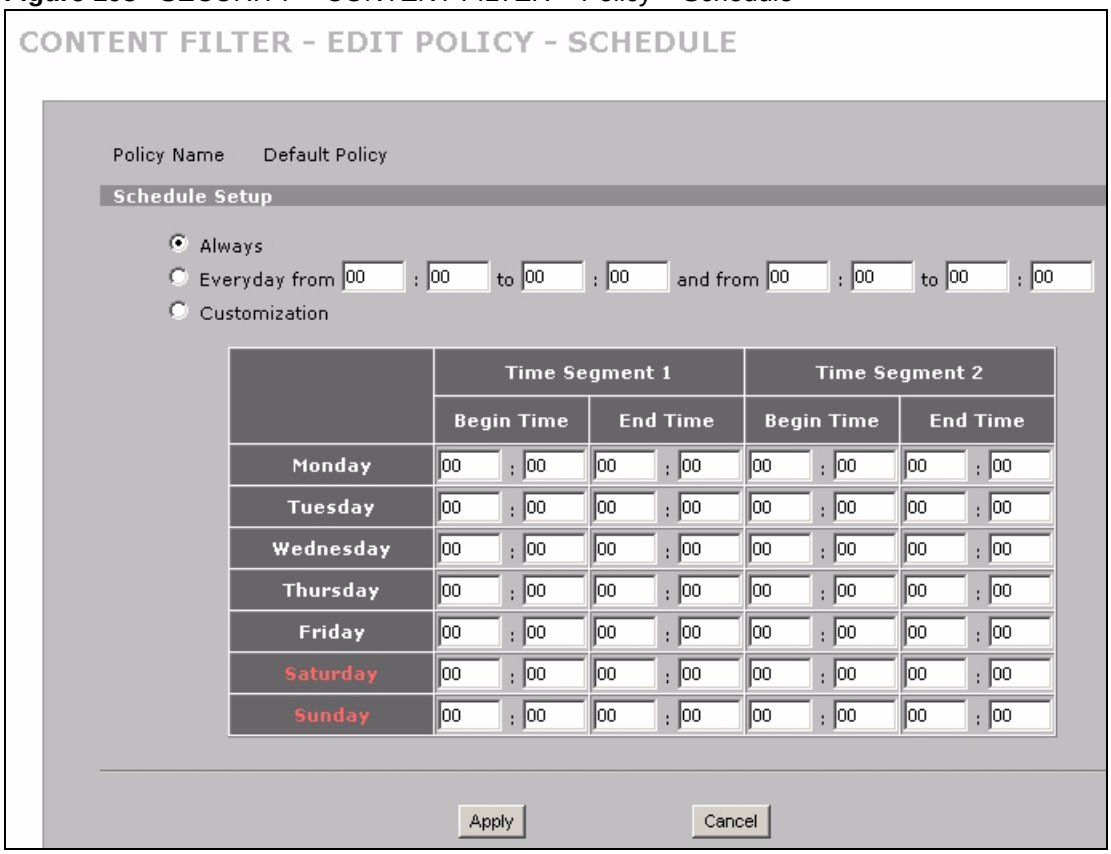
| LABEL | DESCRIPTION |
|---|---|
| Policy Name | This is the name of the content filter policy that you are configuring. |
| Web Site List Customization | |
| Enable Web site customization | Select this check box to allow trusted web sites and block forbidden web sites. Content filter list customization may be enabled and disabled without re-entering these site names. |
| Disable all Web traffic except for trusted Web sites | When this box is selected, the ZyWALL only allows Web access to sites on the **Trusted Web Site** list. If they are chosen carefully, this is the most effective way to block objectionable material. |
| Don't block 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 Site** list to the LAN. In certain cases, it may be desirable to allow Java, ActiveX or Cookies from sites that are known and trusted. |
| Available Trusted Object | This list displays the trusted host names you configured in the **SECURITY > CONTENT FILTER > Object** screen (click **Available Trusted Object** to go there). Select the ones to which you want to allow access and use the arrow button to move them to the **Trusted Web Sites** list. |
| Trusted Web Sites | This list displays web sites to which this content filtering policy allows access. Select an entry and use the arrow button to remove it from the list. |
| Available Forbidden Object | This list displays the forbidden host names you configured in the **SECURITY > CONTENT FILTER > Object** screen (click **Available Forbidden Object** to go there). Select the ones you want this policy to block and use the arrow button to move them to the **Forbidden Web Sites** list. |
| Forbidden Web Sites | This list displays web sites to which this content filtering policy blocks access. Select an entry and use the arrow button to remove it from the list. |
| Keyword Blocking | Keyword blocking allows you to block websites with URLs that contain certain keywords in the domain name or IP address. |
| Block Web sites which contain these keywords. | Select this check box to enable keyword blocking. |
| Available Keyword Object | This list displays the keywords you configured in the **SECURITY > CONTENT FILTER > Object** screen (click **Available Keyword Object** to go there). Select the ones you want this policy to block and use the arrow button to move them to **Keyword List**. |
| Keyword List | This list displays the keywords that this content filtering policy blocks. Select an entry and use the arrow button to remove it from the list. |
| Apply | Click **Apply** to save your settings and exit this screen. |
| Cancel | Click **Cancel** to exit this screen without saving. |

## 17.7 Content Filter Policy: Schedule

Click **SECURITY** > **CONTENT FILTER** > **Policy** and then a policy's schedule icon to display the following screen.

Use this screen to set for which days and times the policy applies.

**Figure 193** SECURITY > CONTENT FILTER > Policy > Schedule




The following table describes the labels in this screen.

**Table 97** SECURITY > CONTENT FILTER > Policy > Schedule

| LABEL | DESCRIPTION |
|---|---|
| Policy Name | This is the name of the content filter policy that you are configuring. |
| Schedule Setup | Content filtering scheduling applies to the filter list, customized sites and keywords. Restricted web server data, such as ActiveX, Java, Cookies and Web Proxy are not affected. |
| Always | Select this option to have content filtering active all the time. |
| Everyday from/to | Select this option to have content filtering active during the specified time interval(s) of each day. In the **from** and **to** fields, enter the time period(s), in 24-hour format, during which content filtering will be enforced. |
| Customization | Select this option to have content filtering only active during the specified time interval(s) of the specified day(s). In the **Begin Time** and **End Time** fields, enter the time period(s), in 24-hour format, for individual day(s) of the week. |
| Apply | Click **Apply** to save your settings and exit this screen. |
| Cancel | Click **Cancel** to exit this screen without saving. |

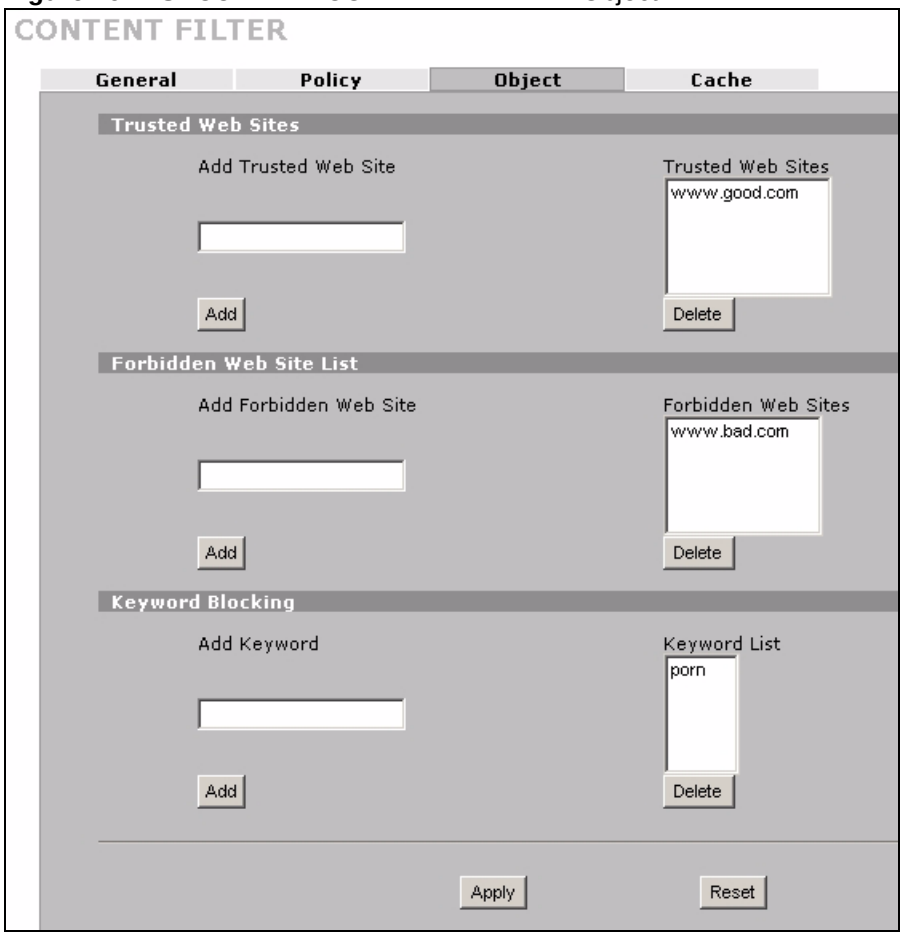
## 17.8 Content Filter Object

Click **SECURITY** > **CONTENT FILTER** > **Object** to display the following screen.

Use this screen to configure a list of allowed web site addresses for this policy and a list of 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.

To use this screens settings in content filtering, you must use the **SECURITY > CONTENT FILTER > Policy > Customization** screen to set individual policies to add or remove specific sites or keywords for individual policies.

**Figure 194** SECURITY > CONTENT FILTER > Object



The following table describes the labels in this screen.

**Table 98** SECURITY > CONTENT FILTER > Object

| LABEL | DESCRIPTION |
|---|---|
| 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. You can enter up to 32 entries. |
| 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”, etc. |
| 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 Site** 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. You can enter up to 32 entries. |
| 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 blocked. For example, entering “bad-site.com” also blocks “www.bad-site.com”, “partner.bad-site.com”, “press.bad-site.com”, etc. |
| 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 Site** list, and then click this button to delete it from that list. |
| Keyword Blocking | **Keyword Blocking** allows you to block websites with URLs that contain certain keywords in the domain name or IP address.<br>By default, the ZyWALL checks the URL’s domain name or IP address when performing keyword blocking.<br>This means that the ZyWALL checks the characters that come before the first slash in the URL.<br>For example, with the URL www.zyxel.com/news/pressroom.php, content filtering only searches for keywords within www.zyxel.com.<br>See the CLI reference guide to set the ZyWALL to check the full path of the URL (the characters that come before the last slash in the URL). |
| Add Keyword | Enter a keyword (up to 31 printable ASCII characters) to block. You can also enter a numerical IP address. |
| Keyword List | 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 **Keyword List**, and then click this button to delete it from that list. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# 17.9 Content Filtering Cache

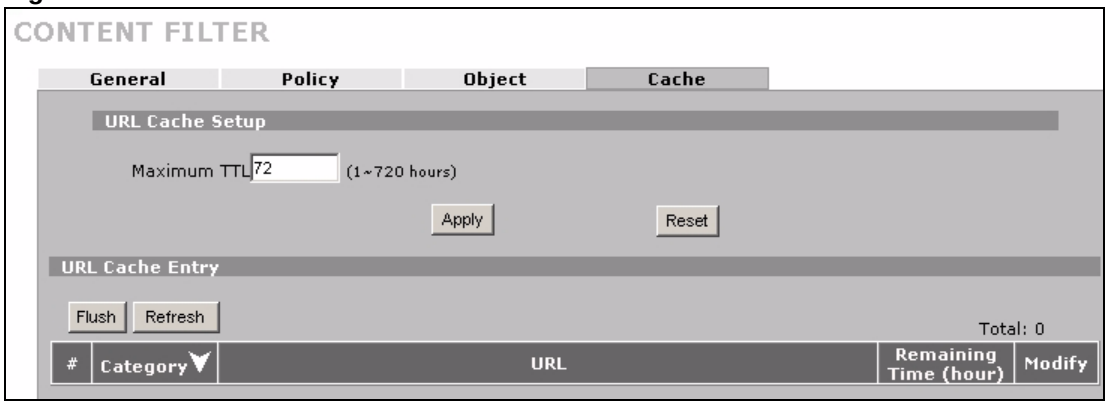
Click **SECURITY** > **CONTENT FILTER** > **Cache** to display the **CONTENT FILTER Cache** screen.

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.

Please see Section 18.4 on page 354 for how to submit a web site that has been incorrectly categorized.

**Figure 195** SECURITY > CONTENT FILTER > Cache




The following table describes the labels in this screen.

**Table 99** SECURITY > CONTENT FILTER > Cache

| LABEL | DESCRIPTION |
|---|---|
| URL Cache Setup | |
| Maximum TTL | Type the maximum time to live (TTL) (1 to 720 hours). This sets how long the ZyWALL is to allow an entry to remain in the URL cache before discarding it. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |
| URL Cache Entry | |
| Flush | Click this button to clear all web site addresses from the cache manually. |
| Refresh | Click this button to reload the cache. |
| # | This is the index number of a categorized web site address record. |
| Category | This field shows the site category to which requested access belongs. |
| URL | This is a web site's address that the ZyWALL previously checked with the external content filtering database. |
| Remaining Time (hour) | This is the number of hours left before the URL entry is discarded from the cache. |
| Modify | Click the delete icon to remove the URL entry from the cache. |

# 18

# Content Filtering Reports

## 18.1 Overview

This chapter describes how to view content filtering reports after you have activated the category-based content filtering subscription service.

See Chapter 6 on page 141 on how to create a myZyXEL.com account, register your device and activate the subscription services using the **REGISTRATION** screens.

## 18.2 Checking Content Filtering Activation

After you activate content filtering, you need to wait up to five minutes for content filtering to be turned on.

Since there will be no content filtering activation notice, you can do the following to see if content filtering is active.

1. Go to your device's web configurator's **CONTENT FILTER Categories** screen.
2. Select at least one category and click **Apply**.
3. Enter a valid URL or IP address of a web site in the **Test if Web site is blocked** field and click the **Test Against Internet Server** button.
   When content filtering is active, you should see an access blocked or access forwarded message. An error message displays if content filtering is not active.

## 18.3 Viewing Content Filtering Reports

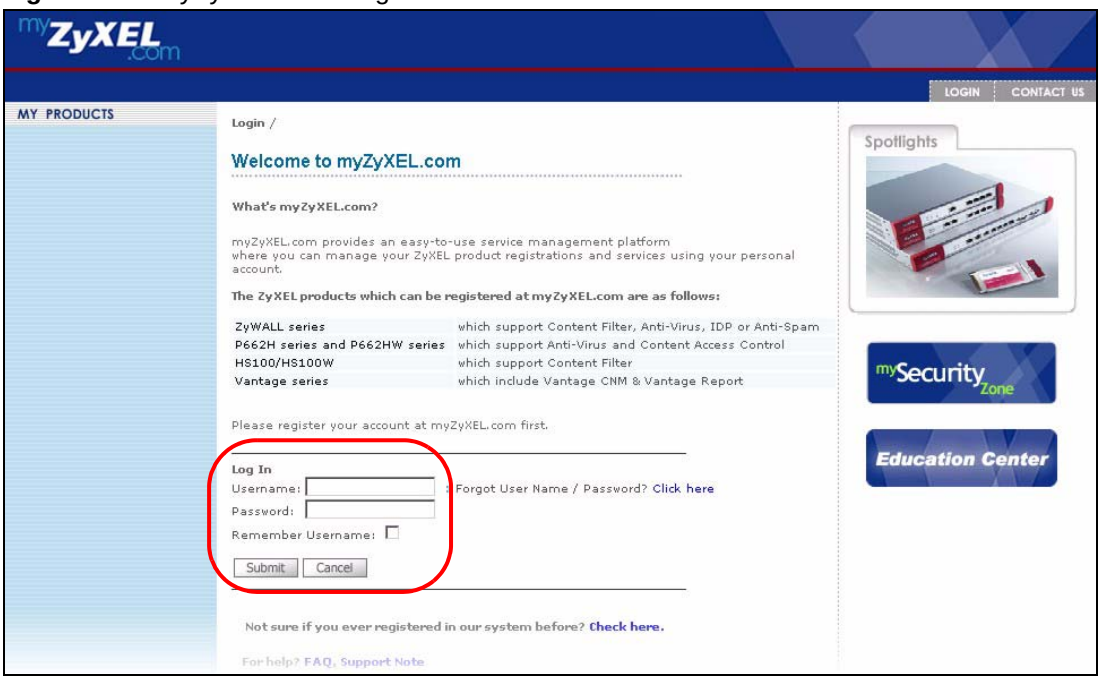
Content filtering reports are generated statistics and charts of access attempts to web sites belonging to the categories you selected in your device content filter screen.

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).

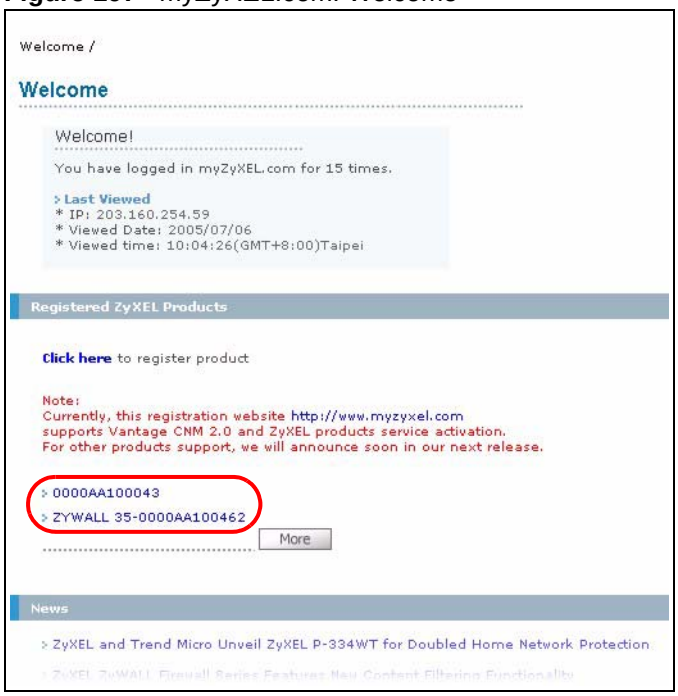
1. Go to http://www.myZyXEL.com.
2. Fill in your myZyXEL.com account information and click **Submit**.

**Figure 196** myZyXEL.com: Login



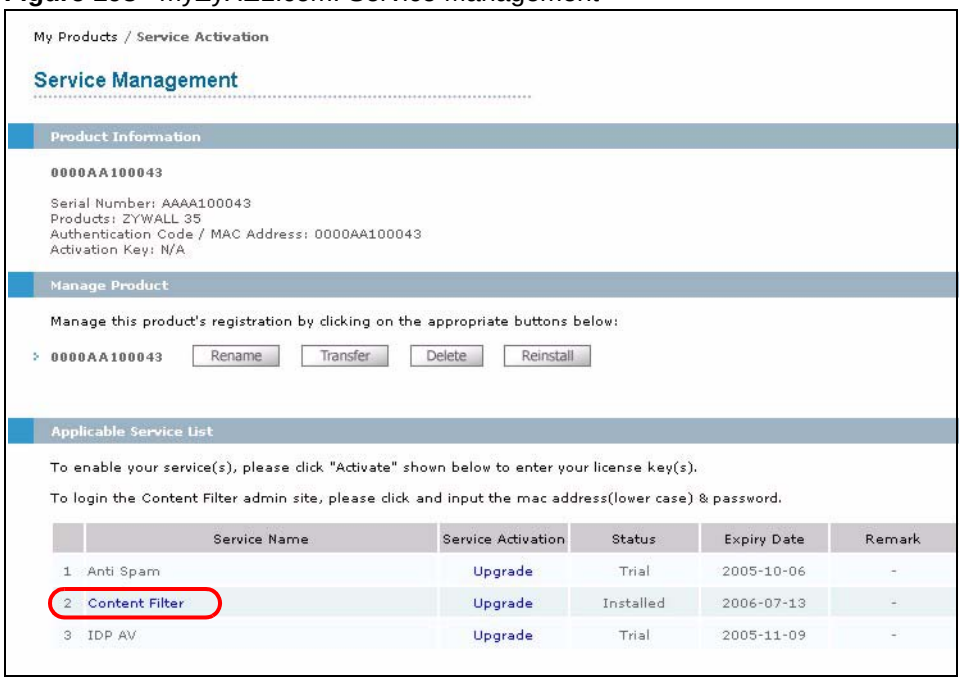

**3** A welcome screen displays. Click your ZyWALL's model name and/or MAC address under **Registered ZyXEL Products**. You can change the descriptive name for your ZyWALL using the **Rename** button in the **Service Management** screen (see Figure 198 on page 351).

**Figure 197** myZyXEL.com: Welcome




**4** In the **Service Management** screen click **Content Filter** in the **Service Name** field to open the Blue Coat login screen.

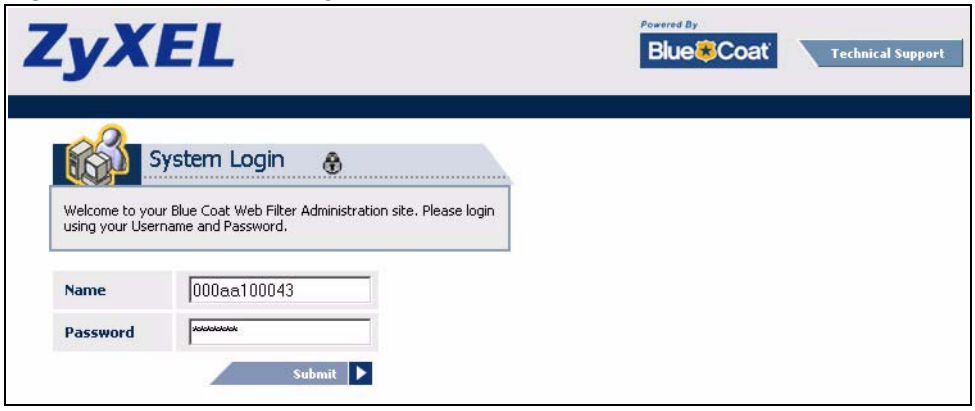
**Figure 198** myZyXEL.com: Service Management




5 Enter your ZyXEL device's MAC address (in lower case) in the **Name** field. You can find this MAC address in the **Service Management** screen (Figure 198 on page 351). Type your myZyXEL.com account password in the **Password** field.

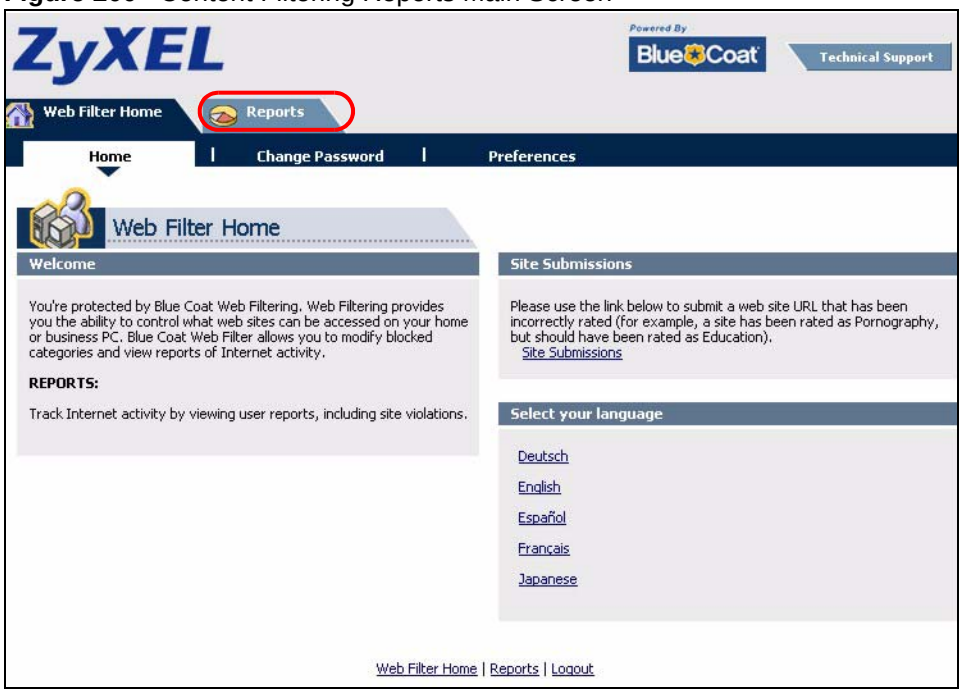
6 Click **Submit**.

**Figure 199** Blue Coat: Login



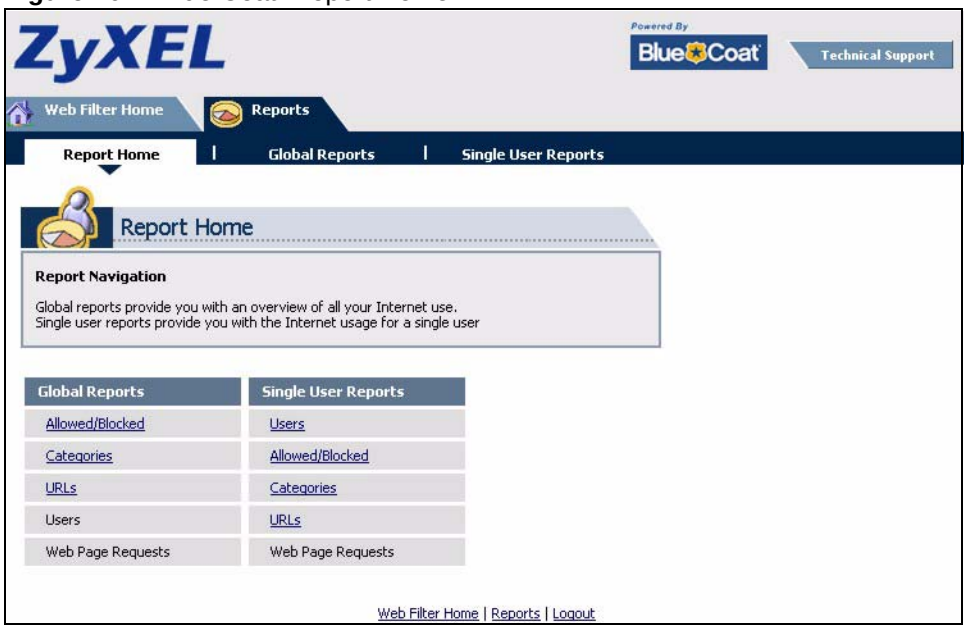

7 In the **Web Filter Home** screen, click the **Reports** tab.

**Figure 200** Content Filtering Reports Main Screen




8 Select items under **Global Reports** or **Single User Reports** to view the corresponding reports.

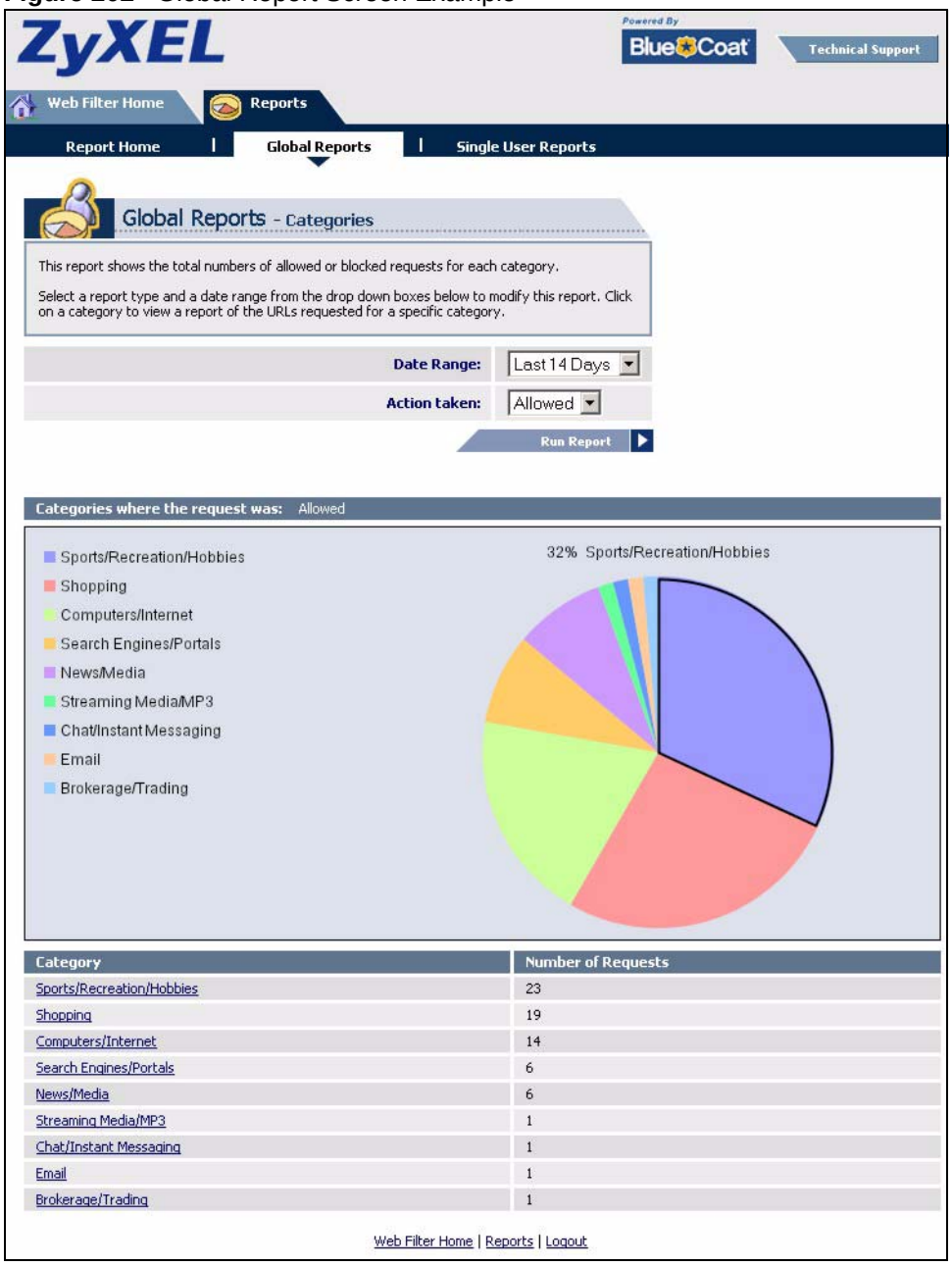
**Figure 201** Blue Coat: Report Home




9 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.

10 A chart and/or list of requested web site categories display in the lower half of the screen.

**Figure 202** Global Report Screen Example




**11** You can click a category in the **Categories** report or click **URLs** in the **Report Home** screen to see the URLs that were requested.

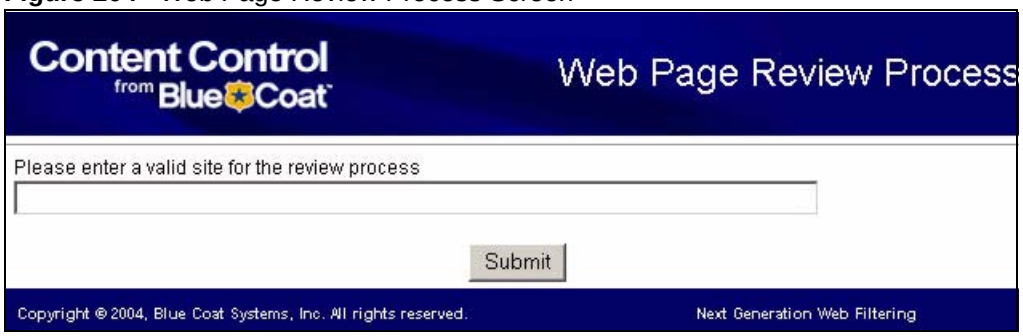
**Figure 203** Requested URLs Example


## 18.4 Web Site Submission

You may find that a web site has not been accurately categorized or that a web site's contents have changed and the content filtering category needs to be updated. Use the following procedure to submit the web site for review.

1. Log into the content filtering reports web site (see Section 18.3 on page 349).
2. In the **Web Filter Home** screen (see Figure 200 on page 352), click **Site Submissions** to open the **Web Page Review Process** screen shown next.

**Figure 204** Web Page Review Process Screen




**3** Type the web site's URL in the field and click **Submit** to have the web site reviewed.

# 19

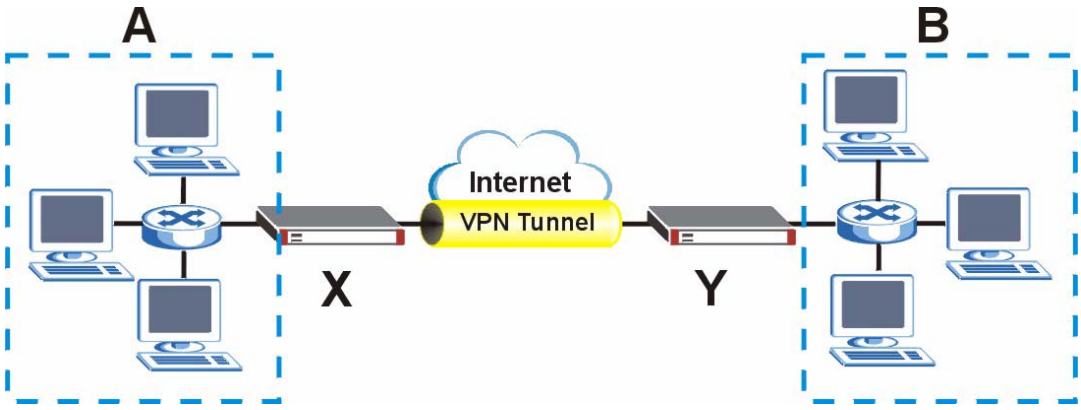
# IPSec VPN

## 19.1 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 205** VPN: Example




The VPN tunnel connects the ZyWALL (**X**) and the remote IPSec router (**Y**). These routers then connect the local network (**A**) and remote network (**B**).

### 19.1.1 What You Can Do in the IPSec VPN Screens

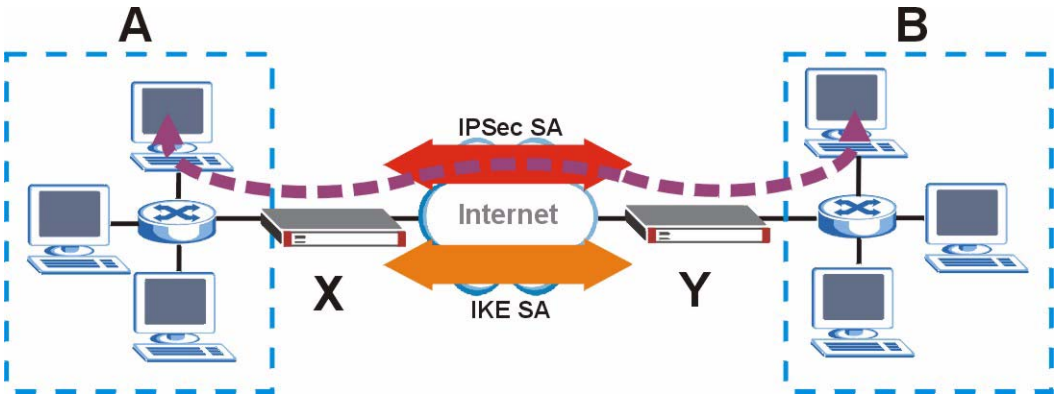
- Use the **VPN Rules (IKE)** screens (see Section 19.2 on page 360) to manage the ZyWALL's list of VPN rules (tunnels) that use IKE SAs.
- Use the **VPN Rules (Manual)** screens (see Section 19.7 on page 375) to manage the ZyWALL's list of VPN rules (tunnels) that use manual keys. You may want to configure a VPN rule that uses manual key management if you are having problems with IKE key management.
- Use the **SA Monitor** screen (see Section 19.9 on page 379) to display and manage active VPN connections.

- Use the **VPN Global Setting** screen (see Section 19.10 on page 379) to change settings that apply to all of your VPN tunnels.

## 19.1.2 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 206** VPN: IKE SA and IPSec SA



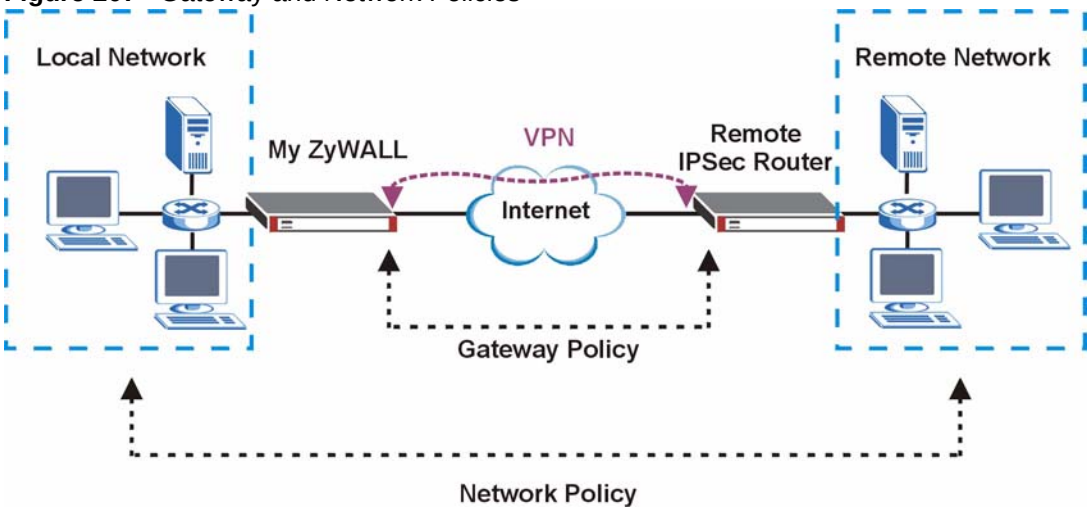

In this example, a computer in network **A** is exchanging data with a computer in network **B**. Inside networks **A** and **B**, the data is transmitted the same way data is normally transmitted in the networks. Between routers **X** and **Y**, the data is protected by tunneling, encryption, authentication, and other security features of the IPSec SA. The IPSec SA is established securely using the IKE SA that routers **X** and **Y** established first.

### Gateway and Network Policies

A VPN (Virtual Private Network) tunnel gives you a secure connection to another computer or network.

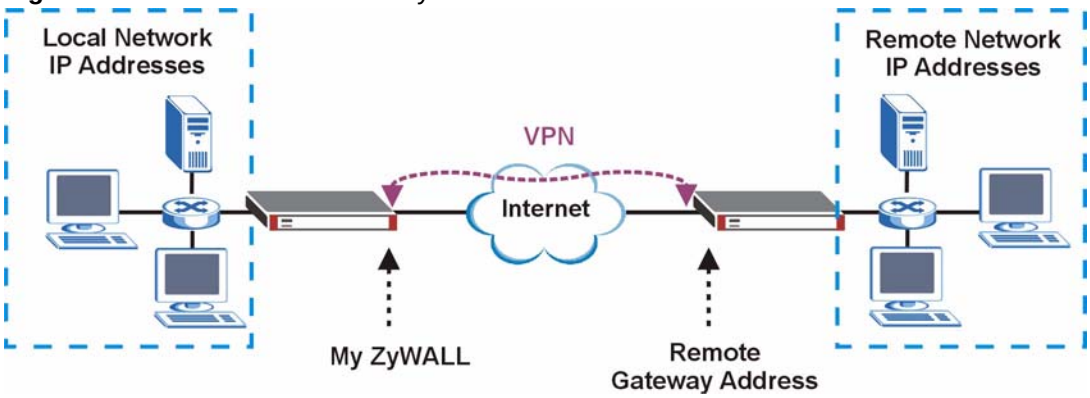
- A gateway policy contains the IKE SA settings. It identifies the IPSec routers at either end of a VPN tunnel. The IKE SA provides a secure connection between the ZyWALL and remote IPSec router.
- A network policy contains the IPSec SA settings. It specifies which devices (behind the IPSec routers) can use the VPN tunnel.

**Figure 207** Gateway and Network Policies




This figure helps explain the main fields in the VPN setup.

**Figure 208** IPSec Fields Summary




### Negotiation Mode

It takes several steps to establish an IKE SA. The negotiation mode determines the number of steps to use. There are two negotiation modes--main mode and aggressive mode. Main mode provides better security, while aggressive mode is faster.

Both routers must use the same negotiation mode.

These modes are discussed in more detail in Negotiation Mode on page 391. Main mode is used in various examples in the rest of this section.

### IP Addresses of the ZyWALL and Remote IPSec Router

In the ZyWALL, you have to specify the IP addresses of the ZyWALL and the remote IPSec router to establish an IKE SA.

You can usually provide a static IP address or a domain name for the ZyWALL. Sometimes, your ZyWALL might also offer another alternative, such as using the IP address of a port or interface.

You can usually provide a static IP address or a domain name for the remote IPSec router as well. Sometimes, you might not know the IP address of the remote IPSec router (for example, telecommuters). In this case, you can still set up the IKE SA, but only the remote IPSec router can initiate an IKE SA.

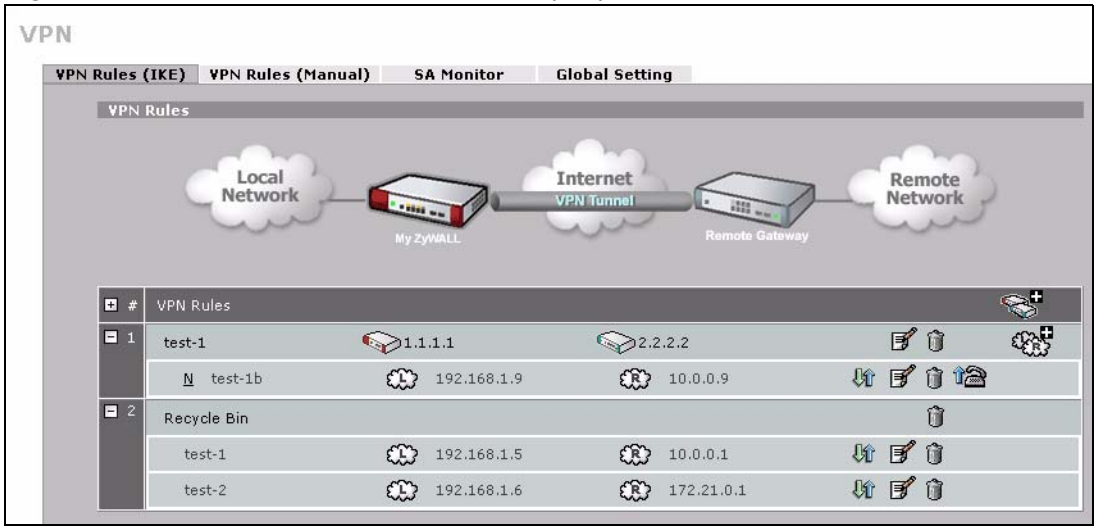
### Finding Out More

- See Section 19.14 on page 388 for IPSec VPN background information.

## 19.2 The VPN Rules (IKE) Screen

Click **SECURITY** > **VPN** to display the **VPN Rules (IKE)** screen. Use this screen to manage the ZyWALL's list of VPN rules (tunnels) that use IKE SAs.

**Figure 209** SECURITY > VPN > VPN Rules (IKE)




The following table describes the labels in this screen.

**Table 100** SECURITY > VPN > VPN Rules (IKE)

| LABEL | DESCRIPTION |
|---|---|
| +/- | In the heading row, click + to expand or - to collapse the VPN rule network policies. |
| VPN Rules | These VPN rules define the settings for creating VPN tunnels for secure connection to other computers or networks. |
|  | Click this icon to add a VPN gateway policy (or IPSec rule). |
| # | This is your VPN rule number. Click + to expand or - to collapse the VPN rule's network policies. |

**Table 100** SECURITY > VPN > VPN Rules (IKE) (continued)

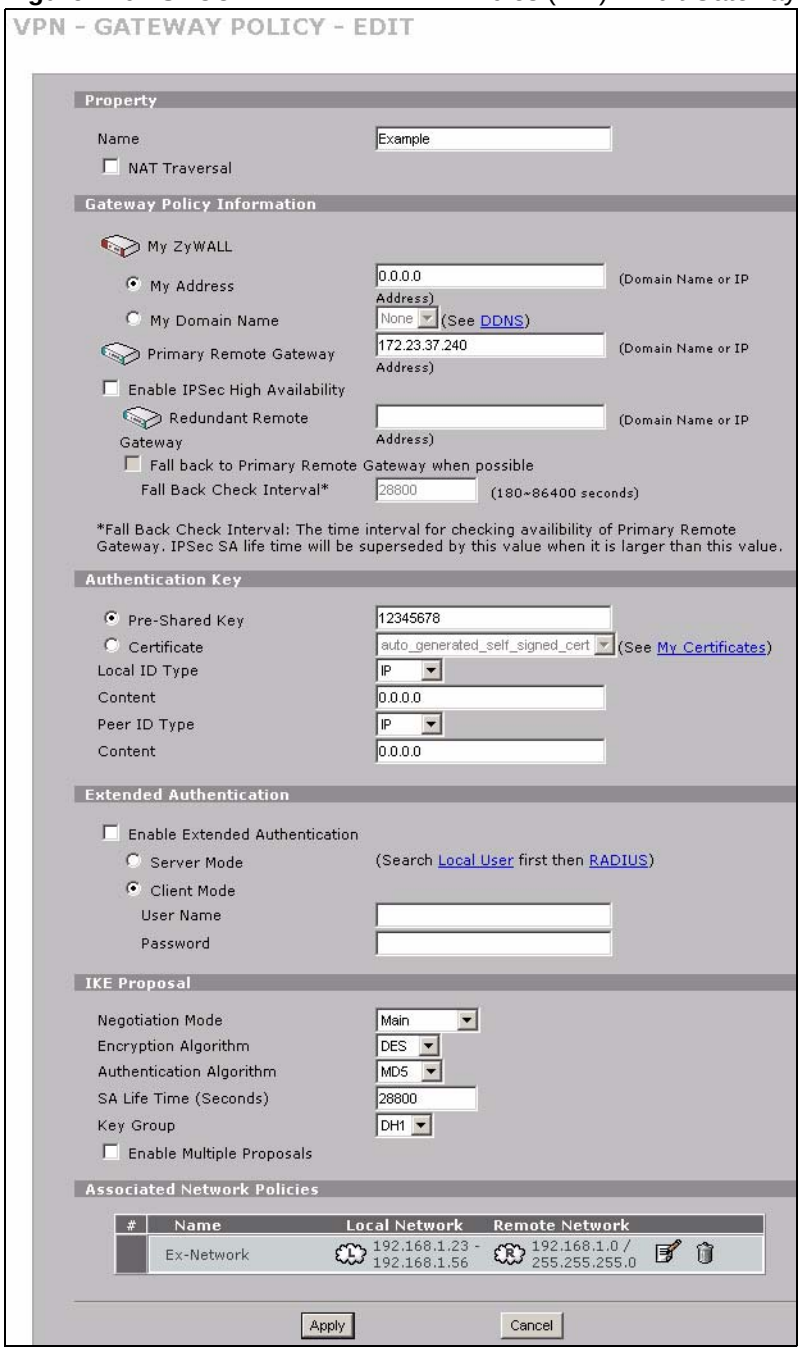
| LABEL | DESCRIPTION |
|---|---|
| Gateway Policies | The first row of each VPN rule represents the gateway policy.<br>The gateway policy identifies the IPSec routers at either end of a VPN tunnel (**My ZyWALL** and **Remote Gateway**) and specifies the authentication, encryption and other settings needed to negotiate a phase 1 IKE SA (click the edit icon to display the other settings). |
|  My ZyWALL | This represents your ZyWALL.<br>The WAN IP address, domain name or dynamic domain name of your ZyWALL displays in router mode.<br>The ZyWALL's IP address displays in bridge mode. |
|  Remote Gateway | This represents the remote secure gateway.<br>The IP address, domain name or dynamic domain name of the remote IPSec router displays if you specify it, otherwise **Dynamic** displays. |
|  | Click this icon to add a VPN network policy. |
| Network Policies | The subsequent rows in a VPN rule are network policies. A network policy identifies the devices behind the IPSec routers at either end of a VPN tunnel and specifies the authentication, encryption and other settings needed to negotiate a phase 2 IPSec SA. |
| Y/N | This field displays whether the network policy is active (**Y**) or not (**N**). Click the setting to change it. |
|  Local Network | This is the network behind the ZyWALL. A network policy specifies which devices (behind the IPSec routers) can use the VPN tunnel. |
|  Remote Network | This is the remote network behind the remote IPsec router. |
|  | Click this icon to display a screen in which you can associate a network policy to a gateway policy or move it to the recycle bin. |
|  | Click this icon to display a screen in which you can change the settings of a gateway or network policy. |
|  | Click this icon to delete a gateway or network policy. When you delete a gateway, the ZyWALL automatically moves the associated network policy(ies) to the recycle bin. When you delete a network policy, it is just deleted. |
|  | Click this icon to establish a VPN connection to a remote network. |
|  | Click this icon to drop a VPN connection to a remote network. |
| Recycle Bin | The recycle bin appears when you have any network policies that are not associated to a gateway policy.<br>• When you delete a gateway, the ZyWALL automatically moves the associated network policy(ies) to the recycle bin.<br>• You can also manually move a network policy that you do not need (but may want to use again later) to the recycle bin. Click the network policy's move or edit icon and set its **Gateway Policy** to **Recycle Bin**. |

## 19.3 The VPN Rules (IKE) Gateway Policy Edit Screen

In the **VPN Rule (IKE)** screen, click the add gateway policy (  ) icon or the edit (  ) icon to display the **VPN-Gateway Policy -Edit** screen.

Use this screen to configure a VPN gateway policy. The gateway policy identifies the IPSec routers at either end of a VPN tunnel (**My ZyWALL** and **Remote Gateway**) and specifies the authentication, encryption and other settings needed to negotiate a phase 1 IKE SA.

**Figure 210** SECURITY > VPN > VPN Rules (IKE) > Edit Gateway Policy



The following table describes the labels in this screen.

**Table 101** SECURITY > VPN > VPN Rules (IKE) > Edit Gateway Policy

| LABEL | DESCRIPTION |
|---|---|
| Property | |
| Name | Type up to 32 characters to identify this VPN gateway policy. You may use any character, including spaces, but the ZyWALL drops trailing spaces. |
| 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>Note: The remote IPSec router must also have NAT traversal enabled. See VPN, NAT, and NAT Traversal on page 392 for more information.<br>You can use NAT traversal with **ESP** protocol using **Transport** or **Tunnel** mode, but not with **AH** protocol nor with manual key management. In order for an IPSec router behind a NAT router to receive an initiating IPSec packet, set the NAT router to forward UDP ports 500 and 4500 to the IPSec router behind the NAT router. |
| Gateway Policy Information | |
| My ZyWALL | When the ZyWALL is in router mode, this field identifies the WAN IP address or domain name of the ZyWALL. You can select **My Address** and enter the ZyWALL's static WAN IP address (if it has one) or leave the field set to 0.0.0.0.<br>The ZyWALL uses its current WAN IP address (static or dynamic) in setting up the VPN tunnel if you leave this field as **0.0.0.0**. If the WAN connection goes down, the ZyWALL uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect.<br>Otherwise, you can select **My Domain Name** and choose one of the dynamic domain names that you have configured (in the **DDNS** screen) to have the ZyWALL use that dynamic domain name's IP address.<br>When the ZyWALL is in bridge mode, this field is read-only and displays the ZyWALL's IP address.<br>The VPN tunnel has to be rebuilt if the **My ZyWALL** IP address changes after setup. |
| Primary Remote Gateway | Type the WAN IP address or the domain name (up to 31 characters) of the IPSec router with which you're making the VPN connection. Set this field to **0.0.0.0** if the remote IPSec router has a dynamic WAN IP address.<br>In order to have more than one active rule with the **Primary Remote Gateway** field set to **0.0.0.0**, the ranges of the local IP addresses cannot overlap between rules.<br>If you configure an active rule with **0.0.0.0** in the **Primary Remote Gateway** field and the LAN's full IP address range as the local IP address, then you cannot configure any other active rules with the **Primary Remote Gateway** field set to **0.0.0.0**. |
| Enable IPSec High Availability | Turn on the high availability feature to use a redundant (backup) VPN connection to another WAN interface on the remote IPSec router if the primary (regular) VPN connection goes down. The remote IPSec router must have a second WAN connection in order for you to use this.<br>To use this, you must identify both the primary and the redundant remote IPSec routers by WAN IP address or domain name (you cannot set either to **0.0.0.0**). |
| Redundant Remote Gateway | Type the WAN IP address or the domain name (up to 31 characters) of the backup IPSec router to use when the ZyWALL cannot connect to the primary remote gateway. |

**Table 101** SECURITY > VPN > VPN Rules (IKE) > Edit Gateway Policy (continued)

| LABEL | DESCRIPTION |
|---|---|
| Fall back to Primary Remote Gateway when possible | Select this to have the ZyWALL change back to using the primary remote gateway if the connection becomes available again. |
| Fall Back Check Interval* | Set how often the ZyWALL should check the connection to the primary remote gateway while connected to the redundant remote gateway.<br>Each gateway policy uses one or more network policies. If the fall back check interval is shorter than a network policy's SA life time, the fall back check interval is used as the check interval and network policy SA life time. If the fall back check interval is longer than a network policy's SA life time, the SA lifetime is used as the check interval and network policy SA life time. |
| Authentication Key | |
| Pre-Shared Key | Select the **Pre-Shared Key** radio button and 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 from 16 to 62 hexadecimal ("0-9", "A-F") characters. You must precede a hexadecimal key with a "0x (zero x), which is not counted as part of the 16 to 62 character range for the key. For example, in "0x0123456789ABCDEF", 0x denotes that the key is hexadecimal and 0123456789ABCDEF is the key itself.<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. |
| Certificate | Select the **Certificate** radio button to identify the ZyWALL by a certificate.<br>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 **My Certificates** to go to the **My Certificates** screen where you can view the ZyWALL's list of certificates. |
| Local ID Type | Select **IP** to identify this ZyWALL by its IP address.<br>Select **DNS** to identify this ZyWALL by a domain name.<br>Select **E-mail** to identify this ZyWALL by an e-mail address.<br>You do not configure the local ID type and content when you set **Authentication Key** to **Certificate**. The ZyWALL takes them from the certificate you select. |
| Content | When you select **IP** in the **Local ID Type** field, type the IP address of your computer in the local **Content** field. The ZyWALL automatically uses the IP address in the **My ZyWALL** field (refer to the **My** ZyWALL field description) if you configure the local **Content** field to **0.0.0.0** or leave it blank.<br>It is recommended that you type an IP address other than **0.0.0.0** in the local **Content** field or use the **DNS** or **E-mail** ID type in the following situations.<br>1. When there is a NAT router between the two IPSec routers.<br>2. When you want the remote IPSec router to be able to distinguish between VPN connection requests that come in from IPSec routers with dynamic WAN IP addresses.<br>When you select **DNS** or **E-mail** in the **Local ID Type** field, type a domain name or e-mail address by which to identify this ZyWALL in the local **Content** field. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string. |

**Table 101** SECURITY > VPN > VPN Rules (IKE) > Edit Gateway Policy (continued)

| LABEL | DESCRIPTION |
|---|---|
| Peer ID Type | Select from the following when you set **Authentication Key** to **Pre-shared Key**.<br>Select **IP** to identify the remote IPSec router by its IP address.<br>Select **DNS** to identify the remote IPSec router by a domain name.<br>Select **E-mail** to identify the remote IPSec router by an e-mail address.<br>Select from the following when you set **Authentication Key** to **Certificate**.<br>Select **IP** to identify the remote IPSec router by the IP address in the subject alternative name field of the certificate it uses for this VPN connection.<br>Select **DNS** to identify the remote IPSec router by the domain name in the subject alternative name field of the certificate it uses for this VPN connection.<br>Select **E-mail** to identify the remote IPSec router by the e-mail address in the subject alternative name field of the certificate it uses for this VPN connection.<br>Select **Subject Name** to identify the remote IPSec router by the subject name of the certificate it uses for this VPN connection.<br>Select **Any** to have the ZyWALL not check the remote IPSec router's ID. |
| Content | The configuration of the peer content depends on the peer ID type.<br>Do the following when you set **Authentication Key** to **Pre-shared Key**.<br>For **IP**, type the IP address of the computer with which you will make the VPN connection. If you configure this field to **0.0.0.0** or leave it blank, the ZyWALL will use the address in the **Primary Remote Gateway** field (refer to the **Primary Remote Gateway** field description).<br>For **DNS** or **E-mail**, type a domain name or e-mail address by which to identify the remote IPSec router. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string.<br>It is recommended that you type an IP address other than **0.0.0.0** or use the **DNS** or **E-mail** ID type in the following situations:<br>1. When there is a NAT router between the two IPSec routers.<br>2. When you want the ZyWALL to distinguish between VPN connection requests that come in from remote IPSec routers with dynamic WAN IP addresses.<br>Do the following when you set **Authentication Key** to **Certificate**.<br>1. For **IP**, type the IP address from the subject alternative name field of the certificate the remote IPSec router will use for this VPN connection. If you configure this field to **0.0.0.0** or leave it blank, the ZyWALL will use the address in the **Primary Remote Gateway** field (refer to the **Primary Remote Gateway** field description).<br>2. For **DNS** or **E-mail**, type the domain name or e-mail address from the subject alternative name field of the certificate the remote IPSec router will use for this VPN connection.<br>3. For **Subject Name**, type the subject name of the certificate the remote IPSec router will use for this VPN connection. Use up to255 ASCII characters including spaces.<br>4. For **Any**, the peer **Content** field is not available.<br>5. Regardless of how you configure the **ID Type** and **Content** fields, two active IPSec SAs cannot have both the local and remote IP address ranges overlap between rules. |
| Extended Authentication | |
| Enable Extended Authentication | Select this check box to activate extended authentication. |

**Table 101** SECURITY > VPN > VPN Rules (IKE) > Edit Gateway Policy (continued)

| LABEL | DESCRIPTION |
|---|---|
| Server Mode | Select **Server Mode** to have this ZyWALL authenticate extended authentication clients that request this VPN connection.<br>You must also configure the extended authentication clients' usernames and passwords in the authentication server's local user database or a RADIUS server (see Chapter 21 on page 427).<br>Click **Local User** to go to the **Local User Database** screen where you can view and/or edit the list of user names and passwords. Click **RADIUS** to go to the **RADIUS** screen where you can configure the ZyWALL to check an external RADIUS server.<br>During authentication, if the ZyWALL (in server mode) does not find the extended authentication clients' user name in its internal user database and an external RADIUS server has been enabled, it attempts to authenticate the client through the RADIUS server. |
| Client Mode | Select **Client Mode** to have your ZyWALL use a username and password when initiating this VPN connection to the extended authentication server ZyWALL. Only a VPN extended authentication client can initiate this VPN connection. |
| User Name | Enter a user name for your ZyWALL to be authenticated by the VPN peer (in server mode). The user name can be up to 31 case-sensitive ASCII characters, but spaces are not allowed. You must enter a user name and password when you select client mode. |
| Password | Enter the corresponding password for the above user name. The password can be up to 31 case-sensitive ASCII characters, but spaces are not allowed. |
| IKE Proposal | |
| Negotiation Mode | Select **Main** or **Aggressive** from the drop-down list box. Multiple SAs connecting through a secure gateway must have the same negotiation mode. |
| Encryption Algorithm | 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>AES - a 128/192/256-bit key with the AES encryption algorithm<br>The ZyWALL and the remote IPSec router must use the same algorithms and keys. 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 IKE SA. Choices are **SHA1** and **MD5**. **SHA1** is generally considered stronger than **MD5**, but it is also slower. |
| SA Life Time (Seconds) | Define the length of time before an IKE SA automatically renegotiates in this field. It may range from 180 to 3,000,000 seconds (almost 35 days).<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. |
| 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. |

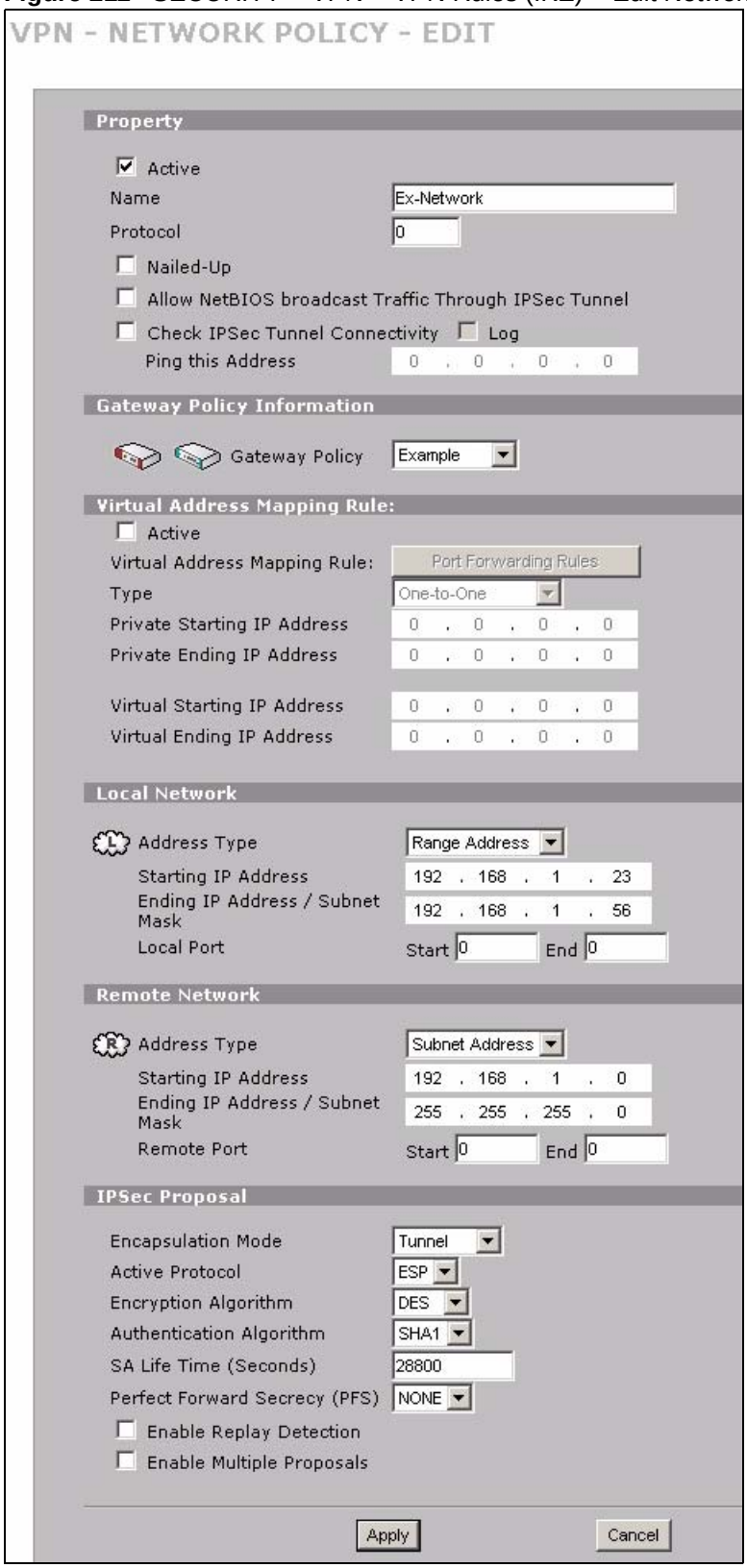
**Table 101** SECURITY > VPN > VPN Rules (IKE) > Edit Gateway Policy (continued)

| LABEL | DESCRIPTION |
|---|---|
| Enable Multiple Proposals | Select this to allow the ZyWALL to use any of its phase 1 key groups and encryption and authentication algorithms when negotiating an IKE SA.<br>When you enable multiple proposals, the ZyWALL allows the remote IPSec router to select which phase 1 key groups and encryption and authentication algorithms to use for the IKE SA, even if they are less secure than the ones you configure for the VPN rule.<br>Clear this to have the ZyWALL use only the configured phase 1 key groups and encryption and authentication algorithms when negotiating an IKE SA. |
| Associated Network Policies | The following table shows the policy(ies) you configure for this rule.<br>To add a VPN policy, click the add network policy ( ) icon in the **VPN Rules (IKE)** screen (see Figure 209 on page 360). Refer to Section 19.4 on page 367 for more information. |
| # | This field displays the policy index number. |
| Name | This field displays the policy name. |
| Local Network | This field displays one or a range of IP address(es) of the computer(s) behind the ZyWALL. |
| Remote Network | This field displays one or a range of IP address(es) of the remote network behind the remote IPsec router. |
| Edit | Click this icon to open the screen where you can configure the network policy. |
| Delete | Click this icon to remove the network policy. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving. |

## 19.4 The Network Policy Edit Screen

Click **SECURITY** > **VPN** and the add network policy ( ) icon or a network policy's edit icon in the **VPN Rules (IKE)** screen to display the **VPN-Network Policy -Edit** screen. Use this screen to configure a network policy. A network policy identifies the devices behind the IPSec routers at either end of a VPN tunnel and specifies the authentication, encryption and other settings needed to negotiate a phase 2 IPSec SA.

**Figure 211** SECURITY > VPN > VPN Rules (IKE) > Edit Network Policy



The following table describes the labels in this screen.

**Table 102** SECURITY > VPN > VPN Rules (IKE) > Edit Network Policy

| LABEL | DESCRIPTION |
|---|---|
| Active | If the **Active** check box is selected, packets for the tunnel trigger the ZyWALL to build the tunnel.<br>Clear the **Active** check box to turn the network policy off. The ZyWALL does not apply the policy. Packets for the tunnel do not trigger the tunnel.<br>If you clear the **Active** check box while the tunnel is up (and click **Apply**), you turn off the network policy and the tunnel goes down. |
| Name | Type a name to identify this VPN network policy. You may use any character, including spaces, but the ZyWALL drops trailing spaces. |
| Protocol | Specify the number of an IP protocol type.<br>Enter 1 for ICMP, 6 for TCP, 17 for UDP, and so on. 0 is the default and signifies any protocol. |
| Nailed-Up | Select this check box to turn on the nailed up feature for this SA.<br>Turn on nailed up to have the ZyWALL automatically reinitiate the SA after the SA lifetime times out, even if there is no traffic. The ZyWALL also reinitiates the SA when it restarts.<br>The ZyWALL also rebuilds the tunnel if it was disconnected due to the output or input idle timer. |
| Allow NetBIOS Traffic Through IPSec Tunnel | This field is not available when the ZyWALL is in bridge mode.<br>NetBIOS (Network Basic Input/Output System) 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 VPN tunnels in order to allow local computers to find computers on the remote network and vice versa.<br>Select this check box to send NetBIOS packets through the VPN connection. |
| Check IPSec Tunnel Connectivity | Select the check box and configure an IP address in the **Ping this Address** field to have the ZyWALL periodically test the VPN tunnel to the remote IPSec router.<br>The ZyWALL pings the IP address every minute. The ZyWALL starts the IPSec connection idle timeout timer when it sends the ping packet. If there is no traffic from the remote IPSec router by the time the timeout period expires, the ZyWALL disconnects the VPN tunnel. |
| Log | Select this check box to set the ZyWALL to create logs when it cannot ping the remote device. |
| Ping this Address | If you select **Check IPSec Tunnel Connectivity**, enter the IP address of a computer at the remote IPSec network. The computer's IP address must be in this IP policy's remote range (see the **Remote Network** fields). |
| Gateway Policy Information | |
| Gateway Policy | Select the gateway policy with which to use the VPN policy or store it in the recycle bin (without an association to any gateway policy). |
| Virtual Address Mapping Rule | Virtual address mapping over VPN is available with the routing mode. |
| Active | Enable this feature to have the ZyWALL use virtual (translated) IP addresses for the local network for the VPN connection. You do not configure the **Local Network** fields when you enable virtual address mapping.<br>Virtual address mapping allows local and remote networks to have overlapping IP addresses. Virtual address mapping (NAT over IPSec) translates the source IP addresses of computers on your local network to other (virtual) IP addresses before sending the packets to the remote IPSec router. This translation hides the source IP addresses of computers in the local network. |

**Table 102** SECURITY > VPN > VPN Rules (IKE) > Edit Network Policy (continued)

| LABEL | DESCRIPTION |
|---|---|
| Port Forwarding Rules | If you are configuring a **Many-to-One** rule, click this button to go to a screen where you can configure port forwarding for your VPN tunnels. The VPN network policy port forwarding rules let the ZyWALL forward traffic coming in through the VPN tunnel to the appropriate IP address. |
| Type | Select **One-to-One** to translate a single (static) IP address on your LAN to a single virtual IP address.<br>Select **Many-to-One** to translate a range of (static) IP addresses on your LAN to a single virtual IP address. Many-to-one rules are for traffic going out from your LAN, through the VPN tunnel, to the remote network. Use port forwarding rules to allow incoming traffic from the remote network.<br>Select **Many One-to-One** to translate a range of (static) IP addresses on your LAN to a range of virtual IP addresses. |
| Private Starting IP Address | Specify the IP addresses of the devices behind the ZyWALL that can use the VPN tunnel.<br>When you select **One-to-One** in the **Type** field, enter the (static) IP address of a computer on the LAN behind your ZyWALL.<br>When you select **Many-to-One** or **Many One-to-One** in the **Type** field, enter the beginning (static) IP address in a range of computers on the LAN behind your ZyWALL. |
| Private Ending IP Address | When you select **Many-to-One** or **Many One-to-One** in the **Type** field, enter the ending (static) IP address in a range of computers on the LAN behind your ZyWALL. |
| Virtual Starting IP Address | Enter the (static) IP addresses that represent the translated private IP addresses. These must correspond to the remote IPSec router's configured remote IP addresses.<br>When you select **One-to-One** or **Many-to-One** in the **Type** field, enter an IP address as the translated IP address. Many-to-one rules are only for traffic going to the remote network. Use port forwarding rules to allow incoming traffic from the remote network.<br>When you select **Many One-to-One** in the **Type** field, enter the beginning IP address of a range of translated IP addresses. |
| Virtual Ending IP Address | When you select **Many One-to-One** in the **Type** field, enter the ending (static) IP address of a range of translated IP addresses.<br>The size of the private address range must be equal to the size of the translated virtual address range. |
| Local Network | Specify the IP addresses of the devices behind the ZyWALL that can use the VPN tunnel. The local IP addresses must correspond to the remote IPSec router's configured remote IP addresses.<br>Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time. |
| Address Type | Use the drop-down list box to choose **Single Address**, **Range Address**, or **Subnet Address**. Select **Single Address** for a single IP address. Select **Range Address** for a specific range of IP addresses. Select **Subnet Address** to specify IP addresses on a network by their subnet mask. |
| Starting IP Address | When the **Address Type** field is configured to **Single Address**, enter a (static) IP address on the LAN behind your ZyWALL. When the **Address Type** field is configured to **Range Address**, enter the beginning (static) IP address, in a range of computers on the LAN behind your ZyWALL. When the **Address Type** field is configured to **Subnet Address**, this is a (static) IP address on the LAN behind your ZyWALL. |

**Table 102** SECURITY > VPN > VPN Rules (IKE) > Edit Network Policy (continued)

| LABEL | DESCRIPTION |
|---|---|
| Ending IP Address/ Subnet Mask | When the **Address Type** field is configured to **Single Address**, this field is N/A. When the **Address Type** field is configured to **Range Address**, enter the end (static) IP address, in a range of computers on the LAN behind your ZyWALL. When the **Address Type** field is configured to **Subnet Address**, this is a subnet mask on the LAN behind your ZyWALL. |
| Local Port | 0 is the default and signifies any port. Type a port number from 0 to 65535 in the **Start** and **End** fields. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3. |
| Remote Network | Specify the IP addresses of the devices behind the remote IPSec router that can use the VPN tunnel. The remote IP addresses must correspond to the remote IPSec router's configured local IP addresses.<br>Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time. |
| Address Type | Use the drop-down list box to choose **Single Address**, **Range Address**, or **Subnet Address**. Select **Single Address** with a single IP address. Select **Range Address** for a specific range of IP addresses. Select **Subnet Address** to specify IP addresses on a network by their subnet mask. |
| Starting IP Address | When the **Address Type** field is configured to **Single Address**, enter a (static) IP address on the network behind the remote IPSec router. When the Addr Type field is configured to **Range Address**, enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Address Type** field is configured to **Subnet Address**, enter a (static) IP address on the network behind the remote IPSec router. |
| Ending IP Address/ Subnet Mask | When the **Address Type** field is configured to **Single Address**, this field is N/A. When the **Address Type** field is configured to **Range Address**, enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Address Type** field is configured to **Subnet Address**, enter a subnet mask on the network behind the remote IPSec router. |
| Remote Port | 0 is the default and signifies any port. Type a port number from 0 to 65535 in the **Start** and **End** fields. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3. |
| IPSec Proposal | |
| Encapsulation Mode | Select **Tunnel** mode or **Transport** mode. |
| Active Protocol | Select the security protocols used for an SA.<br>Both **AH** and **ESP** increase processing requirements and communications latency (delay). |
| Encryption Algorithm | Select which key size and encryption algorithm to use in this 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>AES - a 128/192/256-bit key with the AES encryption algorithm<br>The ZyWALL and the remote IPSec router must use the same algorithms and keys. 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. |

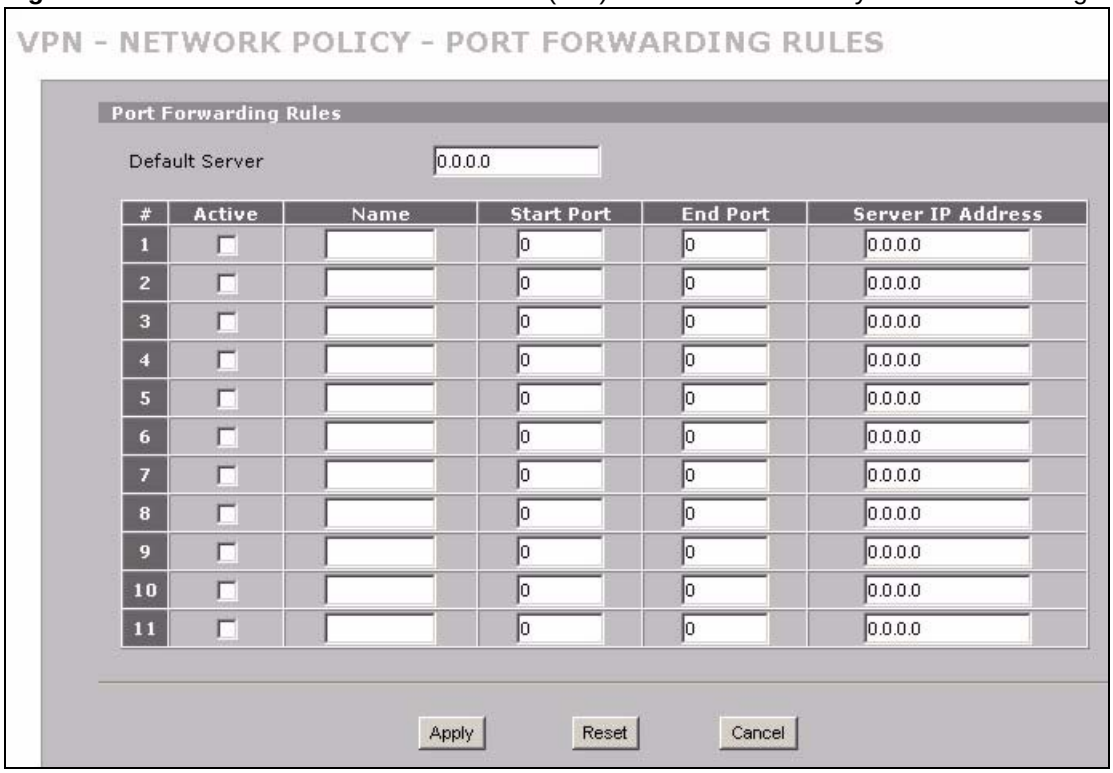
**Table 102** SECURITY > VPN > VPN Rules (IKE) > Edit Network Policy (continued)

| LABEL | DESCRIPTION |
|---|---|
| SA Life Time (Seconds) | Define the length of time before an IPSec SA automatically renegotiates in this field. The minimum value is 180 seconds.<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) | 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>**NONE** - disable PFS<br>**DH1** - enable PFS and use a 768-bit random number<br>**DH2** - enable PFS and use a 1024-bit random number<br>**DH5** - enable PFS and use a 1536-bit random number<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. |
| Enable Replay Detection | As a VPN setup is processing intensive, the system is vulnerable to Denial of Service (DOS) attacks. The IPSec receiver can detect and reject old or duplicate packets to protect against replay attacks. Enable replay detection by selecting this check box. |
| Enable Multiple Proposals | Select this to allow the ZyWALL to use any of its phase 2 encryption and authentication algorithms when negotiating an IPSec SA.<br>When you enable multiple proposals, the ZyWALL allows the remote IPSec router to select which phase 2 encryption and authentication algorithms to use for the IPSec SA, even if they are less secure than the ones you configure for the VPN rule.<br>Clear this to have the ZyWALL use only the configured phase 2 encryption and authentication algorithms when negotiating an IPSec SA. |
| Apply | Click **Apply** to save the changes. |
| Cancel | Click **Cancel** to discard all changes and return to the main VPN screen. |

## 19.5 The Network Policy Edit: Port Forwarding Screen

Click **SECURITY** > **VPN** and the add network policy ( ) icon in the **VPN Rules (IKE)** screen to display the **VPN-Network Policy -Edit** screen. Then, under **Virtual Address Mapping Rule**, select **Many-to-One** as the **Type** and click the **Port Forwarding Rules** button to open the following screen. Use this screen to configure port forwarding for your VPN tunnels to let the ZyWALL forward traffic coming in through the VPN tunnel to the appropriate IP address on the LAN.

**Figure 212** SECURITY > VPN > VPN Rules (IKE) > Edit Network Policy > Port Forwarding




The following table describes the labels in this screen.

**Table 103** SECURITY > VPN > VPN Rules (IKE) > Edit Network Policy > Port Forwarding

| LABEL | DESCRIPTION |
|---|---|
| Default Server | In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in this screen. If you do not assign a default server IP address, all packets received for ports not specified in this screen are discarded. |
| # | Number of an individual port forwarding server entry. |
| Active | Select this check box to activate the port forwarding server entry. |
| Name | Enter a descriptive name for identifying purposes. |
| Start Port | Type a port number in this field.<br>To forward only one port, type the port number again in the **End Port** field.<br>To forward a series of ports, type the start port number here and the end port number in the **End Port** field. |
| End Port | Type a port number in this field.<br>To forward only one port, type the port number in the **Start Port** field above and then type it again in this field.<br>To forward a series of ports, type the last port number in a series that begins with the port number in the **Start Port** field above. |
| Server IP Address | Type your server IP address in this field. |
| Apply | Click this button to save these settings. |
| Reset | Click this button to begin configuring this screen afresh. |
| Cancel | Click this button to return to the **VPN-Network Policy -Edit** screen without saving your changes. |

## 19.6 The Network Policy Move Screen

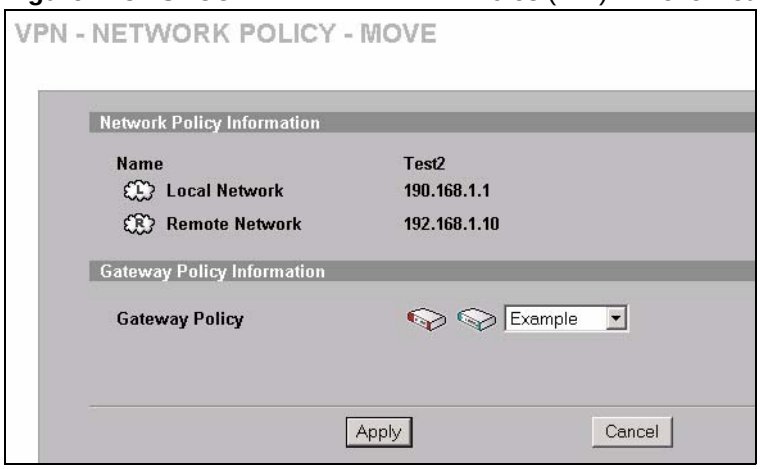
Click the move ( ) icon in the **VPN Rules (IKE)** screen to display the **VPN Rules (IKE): Network Policy Move** screen.

A VPN (Virtual Private Network) tunnel gives you a secure connection to another computer or network. Each VPN tunnel uses a single gateway policy and one or more network policies.

- The gateway policy contains the IKE SA settings. It identifies the IPSec routers at either end of a VPN tunnel.
- The network policy contains the IPSec SA settings. It specifies which devices (behind the IPSec routers) can use the VPN tunnel.

Use this screen to associate a network policy to a gateway policy.

**Figure 213** SECURITY > VPN > VPN Rules (IKE) > Move Network Policy




The following table describes the labels in this screen.

**Table 104** SECURITY > VPN > VPN Rules (IKE) > Move Network Policy

| LABEL | DESCRIPTION |
|---|---|
| Network Policy Information | The following fields display the general network settings of this VPN policy. |
| Name | This field displays the policy name. |
| Local Network | This field displays one or a range of IP address(es) of the computer(s) behind the ZyWALL. |
| Remote Network | This field displays one or a range of IP address(es) of the remote network behind the remote IPsec router. |
| Gateway Policy Information | |
| Gateway Policy | Select the name of a VPN rule (or gateway policy) to which you want to associate this VPN network policy.<br>If you do not want to associate a network policy to any gateway policy, select **Recycle Bin** from the drop-down list box. The **Recycle Bin** gateway policy is a virtual placeholder for any network policy(ies) without an associated gateway policy. When there is a network policy in **Recycle Bin**, the **Recycle Bin** gateway policy automatically displays in the **VPN Rules (IKE)** screen. |
| Apply | Click **Apply** to save the changes. |
| Cancel | Click **Cancel** to discard all changes and return to the main VPN screen. |

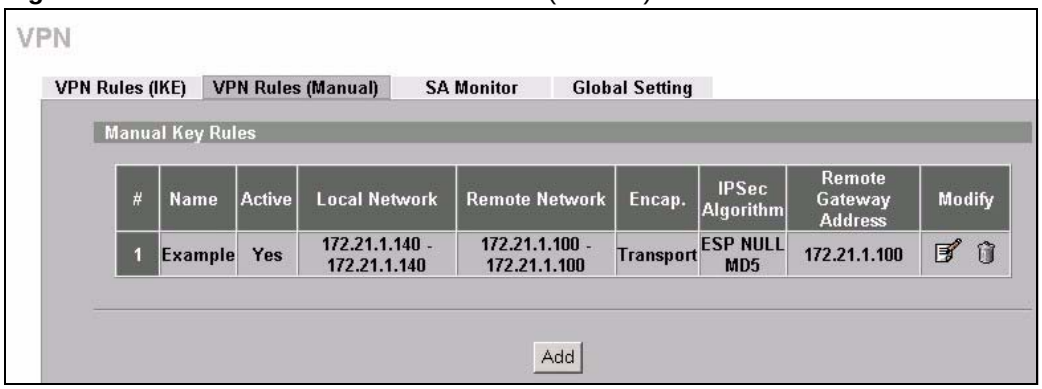
# 19.7 The VPN Rules (Manual) Screen

Refer to Figure 208 on page 359 for a graphical representation of the fields in the web configurator.

Click **SECURITY** > **VPN** > **VPN Rules (Manual)** to open the **VPN Rules (Manual)** screen.

Use this screen to manage the ZyWALL's list of VPN rules (tunnels) that use manual keys. You may want to configure a VPN rule that uses manual key management if you are having problems with IKE key management.

**Figure 214** SECURITY > VPN > VPN Rules (Manual)




The following table describes the labels in this screen.

**Table 105** SECURITY > VPN > VPN Rules (Manual)

| LABEL | DESCRIPTION |
|---|---|
| # | This is the VPN policy index number. |
| Name | This field displays the identification name for this VPN policy. |
| Active | This field displays whether the VPN policy is active or not. A **Yes** signifies that this VPN policy is active. **No** signifies that this VPN policy is not active. |
| Local Network | This is the IP address(es) of computer(s) on your local network behind your ZyWALL.<br>The same (static) IP address is displayed twice when the **Local Network Address Type** field in the **VPN - Manual Key - Edit** screen is configured to **Single Address**.<br>The beginning and ending (static) IP addresses, in a range of computers are displayed when the **Local Network Address Type** field in the **VPN - Manual Key - Edit** screen is configured to **Range Address**.<br>A (static) IP address and a subnet mask are displayed when the **Local Network Address Type** field in the **VPN - Manual Key - Edit** screen is configured to **Subnet Address**. |
| Remote Network | This is the IP address(es) of computer(s) on the remote network behind the remote IPSec router.<br>This field displays **N/A** when the **Remote Gateway Address** field displays **0.0.0.0**. In this case only the remote IPSec router can initiate the VPN.<br>The same (static) IP address is displayed twice when the **Remote Network Address Type** field in the **VPN - Manual Key - Edit** screen is configured to **Single Address**.<br>The beginning and ending (static) IP addresses, in a range of computers are displayed when the **Remote Network Address Type** field in the **VPN - Manual Key - Edit** screen is configured to **Range Address**.<br>A (static) IP address and a subnet mask are displayed when the **Remote Network Address Type** field in the **VPN - Manual Key - Edit** screen is configured to **Subnet Address**. |

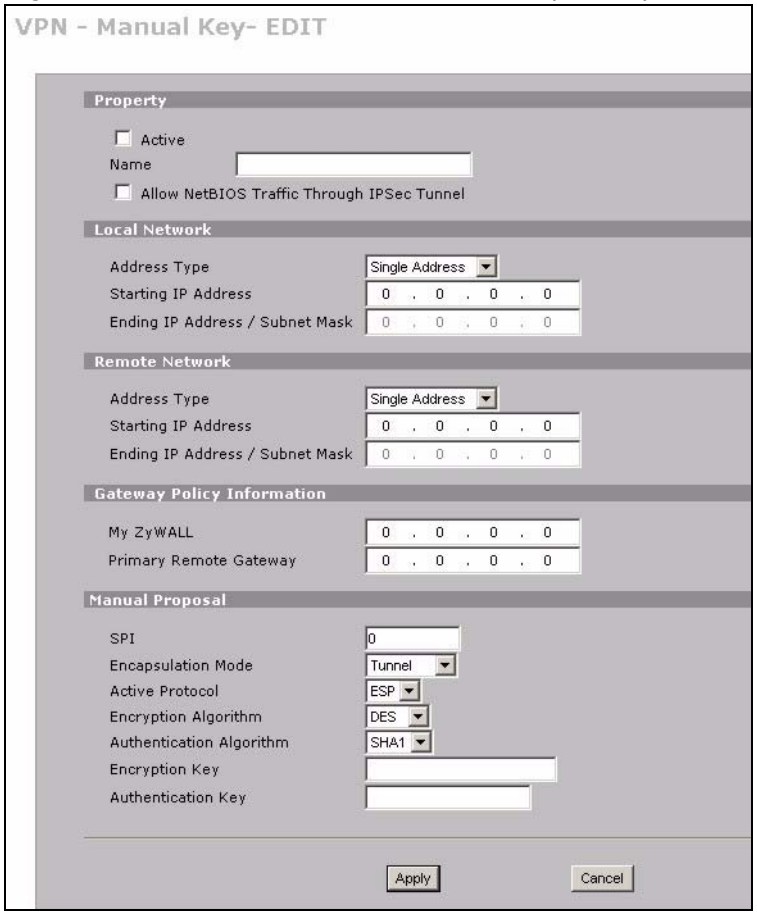
**Table 105** SECURITY > VPN > VPN Rules (Manual) (continued)

| LABEL | DESCRIPTION |
|---|---|
| Encap. | This field displays **Tunnel** or **Transport** mode (**Tunnel** is the default selection). |
| IPSec Algorithm | This field displays the security protocols used for an SA.<br>Both **AH** and **ESP** increase ZyWALL processing requirements and communications latency (delay). |
| Remote Gateway Address | This is the static WAN IP address of the remote IPSec router. |
| Modify | Click the edit icon to edit the VPN policy.<br>Click the delete icon to remove the VPN policy. A window displays asking you to confirm that you want to delete the VPN rule. When a VPN policy is deleted, subsequent policies move up in the page list. |
| Add | Click **Add** to add a new VPN policy. |

# 19.8 The VPN Rules (Manual): Edit Screen

Click the **Add** button or the edit icon on the **VPN Rules (Manual)** screen to open the following screen. Use this screen to configure VPN rules that use manual keys. Manual key management is useful if you have problems with IKE key management. See IPSec SA Using Manual Keys on page 395 for more information about IPSec SAs using manual keys.

**Figure 215** SECURITY > VPN > VPN Rules (Manual) > Edit



The following table describes the labels in this screen.

**Table 106** SECURITY > VPN > VPN Rules (Manual) > Edit

| LABEL | DESCRIPTION |
|---|---|
| Property | |
| Active | Select this check box to activate this VPN policy. |
| Name | Type up to 32 characters to identify this VPN policy. You may use any character, including spaces, but the ZyWALL drops trailing spaces. |
| Allow NetBIOS Traffic Through IPSec Tunnel | This field is not available when the ZyWALL is in bridge mode.<br>NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to find other computers. It may sometimes be necessary to allow NetBIOS packets to pass through VPN tunnels in order to allow local computers to find computers on the remote network and vice versa.<br>Select this check box to send NetBIOS packets through the VPN connection. |
| Local Network | Specify the IP addresses of the devices behind the ZyWALL that can use the VPN tunnel. The local IP addresses must correspond to the remote IPSec router's configured remote IP addresses.<br>Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time. |
| Address Type | Use the drop-down list box to choose **Single Address**, **Range Address**, or **Subnet Address**. Select **Single Address** for a single IP address. Select **Range Address** for a specific range of IP addresses. Select **Subnet Address** to specify IP addresses on a network by their subnet mask. |
| Starting IP Address | When the **Address Type** field is configured to **Single Address**, enter a (static) IP address on the LAN behind your ZyWALL. When the **Address Type** field is configured to **Range Address**, enter the beginning (static) IP address, in a range of computers on the LAN behind your ZyWALL. When the **Address Type** field is configured to **Subnet Address**, this is a (static) IP address on the LAN behind your ZyWALL. |
| Ending IP Address/Subnet Mask | When the **Address Type** field is configured to **Single Address**, this field is N/A. When the **Address Type** field is configured to **Range Address**, enter the end (static) IP address, in a range of computers on the LAN behind your ZyWALL. When the **Address Type** field is configured to **Subnet Address**, this is a subnet mask on the LAN behind your ZyWALL. |
| Remote Network | Specify the IP addresses of the devices behind the remote IPSec router that can use the VPN tunnel. The remote IP addresses must correspond to the remote IPSec router's configured local IP addresses.<br>Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time. |
| Address Type | Use the drop-down list box to choose **Single Address**, **Range Address**, or **Subnet Address**. Select **Single Address** with a single IP address. Select **Range Address** for a specific range of IP addresses. Select **Subnet Address** to specify IP addresses on a network by their subnet mask. |
| Starting IP Address | When the **Address Type** field is configured to **Single Address**, enter a (static) IP address on the network behind the remote IPSec router. When the Addr Type field is configured to **Range Address**, enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Address Type** field is configured to **Subnet Address**, enter a (static) IP address on the network behind the remote IPSec router. |

**Table 106** SECURITY > VPN > VPN Rules (Manual) > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Ending IP Address/Subnet Mask | When the **Address Type** field is configured to **Single Address**, this field is N/A. When the **Address Type** field is configured to **Range Address**, enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Address Type** field is configured to **Subnet Address**, enter a subnet mask on the network behind the remote IPSec router. |
| Gateway Policy Information | |
| My ZyWALL | When the ZyWALL is in router mode, enter the WAN IP address of your ZyWALL or leave the field set to **0.0.0.0**.<br>The ZyWALL uses its current WAN IP address (static or dynamic) in setting up the VPN tunnel if you leave this field as **0.0.0.0**. If the WAN connection goes down, the ZyWALL uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect.<br>The VPN tunnel has to be rebuilt if this IP address changes.<br>When the ZyWALL is in bridge mode, this field is read-only and displays the ZyWALL's IP address. |
| Primary Remote Gateway | Type the WAN IP address of the IPSec router with which you're making the VPN connection. |
| Manual Proposal | |
| SPI | Type a unique **SPI** (Security Parameter Index) from one to four characters long. Valid Characters are "0, 1, 2, 3, 4, 5, 6, 7, 8, and 9". |
| Encapsulation Mode | Select **Tunnel** mode or **Transport** mode from the drop-down list box. |
| Active Protocol | Select **ESP** if you want to use ESP (Encapsulation Security Payload). The ESP protocol (RFC 2406) provides encryption as well as some of the services offered by **AH**. If you select **ESP** here, you must select options from the **Encryption Algorithm** and **Authentication Algorithm** fields (described next).<br>Select **AH** if you want to use AH (Authentication Header Protocol). The AH protocol (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not for confidentiality, for which the ESP was designed. If you select **AH** here, you must select options from the **Authentication Algorithm** field (described next). |
| Encryption Algorithm | Select **DES**, **3DES** or **NULL** from the drop-down list box.<br>When **DES** is used for data communications, both sender and receiver must know the **Encryption 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. Select **NULL** to set up a tunnel without encryption. When you select **NULL**, you do not enter an encryption key. |
| Authentication Algorithm | Select **SHA1** or **MD5** from the drop-down list box. **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 **SHA-1** for maximum security. |
| Encryption Key | This field is applicable when you select **ESP** in the **Active Protocol** field above.<br>With **DES**, type a unique key 8 characters long. With **3DES**, type a unique key 24 characters long. Any characters may be used, including spaces, but trailing spaces are truncated. |
| Authentication Key | Type a unique authentication key to be used by IPSec if applicable. Enter 16 characters for **MD5** authentication or 20 characters for **SHA-1** authentication. Any characters may be used, including spaces, but trailing spaces are truncated. |

**Table 106** SECURITY > VPN > VPN Rules (Manual) > Edit (continued)

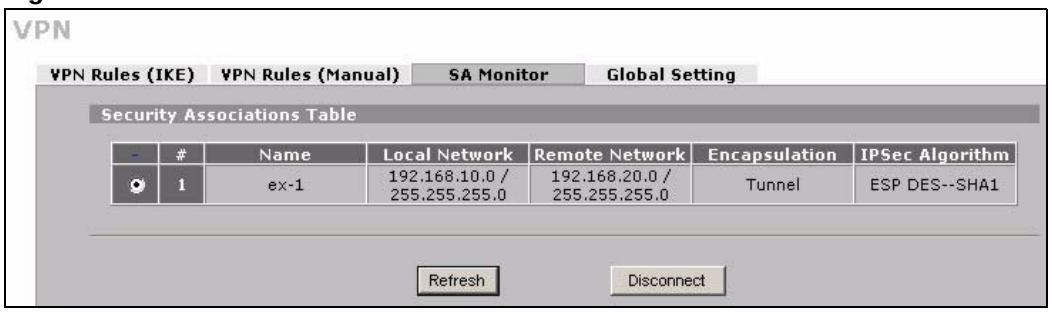
| LABEL | DESCRIPTION |
|---|---|
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving. |

## 19.9 The VPN SA Monitor Screen

In the web configurator, click **SECURITY** > **VPN** > **SA Monitor**. Use this screen to display and manage active VPN connections.

A Security Association (SA) is the group of security settings related to a specific VPN tunnel. This screen displays active VPN connections. Use **Refresh** to display active VPN connections.

**Figure 216** SECURITY > VPN > SA Monitor




The following table describes the labels in this screen.

**Table 107** SECURITY > VPN > SA Monitor

| LABEL | DESCRIPTION |
|---|---|
| # | This is the security association index number. |
| Name | This field displays the identification name for this VPN policy. |
| Local Network | This field displays the IP address of the computer using the VPN IPSec feature of your ZyWALL. |
| Remote Network | This field displays IP address (in a range) of computers on the remote network behind the remote IPSec router. |
| Encapsulation | This field displays **Tunnel** or **Transport** mode. |
| IPSec Algorithm | This field displays the security protocols used for an SA.<br>Both AH and ESP increase ZyWALL processing requirements and communications latency (delay). |
| Refresh | Click **Refresh** to display the current active VPN connection(s). |
| Disconnect | Select a security association index number that you want to disconnect and then click **Disconnect**. |

## 19.10 The VPN Global Setting Screen

Click **SECURITY** > **VPN** > **Global Setting** to open the **VPN Global Setting** screen. Use this screen to change settings that apply to all of your VPN tunnels.

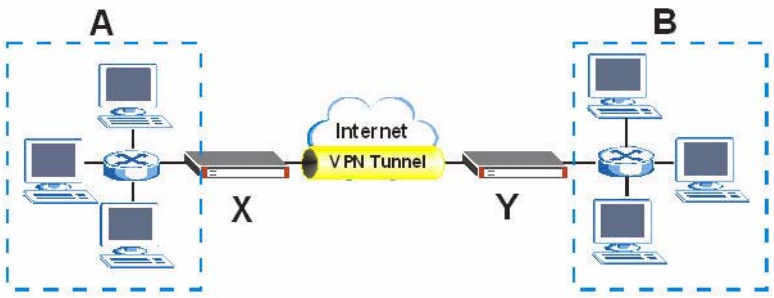
### Local and Remote IP Address Conflict Resolution

Normally, you do not configure your local VPN policy rule's IP addresses to overlap with the remote VPN policy rule's IP addresses. For example, you usually would not configure both with 192.168.1.0. However, overlapping local and remote network IP addresses can occur with dynamic VPN rules or IP alias.

### Dynamic VPN Rule

Local and remote network IP addresses can overlap when you configure a dynamic VPN rule for a remote site (see Figure 217). For example, when you configure ZyWALL X, you configure the local network as 192.168.1.0/24 and the remote network as any (0.0.0.0). The "any" includes all possible IP addresses. It will forward traffic from network A to network B even if both the sender (for example 192.168.1.8) and the receiver (for example 192.168.1.9) are in network A. Note that the remote access can still use the VPN tunnel to access computers on ZyWALL X's network.

**Figure 217** Overlap in a Dynamic VPN Rule



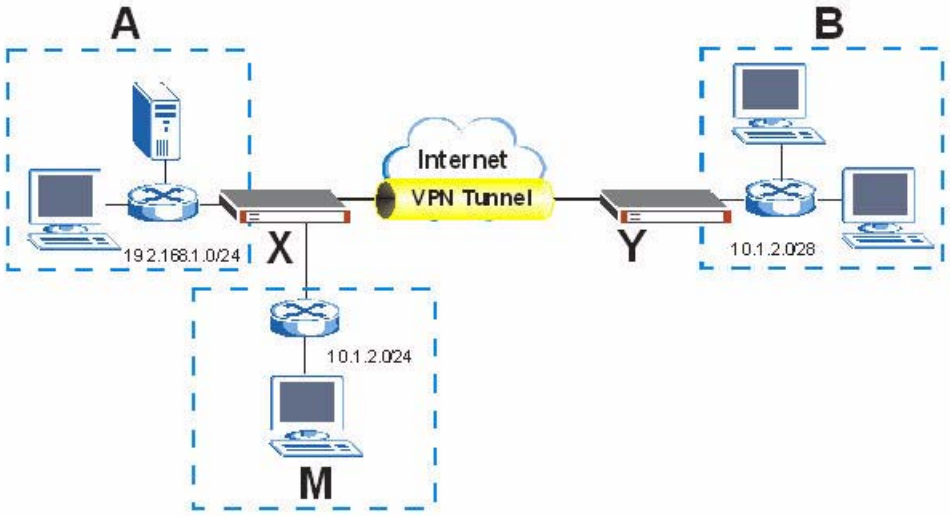

- Setting **Local and Remote IP Address Conflict Resolution** to **The Local Network** has the ZyWALL X check if a packet's destination is also at the local network before forwarding the packet. If it is, the ZyWALL sends the traffic to the local network.
- Setting **Local and Remote IP Address Conflict Resolution** to **The Remote Network** disables the checking for local network IP addresses.

### IP Alias

You could have an IP alias network that overlaps with the VPN remote network (see Figure 218). For example, you have an IP alias network M (10.1.2.0/24) in ZyWALL X's LAN. For the VPN rule, you configure the VPN network as follows.

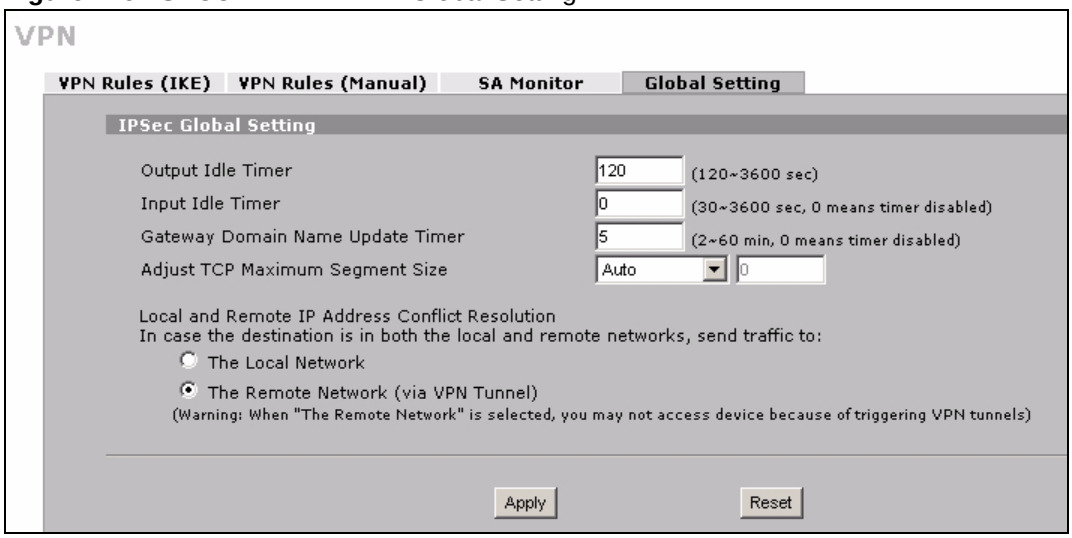
- Local IP address start: 192.168.1.1, end: 192.168.1.254
- Remote IP address start: 10.1.2.240, end: 10.1.2.254
- IP addresses 10.1.2.240 to 10.1.2.254 overlap.

**Figure 218** Overlap in IP Alias and VPN Remote Networks




In this case, if you want to send packets from network A to an overlapped IP (ex. 10.1.2.241) that is in the IP alias network M, you have to set **Local and Remote IP Address Conflict Resolution** to **The Local Network**.

**Figure 219** SECURITY > VPN > Global Setting




The following table describes the labels in this screen.

**Table 108** SECURITY > VPN > Global Setting

| LABEL | DESCRIPTION |
|---|---|
| Output Idle Timer | The ZyWALL disconnects a VPN tunnel if the remote IPSec router does not reply for this number of seconds. |
| Input Idle Timer | When no traffic is received from a remote IPSec router after the specified time period, the ZyWALL disconnects the VPN tunnel. **0** disables the check (this is the default setting).<br>The output idle timer never takes affect if you set this timer to a shorter period. |

**Table 108** SECURITY > VPN > Global Setting (continued)

| LABEL | DESCRIPTION |
|---|---|
| Gateway Domain Name Update Timer | If you use dynamic domain names in VPN rules to identify the ZyWALL and/or the remote IPSec router, the IP address mapped to the domain name can change. The VPN tunnel stops working after the IP address changes. Any users of the VPN tunnel are disconnected until the ZyWALL gets the new IP address from a DNS server and rebuilds the VPN tunnel.<br>Enter the time period (between 2 and 60 minutes) to set how often the ZyWALL queries a DNS server to update the IP address and domain name mapping.<br>If the query returns a new IP address for a dynamic domain name, the ZyWALL disconnects the VPN tunnel. The ZyWALL rebuilds the VPN tunnel (using the new IP address) immediately if the IPSec SA is set to nailed up. Otherwise the ZyWALL rebuilds the VPN tunnel when there are packets for it or you manually dial it.<br>If the ZyWALL and all of the remote IPSec routers use static IP addresses or regular domain names, you can enter **0** to disable this feature. |
| Adjust TCP Maximum Segment Size | The TCP packets are larger after the ZyWALL encrypts them for VPN. The ZyWALL fragments packets that are larger than a connection's MTU (Maximum Transmit Unit).<br>In most cases you should leave this set to **Auto**. The ZyWALL automatically sets the Maximum Segment Size (MSS) of the TCP packets that are to be encrypted by VPN based on the encapsulation type.<br>Select **Off** to not adjust the MSS for the encrypted TCP packets.<br>If your network environment causes fragmentation issues that are affecting your throughput performance, you can manually set a smaller MSS for the TCP packets that are to be encrypted by VPN. Select **User-Defined** and specify a size from 0~1460 bytes. 0 has the ZyWALL use the auto setting. |
| Local and Remote IP Address Conflict Resolution | Select **The Local Network** to send packets destined for overlapping local and remote IP addresses to the local network (you can access the local devices but not the remote devices).<br>Select **The Remote Network (via VPN Tunnel)** to send packets destined for overlapping local and remote IP addresses to the remote network (you can access the remote devices but not the local devices.)<br>If the remote IPSec router also supports NAT over IPSec, it is recommended that you use NAT over IPSec (see Section 19.14 on page 388) if the local and remote IP addresses overlap.<br>If a VPN rule's local and remote network settings are both set to 0.0.0.0 (any), no traffic goes through the VPN tunnel if you select **The Local Network**. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 19.11 Telecommuter VPN/IPSec Examples

The following examples show how multiple telecommuters can make VPN connections to a single ZyWALL at headquarters. The telecommuters use IPSec routers with dynamic WAN IP addresses. The ZyWALL at headquarters has a static public IP address.

## 19.11.1 Telecommuters Sharing One VPN Rule Example

See the following figure and table for an example configuration that allows multiple telecommuters (**A**, **B** and **C** in the figure) to use one VPN rule to simultaneously access a ZyWALL at headquarters (**HQ** in the figure). The telecommuters do not have domain names mapped to the WAN IP addresses of their IPSec routers. The telecommuters must all use the same IPSec parameters but the local IP addresses (or ranges of addresses) should not overlap.

**Figure 220** Telecommuters Sharing One VPN Rule Example

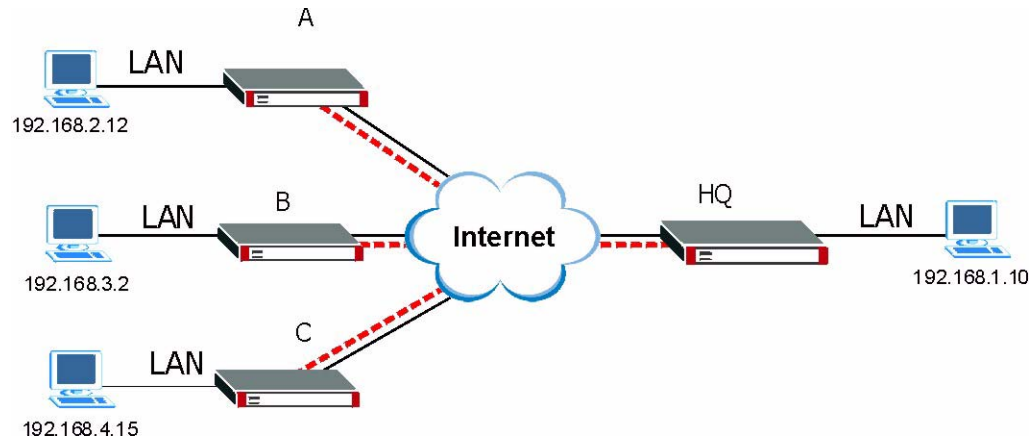



**Table 109** Telecommuters Sharing One VPN Rule Example

| FIELDS | TELECOMMUTERS | HEADQUARTERS |
|---|---|---|
| My ZyWALL: | 0.0.0.0 (dynamic IP address assigned by the ISP) | Public static IP address |
| Remote Gateway Address: | Public static IP address | 0.0.0.0 With this setting only the telecommuter can initiate the IPSec tunnel. |
| Local Network - Single IP Address: | Telecommuter A: 192.168.2.12<br>Telecommuter B: 192.168.3.2<br>Telecommuter C: 192.168.4.15 | 192.168.1.10 |
| Remote Network - Single IP Address: | 192.168.1.10 | Not Applicable |

## 19.11.2 Telecommuters Using Unique VPN Rules Example

In this example the telecommuters (A, B and C in the figure) use IPSec routers with domain names that are mapped to their dynamic WAN IP addresses (use Dynamic DNS to do this).

With aggressive negotiation mode (see Negotiation Mode on page 391), the ZyWALL can use the ID types and contents to distinguish between VPN rules. Telecommuters can each use a separate VPN rule to simultaneously access a ZyWALL at headquarters. They can use different IPSec parameters. The local IP addresses (or ranges of addresses) of the rules configured on the ZyWALL at headquarters can overlap. The local IP addresses of the rules configured on the telecommuters' IPSec routers should not overlap.

See the following table and figure for an example where three telecommuters each use a different VPN rule for a VPN connection with a ZyWALL located at headquarters. The ZyWALL at headquarters (HQ in the figure) identifies each incoming SA by its ID type and content and uses the appropriate VPN rule to establish the VPN connection.

The ZyWALL at headquarters can also initiate VPN connections to the telecommuters since it can find the telecommuters by resolving their domain names.

**Figure 221** Telecommuters Using Unique VPN Rules Example

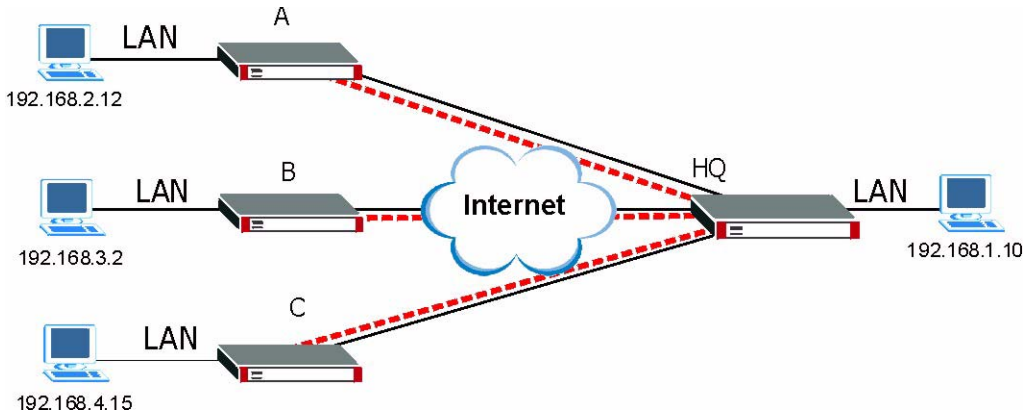



**Table 110** Telecommuters Using Unique VPN Rules Example

| TELECOMMUTERS | HEADQUARTERS |
|---|---|
| All Telecommuter Rules: | All Headquarters Rules: |
| My ZyWALL 0.0.0.0 | My ZyWALL: bigcompanyhq.com |
| Remote Gateway Address: bigcompanyhq.com | Local Network - Single IP Address: 192.168.1.10 |
| Remote Network - Single IP Address: 192.168.1.10 | Local ID Type: E-mail |
| Peer ID Type: E-mail | Local ID Content: bob@bigcompanyhq.com |
| Peer ID Content: bob@bigcompanyhq.com | |
| | |
| Telecommuter A (telecommutera.dydns.org) | Headquarters ZyWALL Rule 1: |
| Local ID Type: IP | Peer ID Type: IP |
| Local ID Content: 192.168.2.12 | Peer ID Content: 192.168.2.12 |
| Local IP Address: 192.168.2.12 | Remote Gateway Address: telecommutera.dydns.org |
| | Remote Address 192.168.2.12 |
| | |
| Telecommuter B (telecommuterb.dydns.org) | Headquarters ZyWALL Rule 2: |
| Local ID Type: DNS | Peer ID Type: DNS |
| Local ID Content: telecommuterb.com | Peer ID Content: telecommuterb.com |
| Local IP Address: 192.168.3.2 | Remote Gateway Address: telecommuterb.dydns.org |
| | Remote Address 192.168.3.2 |

**Table 110** Telecommuters Using Unique VPN Rules Example

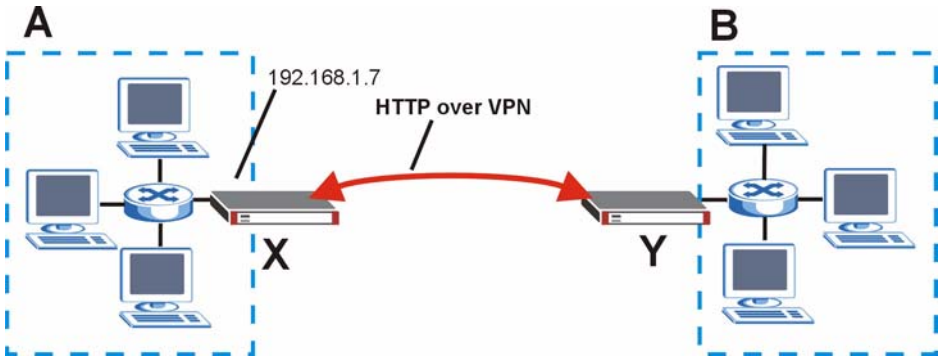
| TELECOMMUTERS | HEADQUARTERS |
|---|---|
| | |
| Telecommuter C (telecommuterc.dydns.org) | Headquarters ZyWALL Rule 3: |
| Local ID Type: E-mail | Peer ID Type: E-mail |
| Local ID Content: myVPN@myplace.com | Peer ID Content: myVPN@myplace.com |
| Local IP Address: 192.168.4.15 | Remote Gateway Address: telecommuterc.dydns.org |
| | Remote Address 192.168.4.15 |

## 19.12 VPN and Remote Management

You can allow someone to use a service (like Telnet or HTTP) through a VPN tunnel to manage the ZyWALL. One of the ZyWALL's ports must be part of the VPN rule's local network. This can be the ZyWALL's LAN port if you do not want to allow remote management on the WAN port. You also have to configure remote management (**REMOTE MGMT**) to allow management access for the service through the specific port.

In the following example, the VPN rule's local network (A) includes the ZyWALL's LAN IP address of 192.168.1.7. Someone in the remote network (B) can use a service (like HTTP for example) through the VPN tunnel to access the ZyWALL's LAN interface. Remote management must also be configured to allow HTTP access on the ZyWALL's LAN interface.

**Figure 222** VPN for Remote Management Example

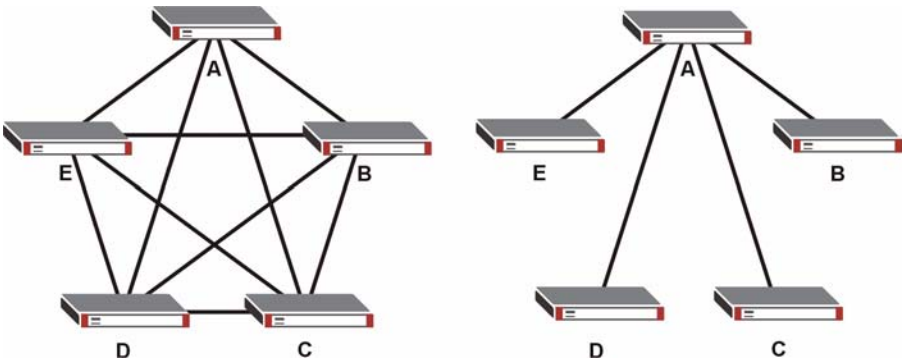



## 19.13 Hub-and-spoke VPN

Hub-and-spoke VPN connects VPN tunnels to form one secure network.

Figure 223 on page 386 shows some example network topologies. In the first (fully-meshed) approach, there is a VPN connection between every pair of routers. In the second (hub-and-spoke) approach, there is a VPN connection between each spoke router (**B**, **C**, **D**, and **E**) and the hub router (**A**). The hub router routes VPN traffic between the spoke routers and itself.

**Figure 223** VPN Topologies



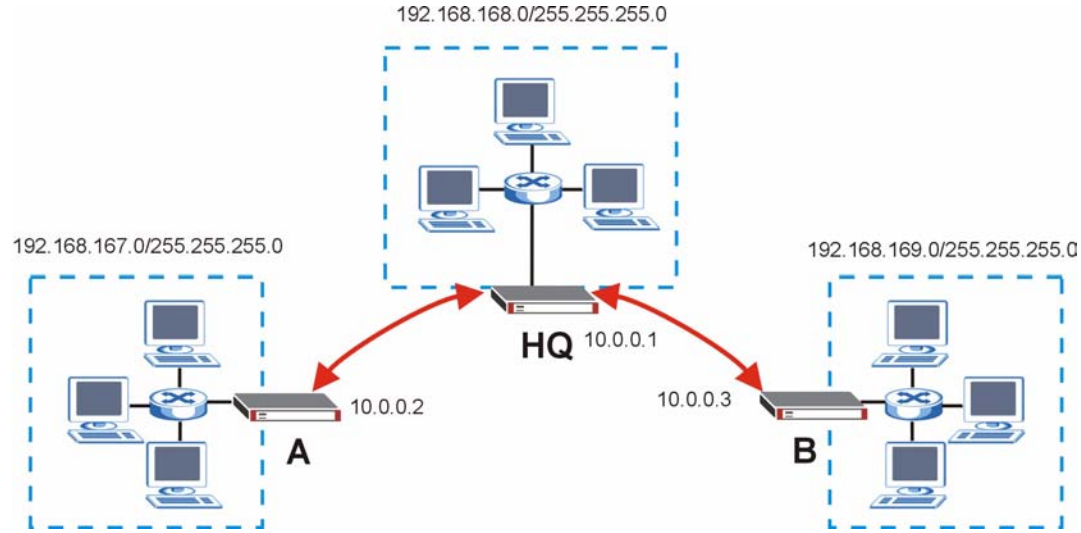

Hub-and-spoke VPN reduces the number of VPN connections that you have to set up and maintain in the network. Small office or telecommuter IPSec routers that support a limited number of VPN tunnels are also able to use VPN to connect to more networks. Hub-and-spoke VPN makes it easier for the hub router to manage the traffic between the spoke routers. If you have the spoke routers access the Internet through the hub-and-spoke VPN tunnel, the hub router can also provide content filtering, IDP, anti-spam and anti-virus protection for the spoke routers.

You should not use a hub-and-spoke VPN in every situation, however. The hub router is a single point of failure, so a hub-and-spoke VPN may not be appropriate if the connection between the spoke routers cannot be down occasionally (for maintenance, for example). In addition, there is a significant burden on the hub router. It receives VPN traffic from one spoke, decrypts it, inspects it to find out where to send it, encrypts it, and sends it to the appropriate spoke. Therefore, a hub-and-spoke VPN is more suitable when there is a minimum amount of traffic between spoke routers.

### 19.13.1 Hub-and-spoke VPN Example

The following figure shows a basic hub-and-spoke VPN. Branch office A uses one VPN rule to access both the headquarters (HQ) network and branch office B's network. Branch office B uses one VPN rule to access both the headquarters and branch office A's networks.

**Figure 224** Hub-and-spoke VPN Example




## 19.13.2 Hub-and-spoke Example VPN Rule Addresses

The VPN rules for this hub-and-spoke example would use the following address settings.

Branch Office A:

- Remote Gateway: 10.0.0.1
- Local IP address: 192.168.167.0/255.255.255.0
- Remote IP address: 192.168.168.0~192.168.169.255

Headquarters:

Rule 1:

- Remote Gateway: 10.0.0.2
- Local IP address: 192.168.168.0~192.168.169.255
- Remote IP address:192.168.167.0/255.255.255.0

Rule 2:

- Remote Gateway: 10.0.0.3
- Local IP address: 192.168.167.0~192.168.168.255
- Remote IP address: 192.168.169.0/255.255.255.0

Branch Office B:

- Remote Gateway: 10.0.0.1
- Local IP address: 192.168.169.0/255.255.255.0
- Remote IP address: 192.168.167.0~192.168.168.255

## 19.13.3 Hub-and-spoke VPN Requirements and Suggestions

Consider the following when implementing a hub-and-spoke VPN.

- The local IP addresses configured in the VPN rules cannot overlap

- The hub router must have at least one separate VPN rule for each spoke. In the local IP address, specify the IP addresses of the hub-and-spoke networks with which the spoke is to be able to have a VPN tunnel. This may require you to use more than one VPN rule.
- If you want to have the spoke routers access the Internet through the hub-and-spoke VPN tunnel, set the VPN rules in the spoke routers to use 0.0.0.0 (any) as the remote IP address.
- Make sure that your **From VPN** and **To VPN** firewall rules do not block the VPN packets.

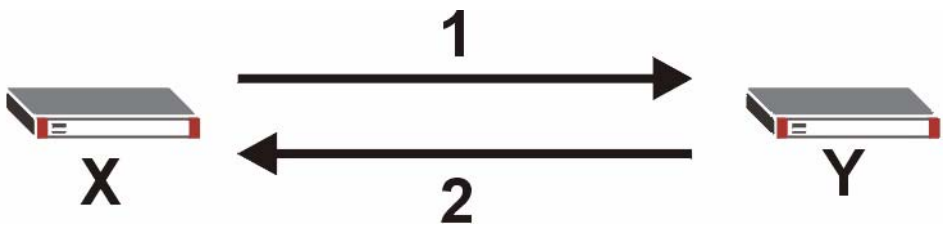
## 19.14 IPSec VPN Background Information

Here is some more detailed IPSec VPN background information.

## 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 below.

**Figure 225** 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 set up only 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 (for example, if the VPN tunnel is not configured correctly), the ZyWALL and remote IPSec router cannot establish an IKE SA.

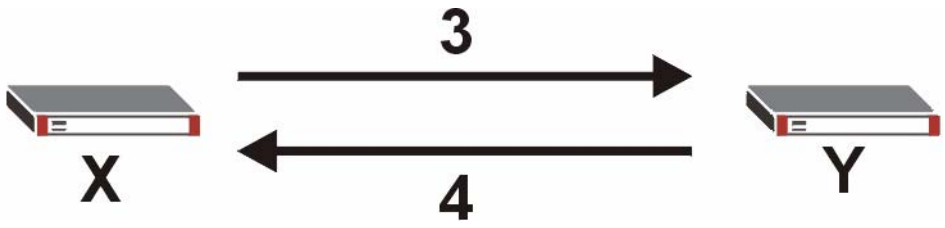
Both routers must use the same encryption algorithm, authentication algorithm, and DH key group.

See the field descriptions for information about specific encryption algorithms, authentication algorithms, and DH key groups. See Diffie-Hellman (DH) Key Exchange on page 389 for more information about DH key groups.

## Diffie-Hellman (DH) Key Exchange

The ZyWALL and the remote IPSec router use a DH key exchange to establish a shared secret, which is used to generate encryption keys for IKE SA and IPSec SA. In main mode, the DH key exchange is done in steps 3 and 4, as illustrated below.

**Figure 226** IKE SA: Main Negotiation Mode, Steps 3 - 4: DH Key Exchange



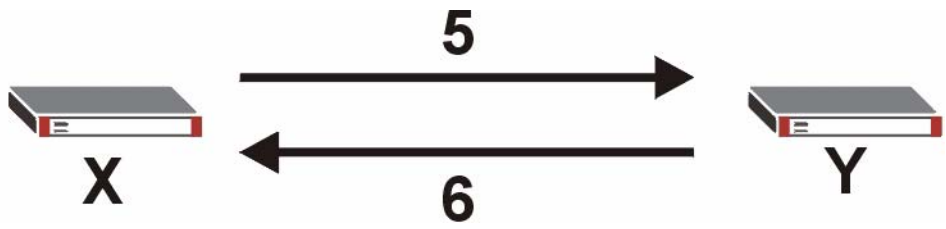

The DH key exchange is based on DH key groups. Each key group is a fixed number of bits long. The longer the key, the more secure the encryption keys, but also the longer it takes to encrypt and decrypt information. For example, DH2 keys (1024 bits) are more secure than DH1 keys (768 bits), but DH2 encryption 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. Their identities are encrypted using the encryption algorithm and encryption key the ZyWALL and remote IPSec router selected in previous steps.

**Figure 227** IKE SA: Main Negotiation Mode, Steps 5 - 6: Authentication




The ZyWALL and remote IPSec router use a pre-shared key in the authentication process, though it is not actually transmitted or exchanged.

The ZyWALL and the remote IPSec router must use the same pre-shared key.

Router identity consists of ID type and ID content. The ID type can be IP address, domain name, or e-mail address, and the ID content is a specific IP address, domain name, or e-mail address. The ID content is only used for identification; the IP address, domain name, or e-mail address that you enter does not have to actually exist.

The ZyWALL and the remote IPSec router each has its own identity, so each one must store two sets of information, one for itself and one for the other router. Local ID type and ID content refers to the ID type and ID content that applies to the router itself, and peer ID type and ID content refers to the ID type and ID content that applies to the other router in the IKE SA.

The ZyWALL's local and peer ID type and ID content must match the remote IPSec router's peer and local ID type and ID content, respectively.

In the following example, the ID type and content match so the ZyWALL and the remote IPSec router authenticate each other successfully.

**Table 111** 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 |

In the following example, the ID type and content do not match so the authentication fails and the ZyWALL and the remote IPSec router cannot establish an IKE SA.

**Table 112** 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: **1.1.1.15** | 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 not as secure as other peer ID types, however.

### Certificates

It is also possible for the ZyWALL and remote IPSec router to authenticate each other with certificates. In this case, the authentication process is different.

- Instead of using the pre-shared key, the ZyWALL and remote IPSec router check each other's certificates.
- The local ID type and ID content come from the certificate. On the ZyWALL, you simply select which certificate to use.
- If you set the peer ID type to **Any**, the ZyWALL authenticates the remote IPSec router using the trusted certificates and trusted CAs you have set up. Alternatively, if you want to use a specific certificate to authenticate the remote IPSec router, you can use the information in the certificate to specify the peer ID type and ID content.

You must set up the certificates for the ZyWALL and remote IPSec router before you can use certificates in IKE SA. See Chapter 20 on page 399 for more information about certificates.

## 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. Extended authentication occurs right after the authentication described in Authentication on page 389.

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.

## 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 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.

Step 1: The ZyWALL sends its proposals to the remote IPSec router. It also starts the Diffie-Hellman key exchange and sends its (unencrypted) identity to the remote IPSec router for authentication.

Step 2: The remote IPSec router selects an acceptable proposal and sends it back to the ZyWALL. It also finishes the Diffie-Hellman key exchange, authenticates the ZyWALL, and sends its (unencrypted) identity to the ZyWALL for authentication.

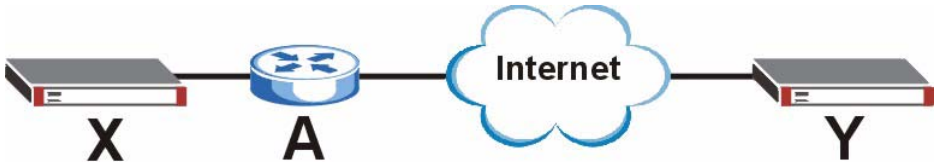
Step 3: The ZyWALL authenticates the remote IPSec router and confirms that the IKE SA is established.

Aggressive mode does not provide as much security as main mode because the identity of the ZyWALL and the identity of the remote IPSec router are not encrypted. It is usually used when the address of the initiator is not known by the responder and both parties want to use pre-shared keys for authentication (for example, telecommuters).

### VPN, NAT, and NAT Traversal

In the following example, there is another router (**A**) between router **X** and router **Y**.

**Figure 228** 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-through 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 394 for more information about active protocols.)

If router A does not have an IPSec pass-through 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.

## 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.

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 and Remote Networks

In an IPSec SA, the local network consists of devices connected to the ZyWALL and may be called the local policy. Similarly, the remote network consists of the devices connected to the remote IPSec router and may be called the remote policy.

You can configure a remote network as 0.0.0.0 (any) when:

- Forwarding all outgoing traffic to the remote gateway.
- The remote network's addresses are unknown or there are many remote networks using one VPN rule (see Section 19.11.1 on page 383 for an example of telecommuters sharing one VPN rule).

It is not recommended to set a VPN rule's local and remote network settings both to 0.0.0.0 (any).

In most cases you should use virtual address mapping (see Virtual Address Mapping on page 393) to avoid overlapping local and remote network IP addresses. See Section 19.10 on page 379 for how the ZyWALL handles overlapping local and remote network IP addresses.

## Virtual Address Mapping

Virtual address mapping (NAT over IPSec) changes the source IP addresses of packets from your local devices to virtual IP addresses before sending them through the VPN tunnel.

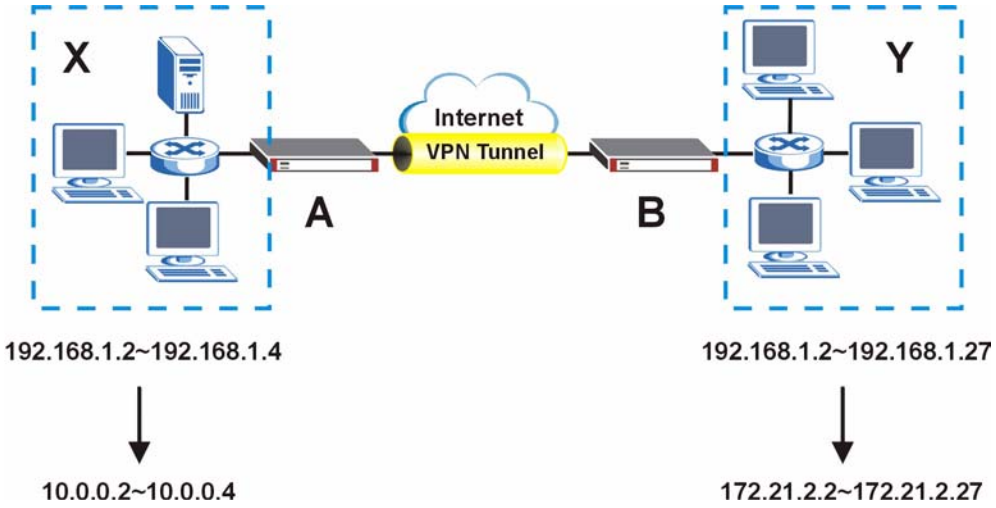
### Avoiding Overlapping Local And Remote Network IP Addresses

If both IPSec routers support virtual address mapping, you can access devices on both networks, even if their IP addresses overlap. You map the ZyWALL's local network addresses to virtual IP addresses and map the remote IPSec router's local IP addresses to other (non-overlapping) virtual IP addresses.

The following diagram shows an example of using virtual address mapping to avoid overlapping local and remote IP addresses. You can set up virtual address mapping on both IPSec routers to allow computers on network **X** to access network **X** and network **Y** computers with the same IP address.

- You set ZyWALL **A** to change the source IP addresses of packets from local network **X** (192.168.1.2 to 192.168.1.4) to virtual IP addresses 10.0.0.2 to 10.0.0.4 before sending them through the VPN tunnel.
- You set ZyWALL **B** to change the source IP addresses of packets from the remote network **Y** (192.168.1.2 to 192.168.1.27) to virtual IP addresses 172.21.2.2 to 172.21.2.27 before sending them through the VPN tunnel.
- On ZyWALL **A**, you specify 172.21.2.2 to 172.21.2.27 as the remote network. On ZyWALL **B**, you specify 10.0.0.2 to 10.0.0.4 as the remote network.

**Figure 229** Virtual Mapping of Local and Remote Network IP Addresses




Computers on network **X** use IP addresses 192.168.1.2 to 192.168.1.4 to access local network devices and IP addresses 172.21.2.2 to 172.21.2.27 to access the remote network devices.

Computers on network **Y** use IP addresses 192.168.1.2 to 192.168.1.27 to access local network devices and IP addresses 10.0.0.2 to 10.0.0.4 to access the remote network devices.

## 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).

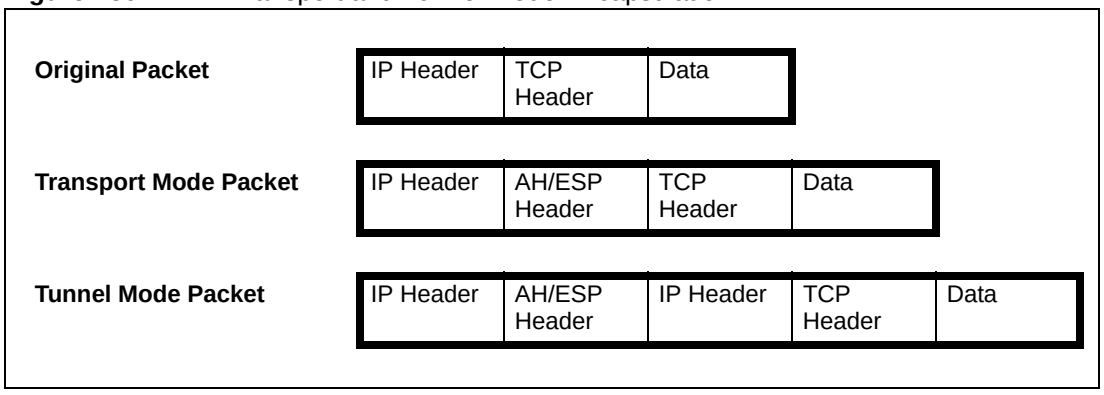
Usually, you should select ESP. AH does not support encryption, and ESP is more suitable with NAT.

## 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.

These modes are illustrated below.

**Figure 230** 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 388), 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.

## 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 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.

### 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.

# Additional IPSec VPN Topics

This section discusses other IPSec VPN topics that apply to either IKE SAs or IPSec SAs or both. Relationships between the topics are also highlighted.

## SA Life Time

SAs have a lifetime that specifies how long the SA lasts until it times out. When an SA times out, the ZyWALL automatically renegotiates the SA in the following situations:

- There is traffic when the SA life time expires
- The IPSec SA is configured on the ZyWALL as nailed up (see below)

Otherwise, the ZyWALL must re-negotiate the SA the next time someone wants to send traffic.

If the IKE SA times out while an IPSec SA is connected, the IPSec SA stays connected.

An IPSec SA can be set to **nailed up**. Normally, the ZyWALL drops the IPSec SA when the life time expires or after two minutes of outbound traffic with no inbound traffic. If you set the IPSec SA to nailed up, the ZyWALL automatically renegotiates the IPSec SA when the SA life time expires, and it does not drop the IPSec SA if there is no inbound traffic.

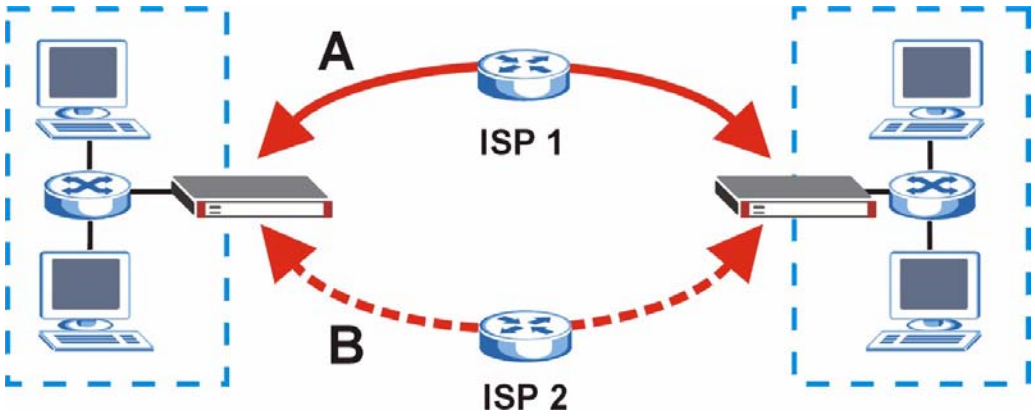
The SA life time and nailed up settings only apply if the rule identifies the remote IPSec router by a static IP address or a domain name. If the **Primary Remote Gateway** field is set to **0.0.0.0**, the ZyWALL cannot initiate the tunnel (and cannot renegotiate the SA).

## IPSec High Availability

IPSec high availability (also known as VPN high availability) allows you to use a redundant (backup) VPN connection to another WAN interface on the remote IPSec router if the primary (regular) VPN connection goes down.

In the following figure, if the primary VPN tunnel (A) goes down, the ZyWALL uses the redundant VPN tunnel (B).

**Figure 231** IPSec High Availability




When setting up an IPSec high availability VPN tunnel, the remote IPSec router:

- Must have multiple WAN connections
- Only needs one corresponding IPSec rule
- Should only have IPSec high availability settings in its corresponding IPSec rule if your ZyWALL has multiple WAN connections
- Should ideally identify itself by a domain name or dynamic domain name (it must otherwise have My Address set to 0.0.0.0)
- Should use a WAN connectivity check to this ZyWALL's WAN IP address

If the remote IPSec router is not a ZyWALL, you may also want to avoid setting the IPSec rule to nailed up.

## Encryption and Authentication Algorithms

In most ZyWALLs, you can select one of the following encryption algorithms for each proposal. The encryption algorithms are listed here in order from weakest to strongest.

- Data Encryption Standard (DES) is a widely used (but breakable) 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.

See the CLI Reference Guide for how to have the AES encryption apply 192-bit or 256-bit keys to 128-bit blocks of data.

You can select one of the following authentication algorithms for each proposal. The algorithms are listed here 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.

# 20

# Certificates

## 20.1 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.

### 20.1.1 What You Can Do in the Certificate Screens

- Use the **My Certificate** screens (see Section 20.2 on page 401) to generate and export self-signed certificates or certification requests and import the ZyWALL's CA-signed certificates.
- Use the **Trusted CA** screens (see Section 20.6 on page 413) to save the certificates of trusted CAs to the ZyWALL. You can also export the certificates to a computer.
- Use the **Trusted Remote Hosts** screens (see Section 20.9 on page 419) to import self-signed certificates from trusted remote hosts.
- Use the **Directory Servers** screen (see Section 20.12 on page 424) to configure a list of addresses of directory servers (that contain lists of valid and revoked certificates).

### 20.1.2 What You Need to Know About Certificates

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. You can use the ZyWALL to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

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. Public-key encryption in general works as follows.

1. Tim wants to send a private message to Jenny. Tim generates a public-private key pair. What is encrypted with one key can only be decrypted using the other.
2. Tim keeps the private key and makes the public key openly available.
3. Tim uses his private key to encrypt the message and sends it to Jenny.
4. Jenny receives the message and uses Tim's public key to decrypt it.
5. Additionally, Jenny uses her own private key to encrypt a message and Tim uses Jenny's public key to decrypt the message.

The ZyWALL uses certificates based on public-key cryptology to authenticate users attempting to establish 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.

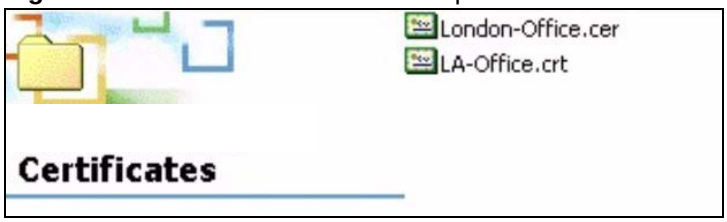
## 20.1.3 Verifying a Certificate

Before you import a trusted CA or trusted remote host certificate into the ZyWALL, you should verify that you have the actual certificate. This is especially true of trusted CA certificates since the ZyWALL also trusts any valid certificate signed by any of the imported trusted CA certificates.

You can use a certificate's fingerprint to verify it. A certificate's fingerprint is a message digest calculated using the MD5 or SHA1 algorithms. The following procedure describes how to check a certificate's fingerprint to verify that you have the actual certificate.

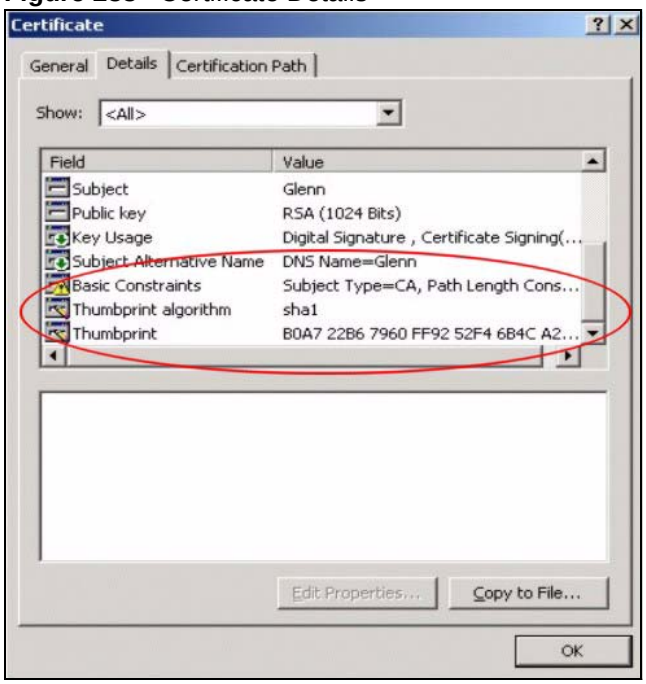
1. Browse to where you have the certificate saved on your computer.
2. Make sure that the certificate has a ".cer" or ".crt" file name extension.

**Figure 232** Certificates on Your Computer




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 233** 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.

## 20.2 The My Certificates Screen

Click **SECURITY > CERTIFICATES > My Certificates** to open the **My Certificates** screen. This is the ZyWALL's summary list of certificates and certification requests. Certificates display in black and certification requests display in gray.

**Figure 234** SECURITY > CERTIFICATES > My Certificates


The following table describes the labels in this screen.

**Table 113** SECURITY > CERTIFICATES > 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. |
| Replace | This button displays when the ZyWALL has the factory default certificate. The factory default certificate is common to all ZyWALLs that use certificates. ZyXEL recommends that you use this button to replace the factory default certificate with one that uses your ZyWALL's MAC address. |
| # | 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>**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>**SELF** represents a self-signed certificate.<br>***SELF** represents the default self-signed certificate, which the ZyWALL uses to sign imported trusted remote host certificates.<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. |

**Table 113** SECURITY > CERTIFICATES > My Certificates (continued)

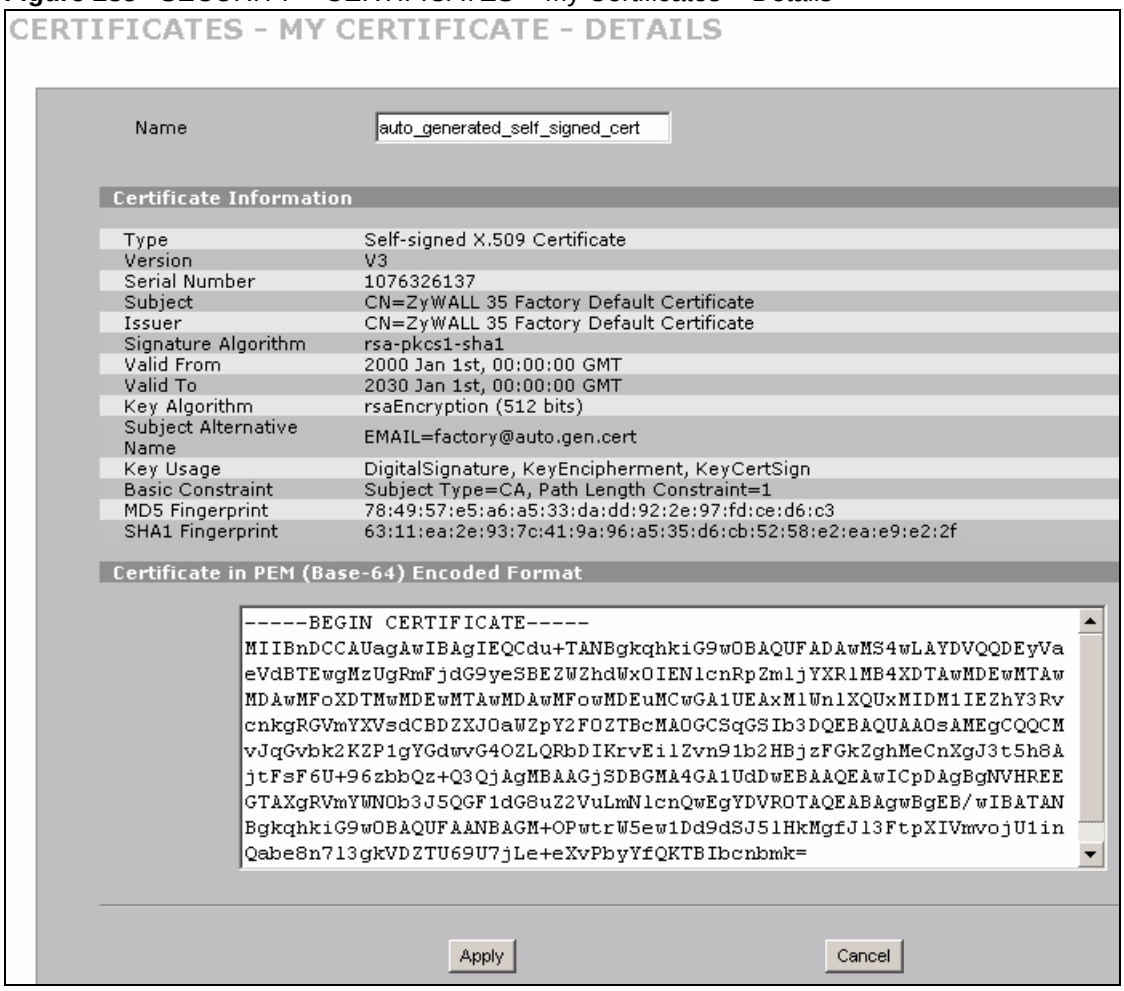
| LABEL | DESCRIPTION |
|---|---|
| Issuer | This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the **Subject** field. |
| Valid From | This field displays the date that the certificate becomes applicable. 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. |
| Modify | Click the details icon to open a screen with an in-depth list of information about the certificate (or certification request).<br>Click the export icon to save the certificate to a computer. For a certification request, click the export icon 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**.<br>Click the delete icon to remove the certificate (or certification request). A window displays asking you to confirm that you want to delete the certificate.<br>You cannot delete a certificate that one or more features is configured to use.<br>Do the following to delete a certificate that shows ***SELF** in the **Type** field.<br>1. Make sure that no other features, such as HTTPS, VPN, SSH are configured to use the ***SELF** certificate.<br>2. Click the details icon next to another self-signed certificate (see the description on the **Create** button if you need to create a self-signed certificate).<br>3. Select the **Default self-signed certificate which signs the imported remote host certificates** check box.<br>4. Click **Apply** to save the changes and return to the **My Certificates** screen.<br>5. The certificate that originally showed ***SELF** displays **SELF** and you can delete it now.<br>Note that subsequent certificates move up by one when you take this action.<br>The poll now icon displays when the ZyWALL generates a certification request successfully but the CA does not issue a certificate and sends a pending notification to the ZyWALL. If the icon displays, you can manually click the icon to have the ZyWALL query the CA (or RA (Registration Authority)) server for a certificate immediately. Otherwise, the ZyWALL checks with the server and updates the status periodically. The poll now icon disappears after the ZyWALL gets a certificate or the request has failed permanently due to being rejected by the CA server. |
| Import | Click **Import** to open a screen where you can save the certificate that you have enrolled from a certification authority from your computer to the ZyWALL. |
| Create | Click **Create** to go to the screen where you can have the ZyWALL generate a certificate or a certification request. |
| Refresh | Click **Refresh** to display the current validity status of the certificates. |

## 20.2.1 The My Certificate Details Screen

Click **SECURITY** > **CERTIFICATES** > **My Certificates** to open the **My Certificates** screen (see Figure 234 on page 402). Click the details icon to open the **My Certificate Details** screen. You can use this screen to view in-depth certificate information and change the certificate's name.

If it is a self-signed certificate, you can also set the ZyWALL to use the certificate to sign the imported trusted remote host certificates.

**Figure 235** SECURITY > CERTIFICATES > My Certificates > Details




The following table describes the labels in this screen.

**Table 114** SECURITY > CERTIFICATES > My Certificates > Details

| LABEL | DESCRIPTION |
|---|---|
| Name | This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this certificate. You may use any character (not including spaces). |
| 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). |

**Table 114** SECURITY > CERTIFICATES > My Certificates > Details (continued)

| LABEL | DESCRIPTION |
|---|---|
| Issuer | This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country.<br>With self-signed certificates, this is the same as the **Subject Name** field. |
| 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. 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 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. |
| 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 64 ASCII characters to convert the binary certificate into a printable form.<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>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). |
| Apply | Click **Apply** to save your changes back to the ZyWALL. You can only change the name, except in the case of a self-signed certificate, which you can also set to be the default self-signed certificate that signs the imported trusted remote host certificates. |
| Cancel | Click **Cancel** to quit and return to the **My Certificates** screen. |

## 20.3 The My Certificate Export Screen

Click **SECURITY** > **CERTIFICATES** > **My Certificates** and then a certificate's export icon to open the **My Certificate Export** screen. Follow the instructions in this screen to choose the file format to use for saving the certificate from the ZyWALL to a computer. You can export a certificate in one of these file formats:

- Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.
- 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.

**Figure 236** SECURITY > CERTIFICATES > My Certificates > Export


The following table describes the labels in this screen.

**Table 115** SECURITY > CERTIFICATES > My Certificates > Export

| LABEL | DESCRIPTION |
|---|---|
| Export the certificate in binary X.509 format. | Binary X.509 is an ITU-T recommendation that defines the formats for X.509 certificates. |
| Export the certificate along with the corresponding private key in PKCS#12 format. | PKCS#12 is a format for transferring public key and private key certificates. You can also password-encrypt the private key in the PKCS #12 file. The file's password is not connected to your certificate's public or private passwords. |
| Password | Type the file's password to use for encrypting the private key. The password is optional, although you must specify one if you want to be able to import the PKCS#12 format certificate into Netscape version 7.2. |
| Retype to confirm | Type the password to make sure that you have entered it correctly. |
| Apply | Click **Apply** 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**. |
| Cancel | Click **Cancel** to quit and return to the **My Certificates** screen. |

## 20.4 The My Certificate Import Screen

You can only import a certificate that matches a corresponding certification request that was generated by the ZyWALL (the certification request contains the private key). The certificate you import replaces the corresponding request in the **My Certificates** screen.

One exception is that you can import a PKCS#12 format certificate without a corresponding certification request since the certificate includes the private key.

Remove any spaces from the certificate's filename before you import it.

### Certificate File Formats

The certification authority 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 64 ASCII characters 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. 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 64 ASCII characters 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.

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.

### 20.4.1 Using the My Certificate Import Screen

Click **SECURITY > CERTIFICATES > My Certificates** and then **Import** to open the **My Certificate Import** screen. Follow the instructions in this screen to save an existing certificate from a computer to the ZyWALL.

**Figure 237** SECURITY > CERTIFICATES > My Certificates > Import


The following table describes the labels in this screen.

**Table 116** SECURITY > CERTIFICATES > 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. |
| Browse | Click **Browse** to find the certificate file you want to upload. |
| Apply | Click **Apply** to save the certificate on the ZyWALL. |
| Cancel | Click **Cancel** to quit and return to the **My Certificates** screen. |

When you import a binary PKCS#12 format certificate, another screen displays for you to enter the password.

**Figure 238** SECURITY > CERTIFICATES > My Certificates > Import: PKCS#12


The following table describes the labels in this screen.

**Table 117** SECURITY > CERTIFICATES > My Certificates > Import: PKCS#12

| LABEL | DESCRIPTION |
|---|---|
| Password | Type the file's password that was created when the PKCS #12 file was exported. |
| Apply | Click **Apply** to save the certificate on the ZyWALL. |
| Cancel | Click **Cancel** to quit and return to the **My Certificates** screen. |

## 20.5 The My Certificate Create Screen

Click **SECURITY** > **CERTIFICATES** > **My Certificates > Create** to open the **My Certificate Create** 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 239** SECURITY > CERTIFICATES > My Certificates > Create (Basic)

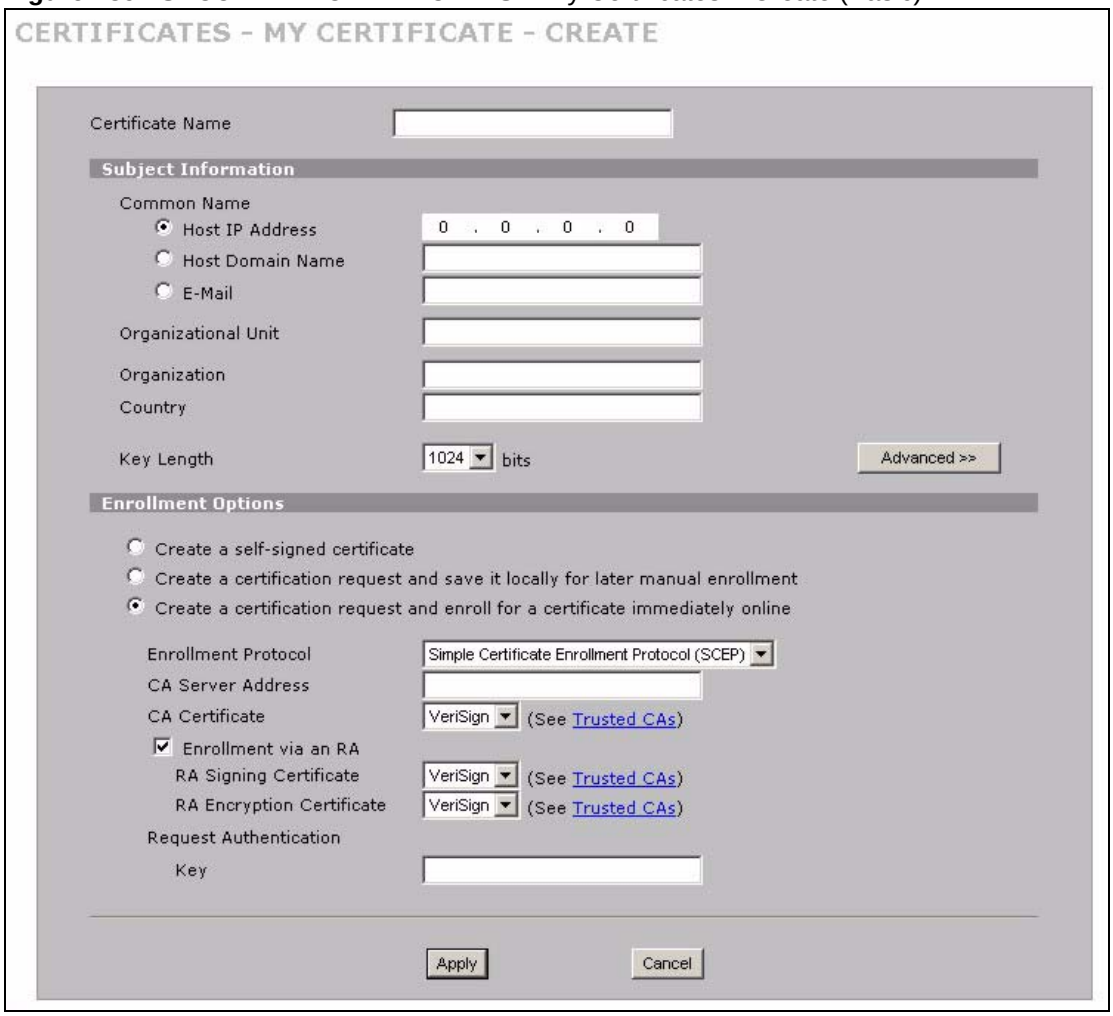
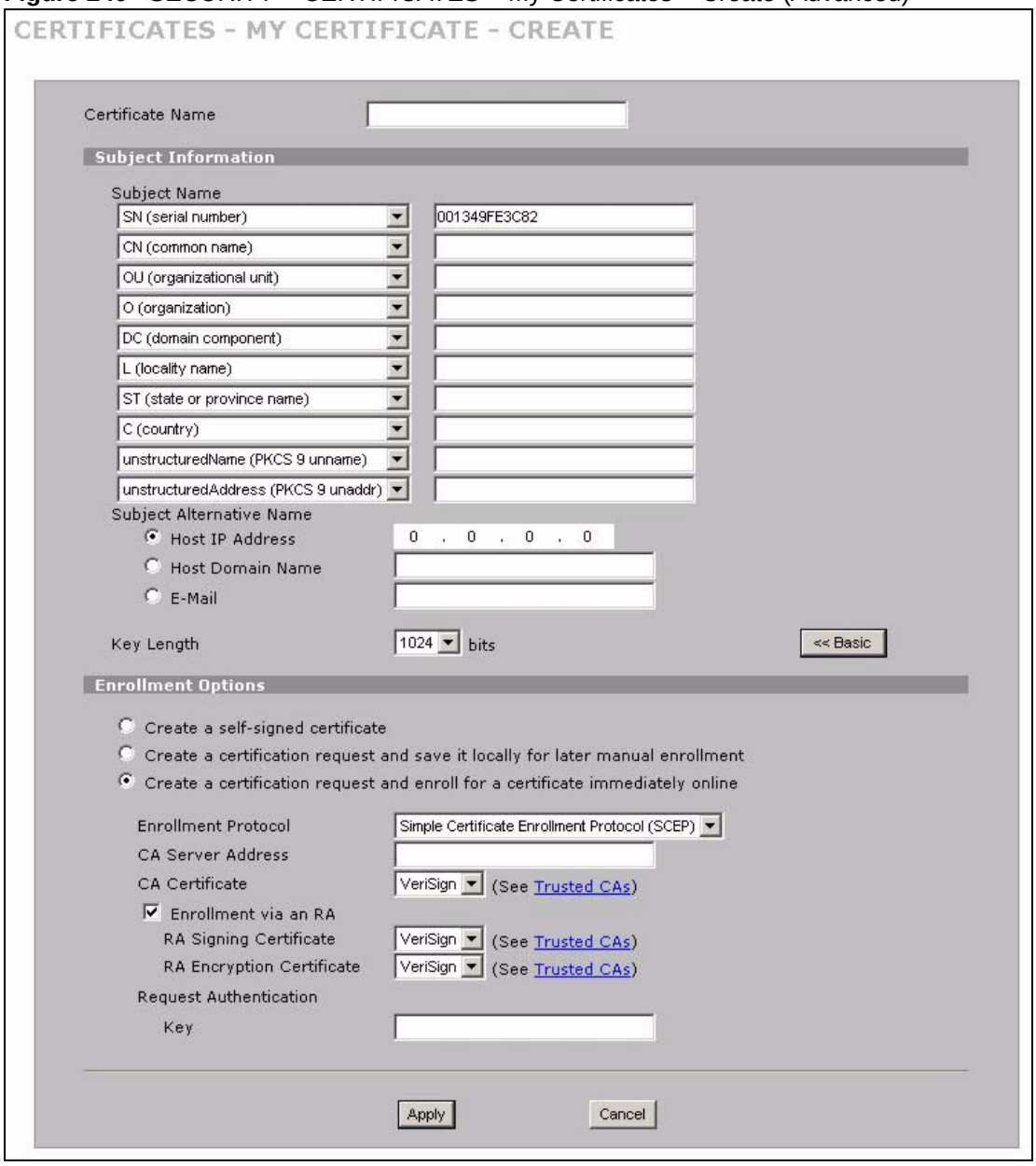


**Figure 240** SECURITY > CERTIFICATES > My Certificates > Create (Advanced)




The following table describes the labels in this screen.

**Table 118** SECURITY > CERTIFICATES > My Certificates > Create

| LABEL | DESCRIPTION |
|---|---|
| Certificate Name | Type up to 31 ASCII characters (not including spaces) to identify this certificate. |
| Subject Information | Use these fields to record information that identifies the owner of the certificate. You do not have to fill in every field, but the **Common Name** is mandatory if you click **<< Basic**. 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. |
| The fields below display when you click **<< Basic**. | |

**Table 118** SECURITY > CERTIFICATES > My Certificates > Create (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 can be up to 31 ASCII characters. The domain name or e-mail address is for identification purposes only and can be any string. |
| Organizational Unit | Type up to 63 characters to identify the organizational unit or department to which the certificate owner belongs. You may use any character, including spaces, but the ZyWALL drops trailing spaces. |
| Organization | Type up to 63 characters to identify the company or group to which the certificate owner belongs. You may use any character, including spaces, but the ZyWALL drops trailing spaces. |
| Country | Type up to 63 characters to identify the nation where the certificate owner is located. You may use any character, including spaces, but the ZyWALL drops trailing spaces. |
| The fields below display when you click **Advanced >>**. | |
| Subject Name | You must configure at least one of these fields.<br>Select an item from the drop-down list box and enter the corresponding information in the field to the right.<br>**SN (serial number)** - select this and enter the certificate's identification number, such as the ZyWALL's MAC address. You can use up to 63 characters.<br>**CN (common name)** - select this and enter a name to identify the owner of the certificate. You can use up to 63 characters.<br>**OU (organizational unit)** - select this and enter a unit within the organization to identify the owner of the certificate. You can use up to 63 characters.<br>**O (organization)** - select this and enter an organization to identify the owner of the certificate. You can use up to 63 characters.<br>**DC (domain component)** - select this and enter the domain component of a domain to identify the owner of the certificate. For example, if the domain is zyxel.com, the domain component is "zyxel" or "com". You can use up to 63 characters.<br>**L (locality name)** - select this and enter the place where the owner of the certificate resides, such as a city or county. You can use up to 63 characters.<br>**ST (state or province name)** - select this and enter the state or province in which the owner of the certificate resides. You can use up to 63 characters.<br>**C (country)** - select this and enter the name of the country at which the owner of the certificate resides. You can use up to 63 characters.<br>**unstructuredName (PKCS 9 unname)** - select this and enter the name of the owner of the certificate as an unstructured ASCII string. You can use up to 63 characters. Check with the certificate's issuing certification authority for their interpretation in this field if you select to apply to a certification authority for a certificate.<br>**unstructuredAddress (PKCS 9 unaddr)** - select this and enter the address of the owner of the certificate as an unstructured ASCII string. You can use up to 63 characters. Check with the certificate's issuing certification authority for their interpretation in this field if you select to apply to a certification authority for a certificate.<br>**MAILTO (PKCS 9 email address)** - select this and enter the email address of the owner of the certificate. You can use up to 63 characters. Check with the certificate's issuing certification authority for their interpretation in this field if you select to apply to a certification authority for a certificate. |

**Table 118** SECURITY > CERTIFICATES > My Certificates > Create (continued)

| LABEL | DESCRIPTION |
|---|---|
| Subject Alternative 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 can be up to 31 ASCII characters. The domain name or e-mail address is for identification purposes only and can be any string. |
| 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. |
| << Basic/Advanced >> | Click **<< Basic** to configure basic subject information. Click **Advanced >>** to configure more subject information for a certificate. |
| 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>Copy the certification request from the **My Certificate Details** screen (see Section 20.2.1 on page 403) and then send it to the certification authority. |
| 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>You must have the certification authority's certificate already imported in the **Trusted CAs** screen.<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 | Select the certification authority's enrollment protocol from the drop-down list box.<br>**Simple Certificate Enrollment Protocol (SCEP)** is a TCP-based enrollment protocol that was developed by VeriSign and Cisco.<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 | Enter the IP address (or URL) of the certification authority server. |
| CA Certificate | Select the certification authority's certificate from the **CA Certificate** drop-down list box.<br>You must have the certification authority's certificate already imported in the **Trusted CAs** screen. Click **Trusted CAs** to go to the **Trusted CAs** screen where you can view (and manage) the ZyWALL's list of certificates of trusted certification authorities. |
| Enrollment via an RA | If you select **Create a certification request and enroll for a certificate immediately online**, you can select this option to apply for a certificate through a RA (Registration Authority). The RA is an intermediary authorized by a CA to verify each subscriber's identity and forward the requests to the CA. After the CA signs and issues the certificates, the RA distributes the certificates to the subscribers. |

**Table 118** SECURITY > CERTIFICATES > My Certificates > Create (continued)

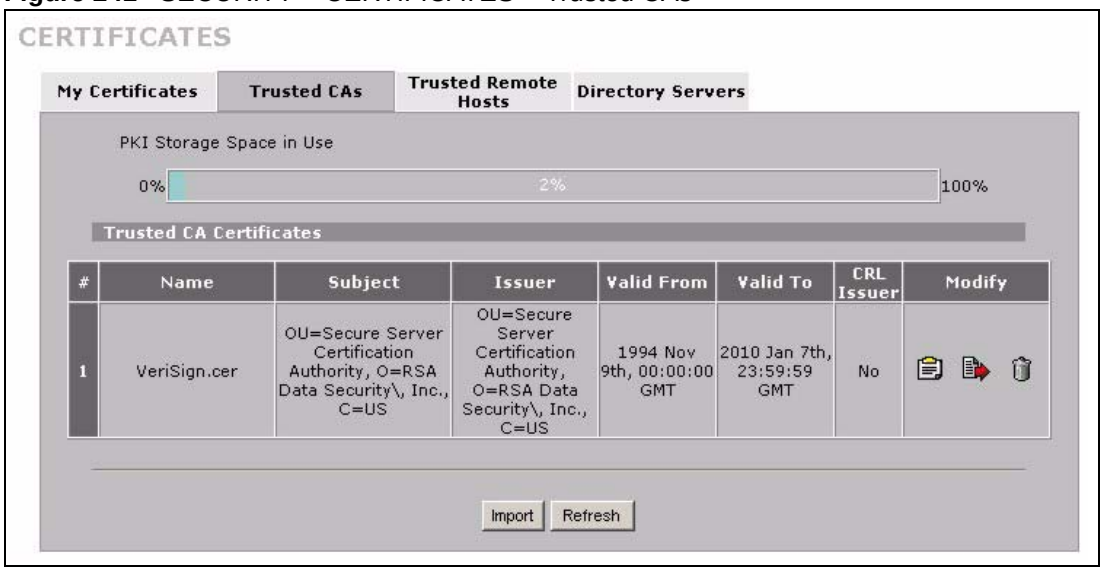
| LABEL | DESCRIPTION |
|---|---|
| RA Signing Certificate | If you select **Enrollment via an RA**, select the CA's RA signing certificate from the drop-down list box. You must have the certificate already imported in the **Trusted CAs** screen.<br>Click **Trusted CAs** to go to the **Trusted CAs** screen where you can view (and manage) the ZyWALL's list of certificates of trusted certification authorities. |
| RA Encryption Certificate | If you select **Enrollment via an RA**, select the CA's RA encryption certificate from the drop-down list box. You must have the certificate already imported in the **Trusted CAs** screen.<br>Click **Trusted CAs** to go to the **Trusted CAs** 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. Fill in both the **Reference Number** and the **Key** fields if your certification authority uses CMP enrollment protocol. Just fill in the **Key** field if your certification authority uses the SCEP enrollment protocol. |
| Reference Number | Enter the reference number that the certification authority gave you. You can use up to 31 ASCII printable characters. Spaces are allowed. |
| Key | Type the key that the certification authority gave you. You can use up to 31 ASCII printable characters. Spaces are allowed. |
| Apply | Click **Apply** to begin certificate or certification request generation. |
| Cancel | Click **Cancel** to quit and return to the **My Certificates** screen. |

- After you click **Apply** in the **My Certificate Create** screen, you see a screen that tells you the ZyWALL is generating the self-signed certificate or certification request.
- After the ZyWALL successfully enrolls a certificate or generates a certification request or a self-signed certificate, you see a screen with a **Return** button that takes you back 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.

## 20.6 The Trusted CAs Screen

Click **SECURITY** > **CERTIFICATES** > **Trusted CAs** to open the **Trusted CAs** screen. This screen displays a summary list of certificates of the certification authorities that you have set the ZyWALL to accept as trusted. The ZyWALL accepts any valid certificate signed by a certification authority on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certification authorities.

**Figure 241** SECURITY > CERTIFICATES > Trusted CAs




The following table describes the labels in this screen.

**Table 119** SECURITY > CERTIFICATES > Trusted CAs

| 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. 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. |
| CRL Issuer | This field displays **Yes** if the certification authority issues CRL (Certificate Revocation Lists) for the certificates that it has issued and you have selected the **Check incoming certificates issued by this CA against a CRL** check box in the certificate's details screen to have the ZyWALL check the CRL before trusting any certificates issued by the certification authority. Otherwise the field displays **No**. |

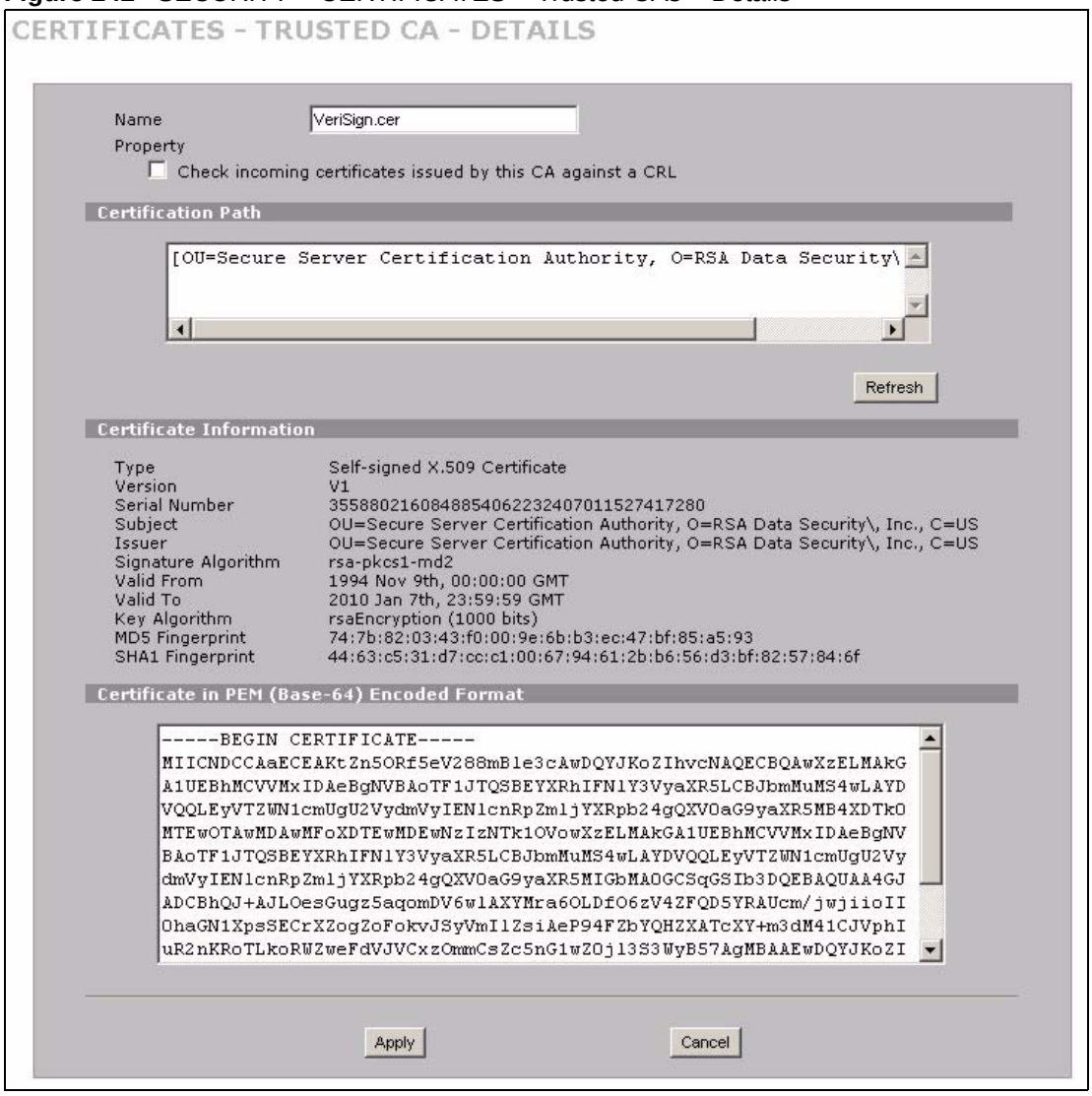
**Table 119** SECURITY > CERTIFICATES > Trusted CAs (continued)

| LABEL | DESCRIPTION |
|---|---|
| Modify | Click the details icon to open a screen with an in-depth list of information about the certificate.<br>Use the export icon to save the certificate to a computer. Click the icon 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**.<br>Click the delete icon to remove the 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. |

## 20.7 The Trusted CA Details Screen

Click **SECURITY** > **CERTIFICATES** > **Trusted CAs** to open the **Trusted CAs** screen. Click the details icon to open the **Trusted CA Details** screen. Use this screen to view in-depth information about the certification authority's 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 242** SECURITY > CERTIFICATES > Trusted CAs > Details




The following table describes the labels in this screen.

**Table 120** SECURITY > CERTIFICATES > Trusted CAs > Details

| LABEL | DESCRIPTION |
|---|---|
| Name | This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this key certificate. You may use any character (not including spaces). |
| Property<br>Check incoming certificates issued by this CA against a CRL | Select this check box to have the ZyWALL check incoming certificates that are issued by this certification authority against a Certificate Revocation List (CRL).<br>Clear this check box to have the ZyWALL not check incoming certificates that are issued by this certification authority against a Certificate Revocation List (CRL). |

**Table 120** SECURITY > CERTIFICATES > Trusted CAs > Details (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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 certification authority, 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. |
| 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. |
| 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>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. |

**Table 120** SECURITY > CERTIFICATES > Trusted CAs > Details (continued)

| LABEL | DESCRIPTION |
|---|---|
| CRL Distribution Points | This field displays how many directory servers with Lists of revoked certificates the issuing certification authority of this certificate makes available. This field also displays the domain names or IP addresses of the servers. |
| 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. |
| 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 64 ASCII characters to convert the 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). |
| Apply | Click **Apply** to save your changes back to the ZyWALL. You can only change the name and/or set whether or not you want the ZyWALL to check the CRL that the certification authority issues before trusting a certificate issued by the certification authority. |
| Cancel | Click **Cancel** to quit and return to the **Trusted CAs** screen. |

## 20.8 The Trusted CA Import Screen

Click **SECURITY** > **CERTIFICATES** > **Trusted CAs** to open the **Trusted CAs** screen and then click **Import** to open the **Trusted CA Import** screen. Follow the instructions in this screen to save a trusted certification authority's certificate from a computer to the ZyWALL. The ZyWALL trusts any valid certificate signed by any of the imported trusted CA certificates.

You must remove any spaces from the certificate's filename before you can import the certificate.

**Figure 243** SECURITY > CERTIFICATES > Trusted CAs > Import


The following table describes the labels in this screen.

**Table 121** SECURITY > CERTIFICATES > Trusted CAs Import

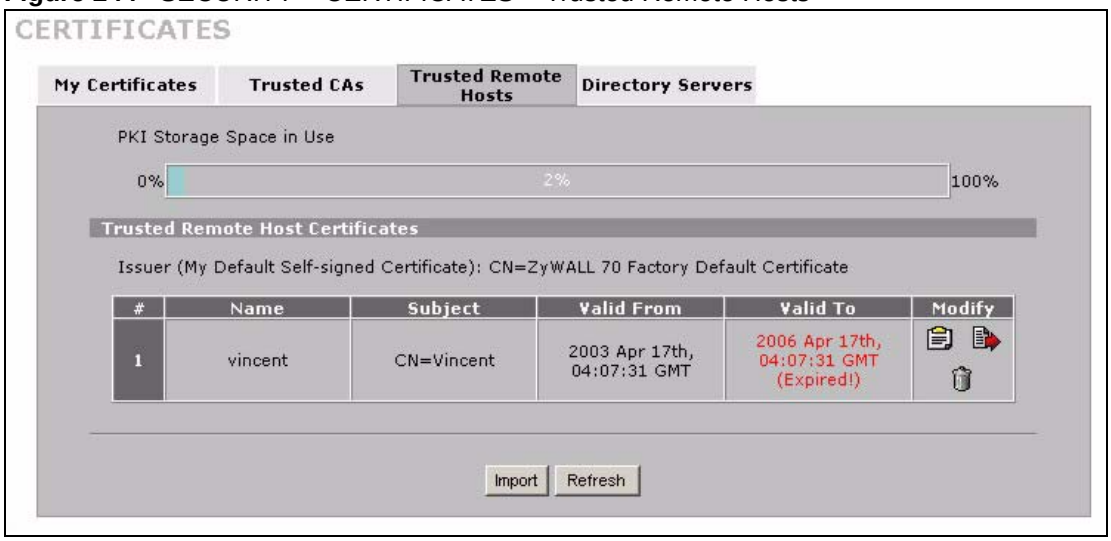
| LABEL | DESCRIPTION |
|---|---|
| File Path | Type in the location of the file you want to upload in this field or click **Browse** to find it. |
| Browse | Click **Browse** to find the certificate file you want to upload. |
| Apply | Click **Apply** to save the certificate on the ZyWALL. |
| Cancel | Click **Cancel** to quit and return to the **Trusted CAs** screen. |

## 20.9 The Trusted Remote Hosts Screen

Click **SECURITY** > **CERTIFICATES** > **Trusted Remote Hosts** to open the **Trusted Remote Hosts** screen. This screen displays a list of the certificates of peers that you trust but which are not signed by one of the certification authorities on the **Trusted CAs** screen.

You do not need to add any certificate that is signed by one of the certification authorities on the **Trusted CAs** screen since the ZyWALL automatically accepts any valid certificate signed by a trusted certification authority as being trustworthy.

**Figure 244** SECURITY > CERTIFICATES > Trusted Remote Hosts




The following table describes the labels in this screen.

**Table 122** SECURITY > CERTIFICATES > Trusted Remote Hosts

| 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. |
| Issuer (My Default Self-signed Certificate) | This field displays identifying information about the default self-signed certificate on the ZyWALL that the ZyWALL uses to sign the trusted remote host 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. |
| 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. |
| Modify | Click the details icon to open a screen with an in-depth list of information about the certificate.<br>Use the export icon to save the certificate to a computer. Click the icon 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**.<br>Click the delete icon to remove the certificate. A window displays asking you to confirm that you want to delete the certificate. 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 remote host (which you trust) from your computer to the ZyWALL. |
| Refresh | Click this button to display the current validity status of the certificates. |

## 20.10 The Trusted Remote Hosts Import Screen

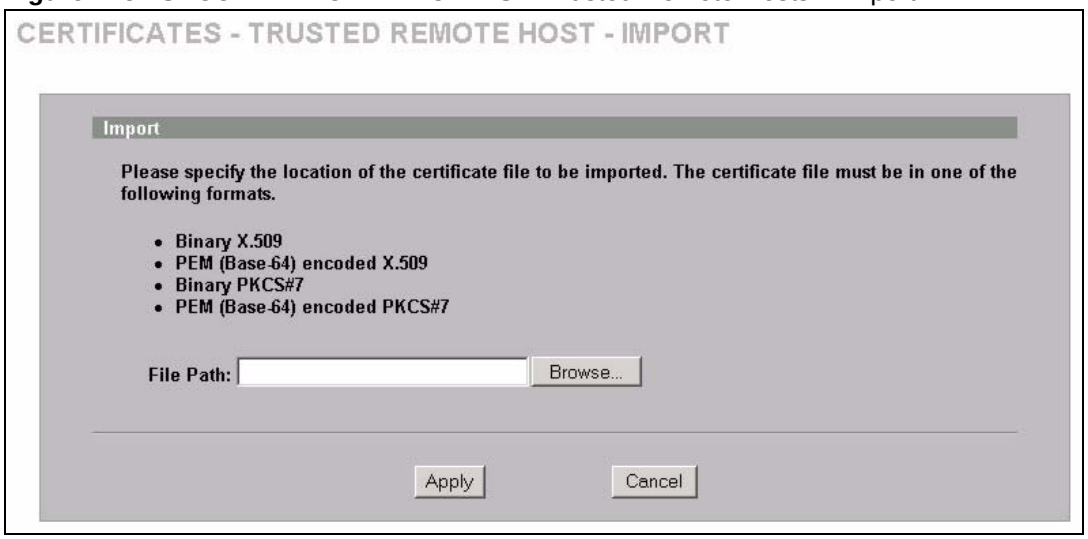
Click **SECURITY** > **CERTIFICATES** > **Trusted Remote Hosts** to open the **Trusted Remote Hosts** screen and then click **Import** to open the **Trusted Remote Host Import** screen.

You may have peers with certificates that you want to trust, but the certificates were not signed by one of the certification authorities on the **Trusted CAs** screen. Follow the instructions in this screen to save a peer's certificates from a computer to the ZyWALL.

You do not need to add any certificate that is signed by one of the certification authorities on the **Trusted CAs** screen since the ZyWALL automatically accepts any valid certificate signed by a trusted certification authority as being trustworthy.

The trusted remote host certificate must be a self-signed certificate; and you must remove any spaces from its filename before you can import it.

**Figure 245** SECURITY > CERTIFICATES > Trusted Remote Hosts > Import




The following table describes the labels in this screen.

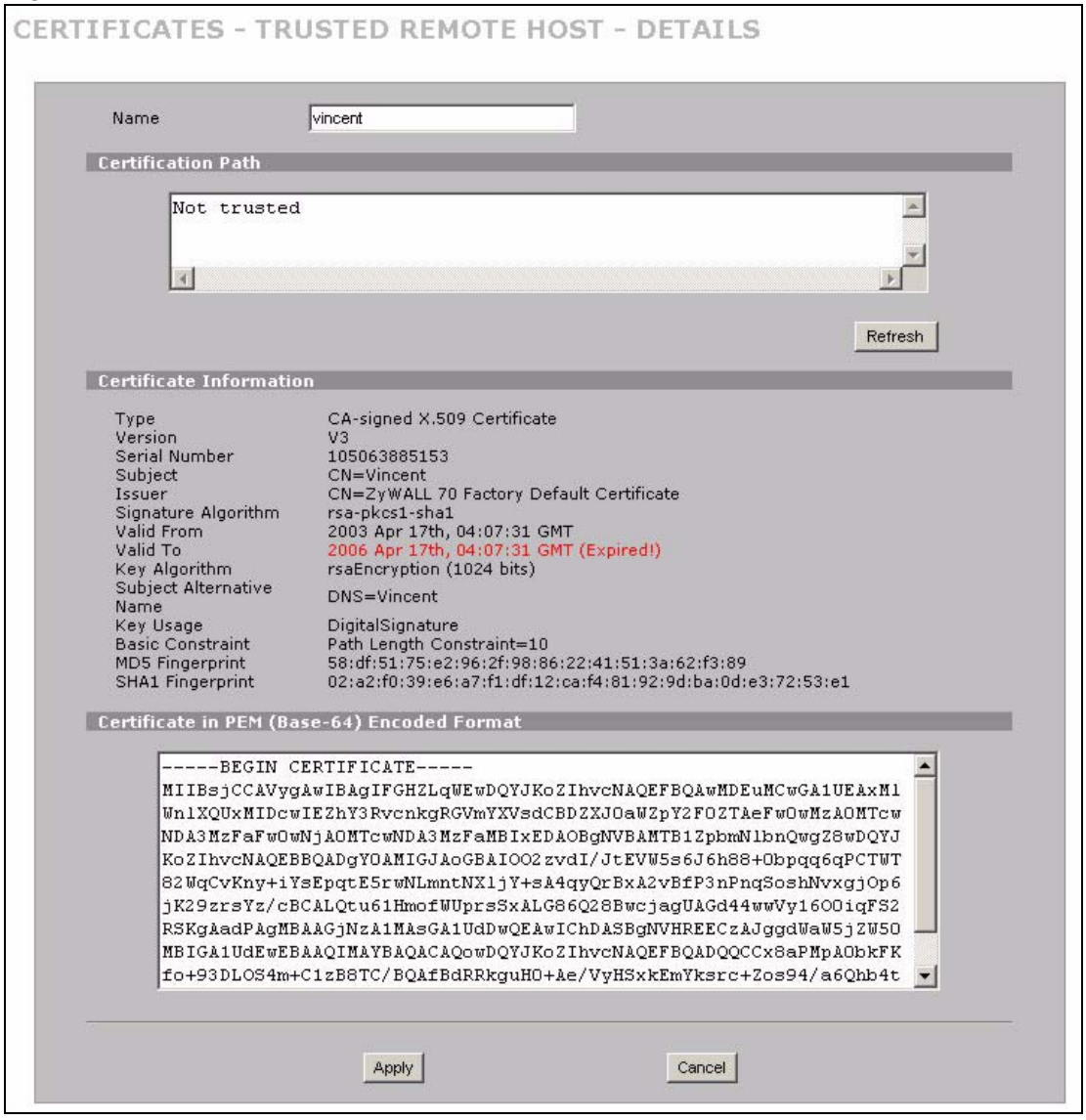
**Table 123** SECURITY > CERTIFICATES > Trusted Remote Hosts > Import

| LABEL | DESCRIPTION |
|---|---|
| File Path | Type in the location of the file you want to upload in this field or click **Browse** to find it. |
| Browse | Click **Browse** to find the certificate file you want to upload. |
| Apply | Click **Apply** to save the certificate on the ZyWALL. |
| Cancel | Click **Cancel** to quit and return to the **Trusted Remote Hosts** screen. |

## 20.11 The Trusted Remote Host Certificate Details Screen

Click **SECURITY** > **CERTIFICATES** > **Trusted Remote Hosts** to open the **Trusted Remote Hosts** screen. Click the details icon to open the **Trusted Remote Host Details** screen. You can use this screen to view in-depth information about the trusted remote host's certificate and/or change the certificate's name.

**Figure 246** SECURITY > CERTIFICATES > Trusted Remote Hosts > Details



The following table describes the labels in this screen.

**Table 124** SECURITY > CERTIFICATES > Trusted Remote Hosts > Details

| LABEL | DESCRIPTION |
|---|---|
| Name | This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this key certificate. You may use any character (not including spaces). |
| Certification Path | Click the **Refresh** button to have this read-only text box display the end entity's own certificate and a list of certification authority certificates in the hierarchy of certification authorities that validate a certificate's issuing certification authority. For a trusted host, the list consists of the end entity's own certificate and the default self-signed certificate that the ZyWALL uses to sign remote host certificates. |
| 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. With trusted remote host certificates, this field always displays CA-signed. The ZyWALL is the Certification Authority that signed the certificate. 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 device that created the certificate. |
| 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 default self-signed certificate on the ZyWALL that the ZyWALL uses to sign the trusted remote host certificates. |
| Signature Algorithm | This field displays the type of algorithm that the ZyWALL used to sign the certificate, which is rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 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. |

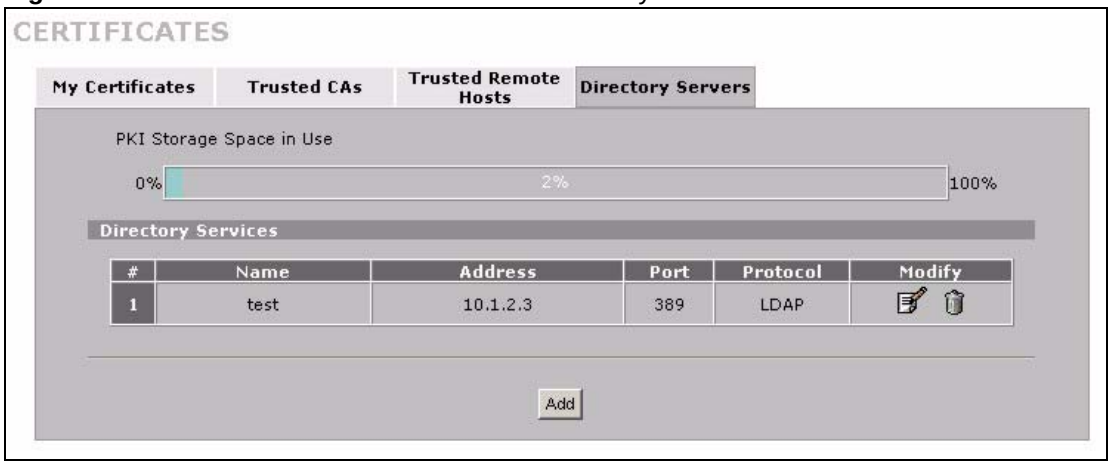
**Table 124** SECURITY > CERTIFICATES > Trusted Remote Hosts > Details (continued)

| LABEL | DESCRIPTION |
|---|---|
| MD5 Fingerprint | This is the certificate's message digest that the ZyWALL calculated using the MD5 algorithm. The ZyWALL uses one of its own self-signed certificates to sign the imported trusted remote host certificates. This changes the fingerprint value displayed here (so it does not match the original). See Section 20.1.3 on page 400 for how to verify a remote host's certificate before you import it into the ZyWALL. |
| SHA1 Fingerprint | This is the certificate's message digest that the ZyWALL calculated using the SHA1 algorithm. The ZyWALL uses one of its own self-signed certificates to sign the imported trusted remote host certificates. This changes the fingerprint value displayed here (so it does not match the original). See Section 20.1.3 on page 400 for how to verify a remote host's certificate before you import it into the ZyWALL. |
| 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 64 ASCII characters to convert the 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). |
| Apply | Click **Apply** to save your changes back to the ZyWALL. You can only change the name of the certificate. |
| Cancel | Click **Cancel** to quit configuring this screen and return to the **Trusted Remote Hosts** screen. |

## 20.12 The Directory Servers Screen

Click **SECURITY** > **CERTIFICATES** > **Directory Servers** to open the **Directory Servers** screen. This screen displays a summary list of directory servers (that contain lists of valid and revoked certificates) that have been saved into the ZyWALL. If you decide to have the ZyWALL check incoming certificates against the issuing certification authority's list of revoked certificates, the ZyWALL first checks the server(s) listed in the **CRL Distribution Points** field of the incoming certificate. If the certificate does not list a server or the listed server is not available, the ZyWALL checks the servers listed here.

**Figure 247** SECURITY > CERTIFICATES > Directory Servers



The following table describes the labels in this screen.

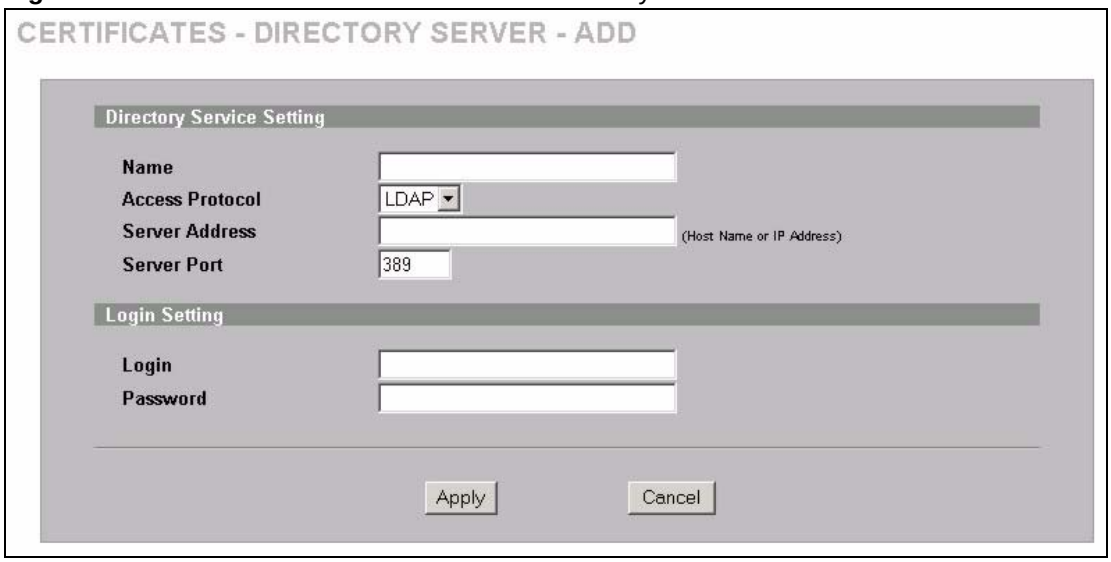
**Table 125** SECURITY > CERTIFICATES > Directory Servers

| 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. |
| # | The index number of the directory server. The servers are listed in alphabetical order. |
| Name | This field displays the name used to identify this directory server. |
| Address | This field displays the IP address or domain name of the directory server. |
| Port | This field displays the port number that the directory server uses. |
| Protocol | This field displays the protocol that the directory server uses. |
| Modify | Click the details icon to open a screen where you can change the information about the directory server.<br>Click the delete icon to remove the directory server entry. A window displays asking you to confirm that you want to delete the directory server. Note that subsequent certificates move up by one when you take this action. |
| Add | Click **Add** to open a screen where you can configure information about a directory server so that the ZyWALL can access it. |

## 20.13 The Directory Server Add or Edit Screen

Click **SECURITY** > **CERTIFICATES** > **Directory Servers** to open the **Directory Servers** screen. Click **Add** (or the details icon) to open the **Directory Server Add** screen. Use this screen to configure information about a directory server that the ZyWALL can access.

**Figure 248** SECURITY > CERTIFICATES > Directory Server > Add



The following table describes the labels in this screen.

**Table 126** SECURITY > CERTIFICATES > Directory Server > Add

| LABEL | DESCRIPTION |
|---|---|
| Directory Service Setting | |
| Name | Type up to 31 ASCII characters (spaces are not permitted) to identify this directory server. |
| Access Protocol | Use the drop-down list box to select the access protocol used by the directory server.<br>**LDAP** (Lightweight Directory Access Protocol) is a protocol over TCP that specifies how clients access directories of certificates and lists of revoked certificates.[A] |
| Server Address | Type the IP address (in dotted decimal notation) or the domain name of the directory server. |
| Server Port | This field displays the default server port number of the protocol that you select in the **Access Protocol** field.<br>You may change the server port number if needed, however you must use the same server port number that the directory server uses.<br>389 is the default server port number for LDAP. |
| Login Setting | |
| Login | The ZyWALL may need to authenticate itself in order to assess the directory server. Type the login name (up to 31 ASCII characters) from the entity maintaining the directory server (usually a certification authority). |
| Password | Type the password (up to 31 ASCII characters) from the entity maintaining the directory server (usually a certification authority). |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to quit configuring this screen and return to the **Directory Servers** screen. |

A. At the time of writing, LDAP is the only choice of directory server access protocol.

# 21

# Authentication Server Screens

## 21.1 Overview

This chapter discusses how to configure the ZyWALL's authentication server feature.

A ZyWALL set to be a VPN extended authentication server can use either the local user database internal to the ZyWALL or an external RADIUS server for an unlimited number of users. The ZyWALL uses the same local user database for VPN extended authentication and wireless LAN security.

### 21.1.1 What You Can Do in the Authentication Server Screens

- Use the **Local User Database** Screen (Section 21.2 on page 428) to configure your ZyWALL's list of local user profiles.
- Use the **RADIUS** Screen (Section 21.3 on page 430) to configure external RADIUS server settings.

### 21.1.2 What You Need To Know About Authentication Server

#### Local User Database

By storing user profiles locally on the ZyWALL, your ZyWALL is able to authenticate users without interacting with a network RADIUS server. However, there is a limit on the number of users you may authenticate in this way.

#### RADIUS

The ZyWALL can use an external RADIUS server to authenticate an unlimited number of users. RADIUS is based on a client-server model that supports authentication and accounting, where access point is the client and the server is the RADIUS server.

- Authentication
  Determines the identity of the users.
- Accounting
  Keeps track of the client's network activity.

RADIUS user is a simple package exchange in which your ZyWALL acts as a message relay between the wireless station and the network RADIUS server.

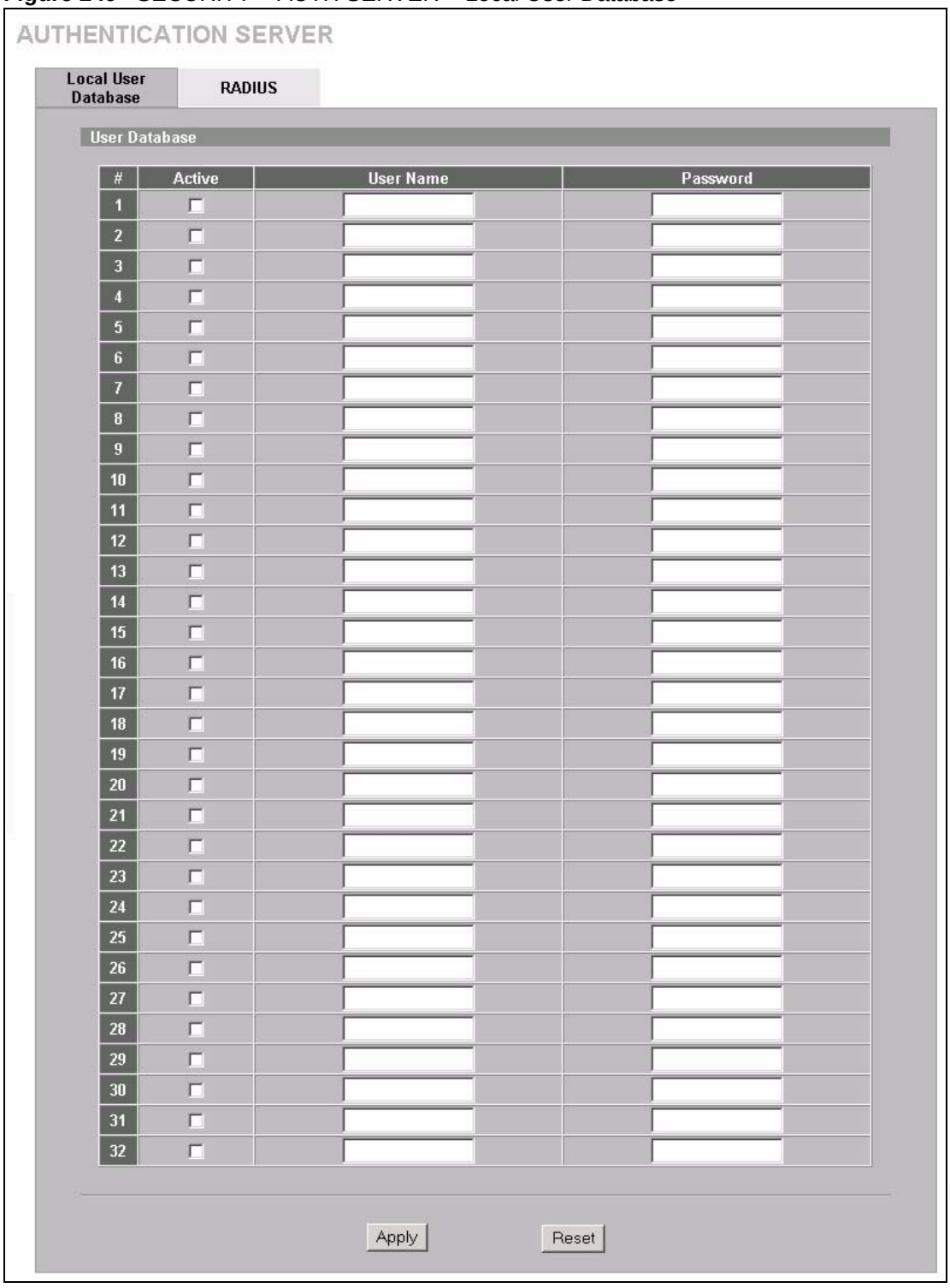
#### Finding Out More

Refer to Section 12.4 on page 244 for more information about RADIUS.

## 21.2 The Local User Database Screen

Click **SECURITY** > **AUTH SERVER** to open the **Local User Database** screen. The local user database is a list of user profiles stored on the ZyWALL. The ZyWALL can use this list of user profiles to authenticate users. Use this screen to change your ZyWALL's list of user profiles.

**Figure 249** SECURITY > AUTH SERVER > Local User Database



The following table describes the labels in this screen.

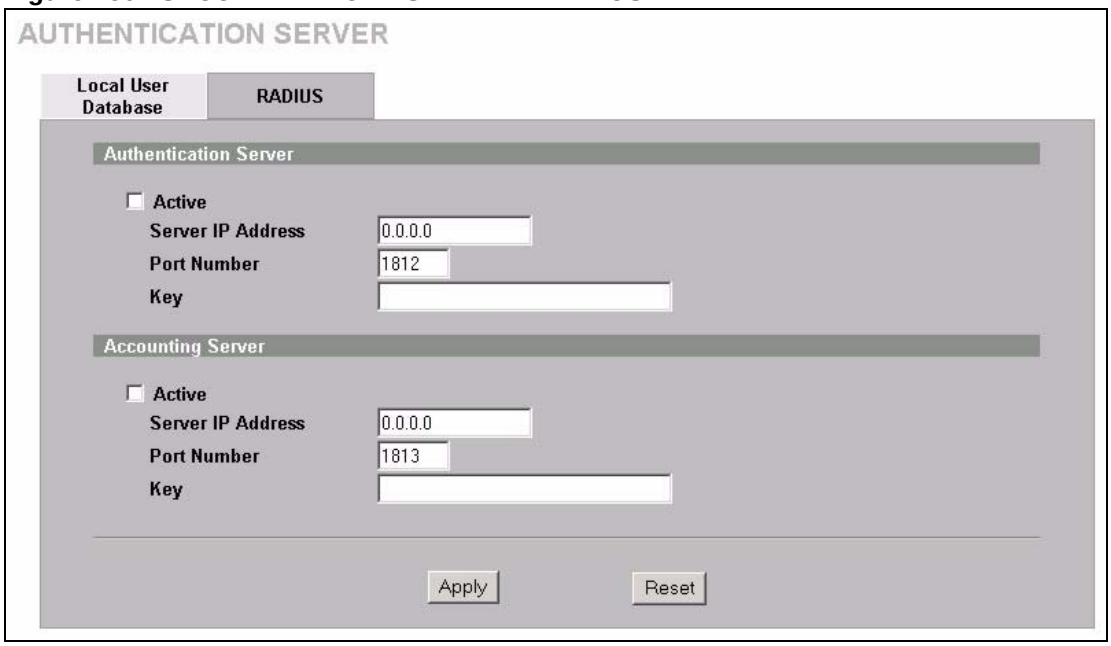
**Table 127** SECURITY > AUTH SERVER > Local User Database

| LABEL | DESCRIPTION |
|---|---|
| Active | Select this check box to enable the user profile. |
| User Name | Enter the user name of the user profile. |
| Password | Enter a password up to 31 characters long for this user profile. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 21.3 The RADIUS Screen

Click **SECURITY** > **AUTH SERVER** > **RADIUS** to open the **RADIUS** screen. Configure this screen to use an external RADIUS server to authenticate users.

**Figure 250** SECURITY > AUTH SERVER > RADIUS




The following table describes the labels in this screen.

**Table 128** SECURITY > AUTH SERVER > RADIUS

| LABEL | DESCRIPTION |
|---|---|
| Authentication Server | |
| Active | Select the check box to enable user authentication through an external authentication server.<br>Clear the check box to enable user authentication using the local user profile on the ZyWALL. |
| Server IP Address | Enter the IP address of the external authentication server in dotted decimal notation. |
| Port Number | 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. |

**Table 128** SECURITY > AUTH SERVER > RADIUS

| LABEL | DESCRIPTION |
|---|---|
| Key | Enter a password (up to 31 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 ZyWALL. |
| Accounting Server | |
| Active | Select the check box to enable user accounting through an external authentication server. |
| Server IP Address | Enter the IP address of the external accounting server in dotted decimal notation. |
| Port Number | The default port of the RADIUS server for accounting is **1813**.<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 31 alphanumeric characters) as the key to be shared between the external accounting server and the ZyWALL.<br>The key is not sent over the network. This key must be the same on the external accounting server and ZyWALL. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# PART IV
# Advanced

# 22

# Network Address Translation (NAT)

## 22.1 Overview

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet. For example, the source address of an outgoing packet, used within one network is changed to a different IP address known within another network.

### 22.1.1 What You Can Do Using the NAT Screens

- Use the **NAT Overview** screen (Section 22.2 on page 436) to configure global NAT settings and enable NAT on a WAN interface.
- Use the **Address Mapping** screens (Section 22.3 on page 438**)** to change your ZyWALL's address mapping settings. Not all fields are available on all models.
- Click **Port Forwarding** screens (Section 22.4 on page 441) to make servers with private IP addresses on your network (behind NAT) visible to the outside world.
- Click **Port Triggering** screens (Section 22.5 on page 445) to change your ZyWALL's trigger port settings.

### 22.1.2 What You Need To Know About NAT

#### NAT Mapping Types

NAT supports five types of IP/port mapping. They are:

- **One to One**: In One-to-One mode, the ZyWALL maps one local IP address to one global IP address.
- **Many to One**: In Many-to-One mode, the ZyWALL maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature (the **SUA** option).
- **Many to Many Overload**: In Many-to-Many Overload mode, the ZyWALL maps the multiple local IP addresses to shared global IP addresses.
- **Many One to One**: In Many-One-to-One mode, the ZyWALL maps each local IP address to a unique global IP address.
- **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world although, it is highly recommended that you use the DMZ port for these servers instead.

The following table summarizes the NAT mapping types.

**Table 129** NAT Mapping Types

| TYPE | IP MAPPING | SMT ABBREVIATION |
|---|---|---|
| One-to-One | ILA1 ←→ IGA1 | 1-1 |
| Many-to-One (SUA/PAT) | ILA1 ←→ IGA1<br>ILA2 ←→ IGA1<br>… | M-1 |
| Many-to-Many Overload | ILA ←→ IGA1<br>ILA2 ←→ IGA2<br>ILA3 ←→ IGA1<br>ILA4 ←→ IGA2<br>… | M-M Ov |
| Many-One-to-One | ILA1 ←→ IGA1<br>ILA2 ←→ IGA2<br>ILA3 ←→ IGA3<br>… | M-1-1 |
| Server | Server 1 IP ←→ IGA1<br>Server 2 IP ←→ IGA1<br>Server 3 IP ←→ IGA1 | Server |

Port numbers do **not** change for **One-to-One** and **Many-One-to-One** NAT mapping types.

#### SUA (Single User Account) Versus NAT

SUA (Single User Account) is a ZyNOS implementation of a subset of NAT that supports two types of mapping: **Many-to-One** and **Server**. The ZyWALL also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses on your network.

When you select **SUA**, WAN-to-LAN and WAN-to-DMZ address translation is performed. If you want (some) computers on your DMZ to have public IP addresses, then select **Full Feature** (not **SUA**) and don't configure NAT mapping rules to those computers with public IP addresses on the DMZ.

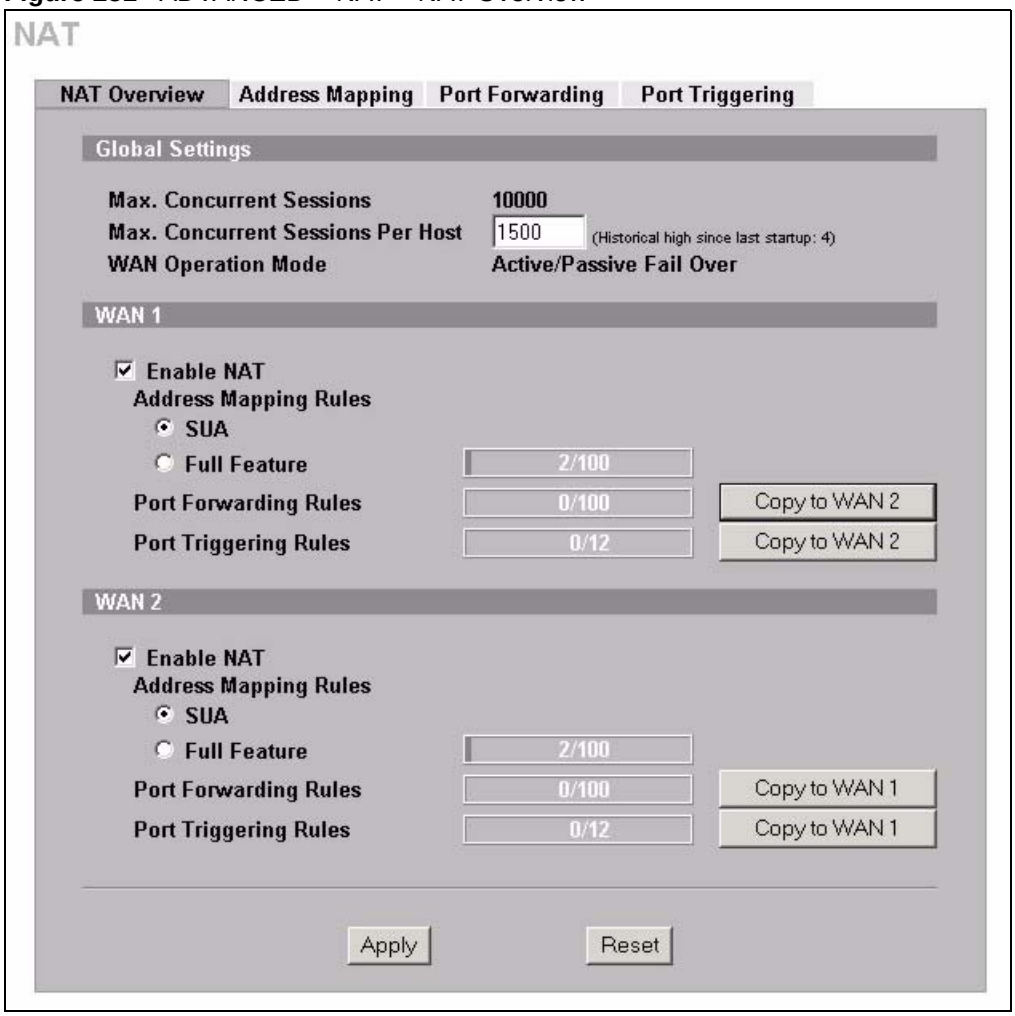
### 22.1.3 Before You Begin

You must create a firewall rule in addition to setting up SUA/NAT, if you want to allow traffic originating from the WAN to be forwarded through the ZyWALL.

## 22.2 The NAT Overview Screen

Click **ADVANCED** > **NAT** to open the **NAT Overview** screen.

**Figure 251** ADVANCED > NAT > NAT Overview




The following table describes the labels in this screen.

**Table 130** ADVANCED > NAT > NAT Overview

| LABEL | DESCRIPTION |
|---|---|
| Global Settings | |
| Max. Concurrent Sessions | This read-only field displays the highest number of NAT sessions that the ZyWALL will permit at one time. |
| Max. Concurrent Sessions Per Host | Use this field to set the highest number of NAT sessions that the ZyWALL will permit a host to have at one time. |
| WAN Operation Mode | This read-only field displays the operation mode of the ZyWALL's WAN interfaces. |
| WAN 1, 2 | |
| Enable NAT | Select this check box to turn on the NAT feature for the WAN interface. Clear this check box to turn off the NAT feature for the WAN interface. |

**Table 130** ADVANCED > NAT > NAT Overview (continued)

| LABEL | DESCRIPTION |
|---|---|
| Address Mapping Rules | Select **SUA** if you have just one public WAN IP address for your ZyWALL. This lets the ZyWALL use its permanent, pre-defined NAT address mapping rules.<br>Select **Full Feature** if you have multiple public WAN IP addresses for your ZyWALL. This lets the ZyWALL use the address mapping rules that you configure. This is the equivalent of what used to be called full feature NAT or multi-NAT.<br>The bar displays how many of the ZyWALL's possible address mapping rules are configured. The first number shows how many address mapping rules are configured on the ZyWALL. The second number shows the maximum number of address mapping rules that can be configured on the ZyWALL. |
| Port Forwarding Rules | The bar displays how many of the ZyWALL's possible port forwarding rules are configured. The first number shows how many port forwarding rules are configured on the ZyWALL. The second number shows the maximum number of port forwarding rules that can be configured on the ZyWALL. |
| Port Triggering Rules | The bar displays how many of the ZyWALL's possible trigger port rules are configured. The first number shows how many trigger port rules are configured on the ZyWALL. The second number shows the maximum number of trigger port rules that can be configured on the ZyWALL. |
| Copy to WAN 2 (and Copy to WAN 1) | Click **Copy to WAN 2** (or **Copy to WAN 1**) to duplicate this WAN interface's NAT port forwarding or trigger port rules on the other WAN interface.<br>Note: Using the copy button overwrites the other WAN interface's existing rules.<br>The copy button is best suited for initial NAT configuration where you have configured NAT port forwarding or trigger port rules for one interface and want to use similar rules for the other WAN interface. You can use the other NAT screens to edit the NAT rules after you copy them from one WAN interface to the other. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

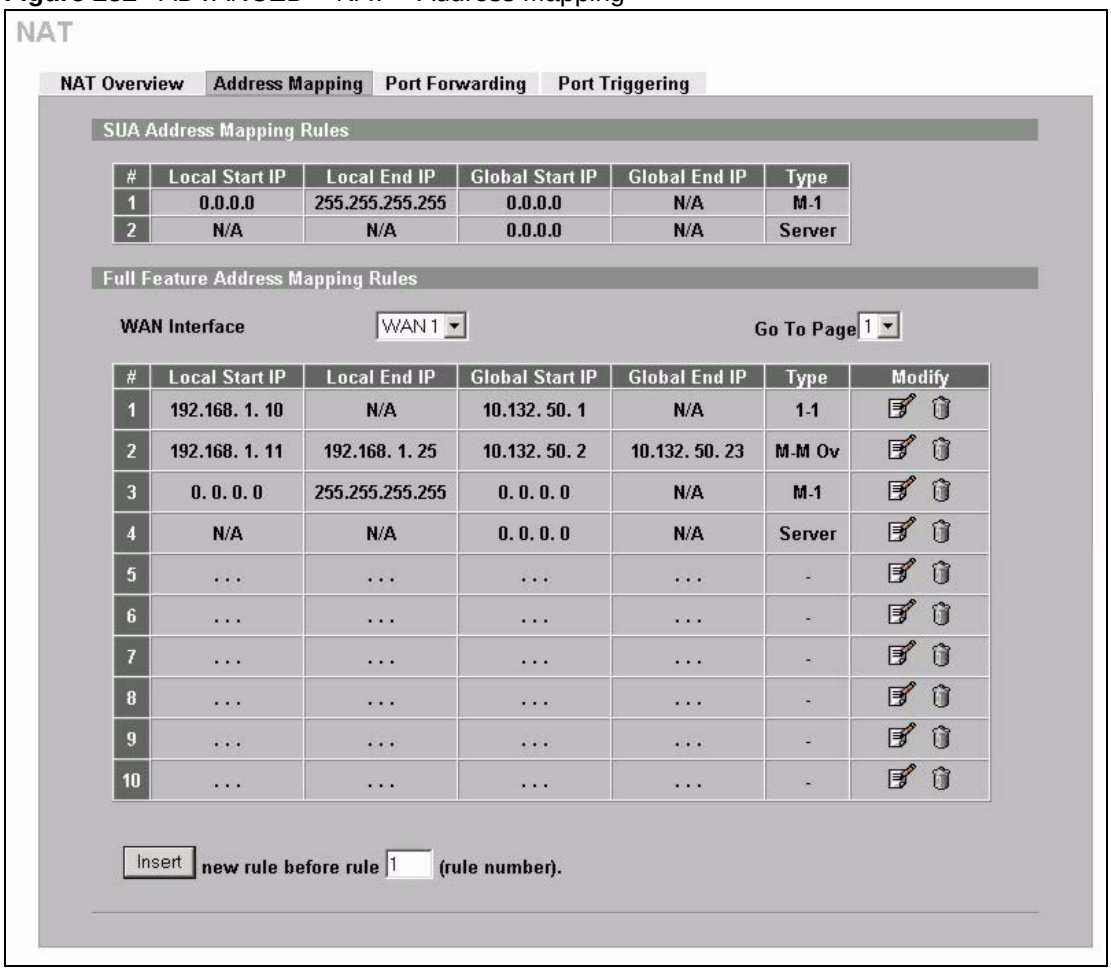
## 22.3 The NAT Address Mapping Screen

Click **ADVANCED** > **NAT** > **Address Mapping** to open the following screen.

Use this screen to change your ZyWALL's address mapping settings. Not all fields are available on all models.

Ordering your rules is important because the ZyWALL applies the rules in the order that you specify. When a rule matches the current packet, the ZyWALL takes the corresponding action and the remaining rules are ignored. If there are any empty rules before your new configured rule, your configured rule will be pushed up by that number of empty rules. For example, if you have already configured rules 1 to 6 in your current set and now you configure rule number 9. In the set summary screen, the new rule will be rule 7, not 9. Now if you delete rule 4, rules 5 to 7 will be pushed up by 1 rule, so old rules 5, 6 and 7 become new rules 4, 5 and 6.

**Figure 252** ADVANCED > NAT > Address Mapping




The following table describes the labels in this screen.

**Table 131** ADVANCED > NAT > Address Mapping

| LABEL | DESCRIPTION |
|---|---|
| SUA Address Mapping Rules | This read-only table displays the default address mapping rules. |
| Full Feature Address Mapping Rules | |
| WAN Interface | Select the WAN interface for which you want to view or configure address mapping rules. |
| Go To Page | Choose a page from the drop-down list box to display the corresponding summary page of address mapping rules. |
| # | This is the rule index number. |
| Local Start IP | This refers to the Inside Local Address (ILA), which is the starting local IP address. If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the **Local Start IP** address. Local IP addresses are **N/A** for **Server** port mapping. |
| Local End IP | This is the end Inside Local Address (ILA). If the rule is for all local IP addresses, then this field displays 255.255.255.255 as the **Local End IP** address. This field is **N/A** for **One-to-One** and **Server** mapping types. |

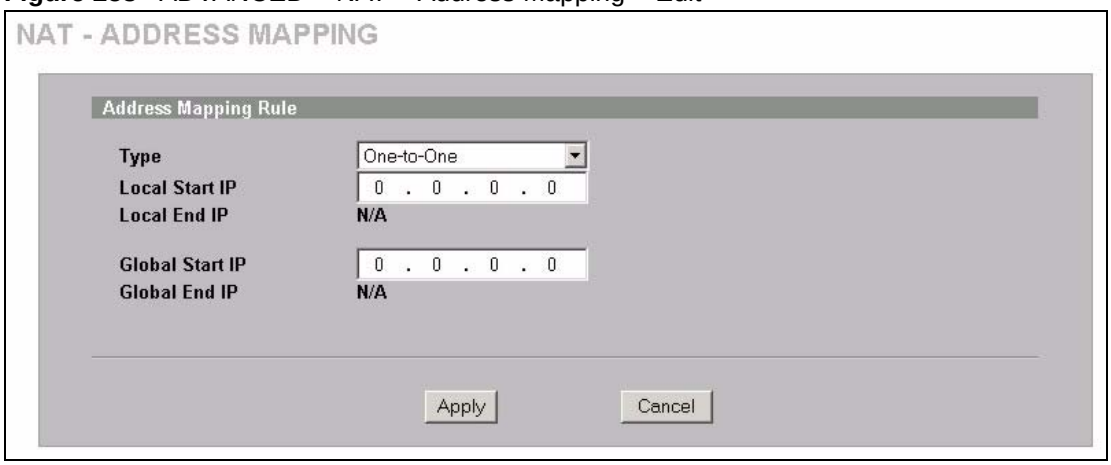
**Table 131** ADVANCED > NAT > Address Mapping (continued)

| LABEL | DESCRIPTION |
|---|---|
| Global Start IP | This refers to the Inside Global IP Address (IGA), that is the starting global IP address. 0.0.0.0 is for a dynamic IP address from your ISP with **Many-to-One** and **Server** mapping types. |
| Global End IP | This is the ending Inside Global Address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server** mapping types. |
| Type | 1. **One-to-One** mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-One NAT mapping type.<br>2. **Many-to-One** mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported only.<br>3. **Many-to-Many Overload** mode maps multiple local IP addresses to shared global IP addresses.<br>4. **Many One-to-One** mode maps each local IP address to unique global IP addresses.<br>5. **Server** allows you to specify inside servers of different services behind the NAT to be accessible to the outside world. |
| Modify | Click the edit icon to go to the screen where you can edit the address mapping rule.<br>Click the delete icon to delete an existing address mapping rule. A window display asking you to confirm that you want to delete the address mapping rule. Note that subsequent address mapping rules move up by one when you take this action. |
| Insert | Click **Insert** to insert a new mapping rule before an existing one. |

## 22.3.1 NAT Address Mapping Edit

Click the edit icon to display the **NAT Address Mapping Edit** screen. Use this screen to edit an address mapping rule. See Section 22.1 on page 435 for information on NAT and address mapping.

**Figure 253** ADVANCED > NAT > Address Mapping > Edit



The following table describes the labels in this screen.

**Table 132** ADVANCED > NAT > Address Mapping > Edit

| LABEL | DESCRIPTION |
|---|---|
| Type | Choose the port mapping type from one of the following.<br>1. **One-to-One**: One-to-One mode maps one local IP address to one global IP address. Note that port numbers do not change for One-to-One NAT mapping type.<br>2. **Many-to-One**: Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature.<br>3. **Many-to-Many Overload**: Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses.<br>4. **Many One-to-One**: Many One-to-One mode maps each local IP address to unique global IP addresses.<br>5. **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world. |
| Local Start IP | This is the starting Inside Local IP Address (ILA). Local IP addresses are **N/A** for **Server** port mapping. |
| Local End IP | This is the end Inside Local IP Address (ILA). If your rule is for all local IP addresses, then enter 0.0.0.0 as the **Local Start IP** address and 255.255.255.255 as the **Local End IP** address.<br>This field is **N/A** for **One-to-One** and **Server** mapping types. |
| Global Start IP | This is the starting Inside Global IP Address (IGA). Enter **0.0.0.0** here if you have a dynamic IP address from your ISP. |
| Global End IP | This is the ending Inside Global IP Address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server** mapping types. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving. |

## 22.4 The Port Forwarding Screen

A port forwarding set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though NAT makes your whole inside network appear as a single computer to the outside world.

You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports.

Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

### 22.4.1 Default Server IP Address

In addition to the servers for specified services, NAT supports a default server IP address. A default server receives packets from ports that are not specified in this screen.

If you do not assign a **Default Server** IP address, the ZyWALL discards all packets received for ports that are not specified here or in the remote management setup.

## 22.4.2 Port Forwarding: Services and Port Numbers

The ZyWALL provides the additional safety of the DMZ ports for connecting your publicly accessible servers. This makes the LAN more secure by physically separating it from your public servers.

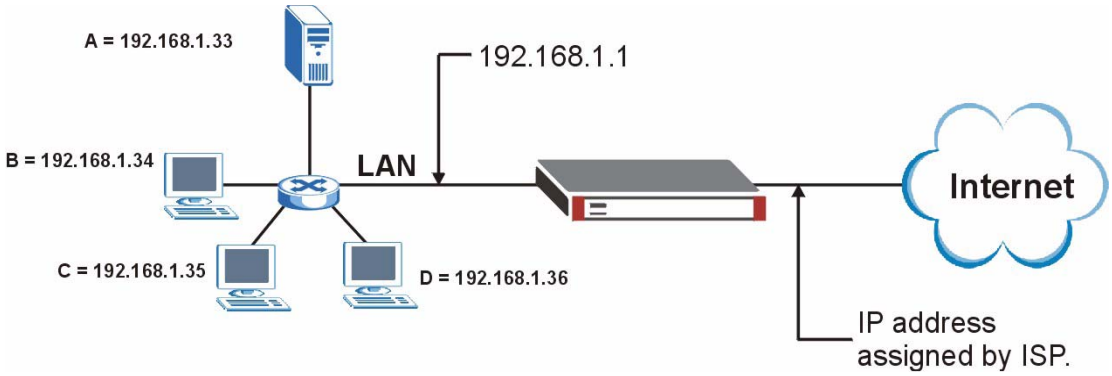
Use the **Port Forwarding** screen to forward incoming service requests to the server(s) on your local network.

The most often used port numbers are shown in the User's Guide appendix Appendix B on page 783. Please refer to RFC 1700 for further information about port numbers.

## 22.4.3 Configuring Servers Behind Port Forwarding (Example)

Let's say 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 254** Multiple Servers Behind NAT Example




## 22.4.4 NAT and Multiple WAN

The ZyWALL has two WAN interfaces. You can configure port forwarding and trigger port rule sets for the first WAN interface and separate sets of rules for the second WAN interface.

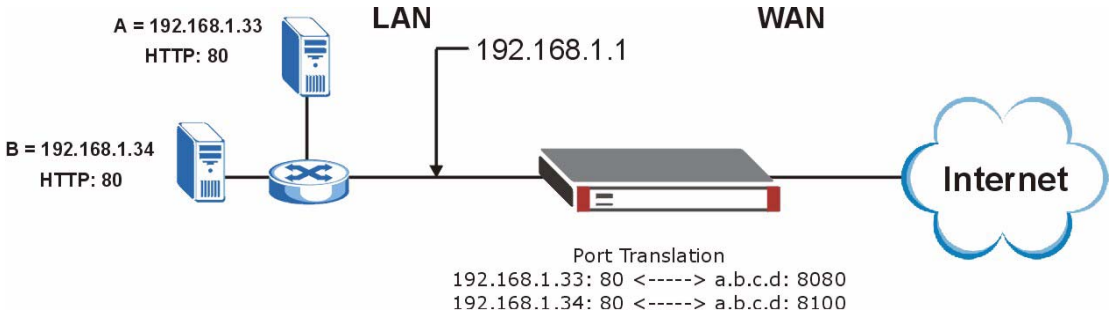
## 22.4.5 Port Translation

The ZyWALL can translate the destination port number or a range of port numbers of packets coming from the WAN to another destination port number or range of port numbers on the local network. When you use port forwarding without port translation, a single server on the local network can use a specific port number and be accessible to the outside world through a single WAN IP address. When you use port translation with port forwarding, multiple servers on the local network can use the same port number and still be accessible to the outside world through a single WAN IP address.

The following example has two web servers on a LAN. Server **A** uses IP address 192.168.1.33 and server **B** uses 192.168.1.34. Both servers use port 80. The letters a.b.c.d represent the WAN port's IP address. The ZyWALL translates port 8080 of traffic received on the WAN port (IP address a.b.c.d) to port 80 and sends it to server **A** (IP address 192.168.1.33). The ZyWALL also translates port 8100 of traffic received on the WAN port (also IP address a.b.c.d) to port 80, but sends it to server **B** (IP address 192.168.1.34).

In this example, anyone wanting to access server A from the Internet must use port 8080. Anyone wanting to access server B from the Internet must use port 8100.

**Figure 255** Port Translation Example




See also Port Restricted Cone NAT on page 449.

## 22.4.6 Configuring The Port Forwarding Screen

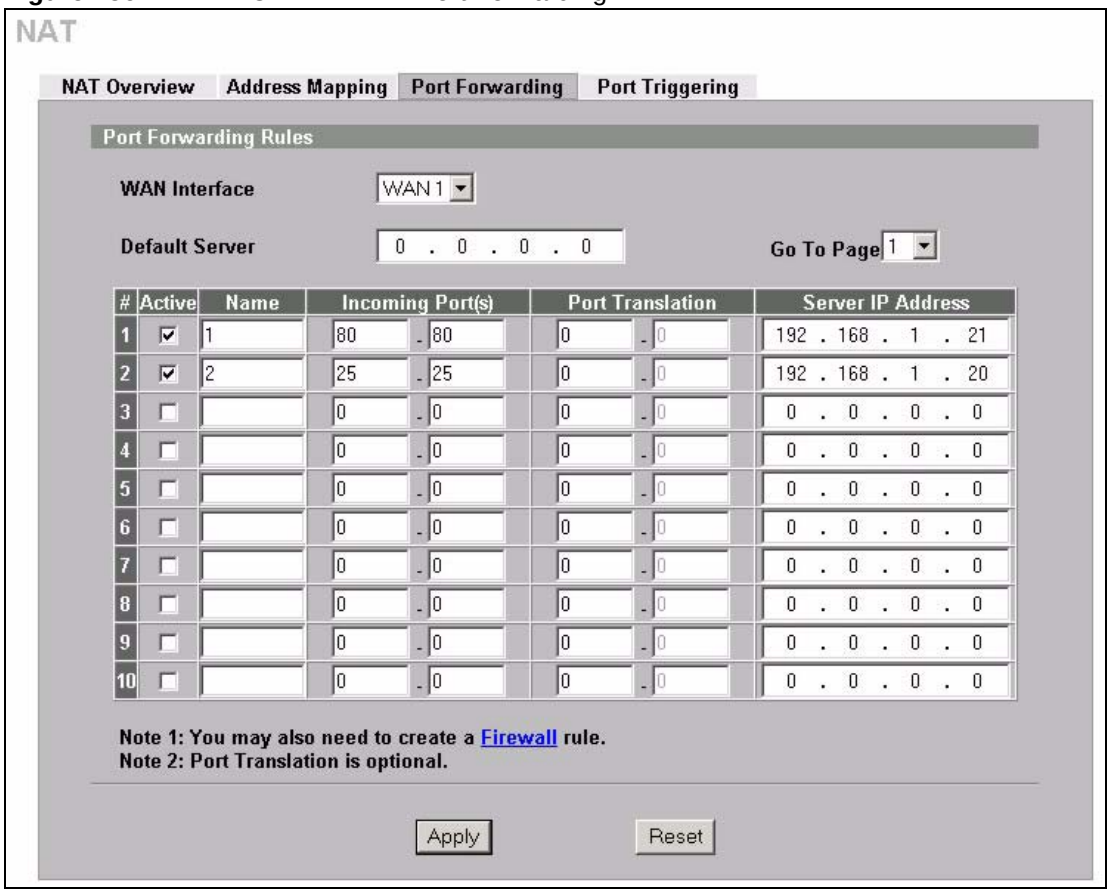
Click **ADVANCED** > **NAT** > **Port Forwarding** to open the **Port Forwarding** screen.

If you do not assign a **Default Server** IP address, the ZyWALL discards all packets received for ports that are not specified here or in the remote management setup.

Refer to Appendix B on page 783 for port numbers commonly used for particular services.

The last port forwarding rule is reserved for Roadrunner services. The rule is activated only when you set the **WAN Encapsulation** to **Ethernet** and the **Service Type** to something other than **Standard**.

**Figure 256** ADVANCED > NAT > Port Forwarding




The following table describes the labels in this screen.

**Table 133** ADVANCED > NAT > Port Forwarding

| LABEL | DESCRIPTION |
|---|---|
| WAN Interface | Select the WAN interface for which you want to view or configure address mapping rules. |
| Default Server | In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in this screen. If you do not assign a **Default Server** IP address, the ZyWALL discards all packets received for ports that are not specified here or in the remote management setup. |
| Go To Page | Choose a page from the drop-down list box to display the corresponding summary page of the port forwarding servers. |
| # | This is the number of an individual port forwarding server entry. |
| Active | Select this check box to enable the port forwarding server entry. Clear this check box to disallow forwarding of these ports to an inside server without having to delete the entry. |

**Table 133** ADVANCED > NAT > Port Forwarding

| LABEL | DESCRIPTION |
|---|---|
| Name | Enter a name to identify this port-forwarding rule. |
| Incoming Port(s) | Enter a port number here. To forward only one port, enter it again in the second field. To specify a range of ports, enter the last port to be forwarded in the second field. |
| Port Translation | Enter the port number here to which you want the ZyWALL to translate the incoming port. For a range of ports, you only need to enter the first number of the range to which you want the incoming ports translated, the ZyWALL automatically calculates the last port of the translated port range. |
| Server IP Address | Enter the inside IP address of the server here. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

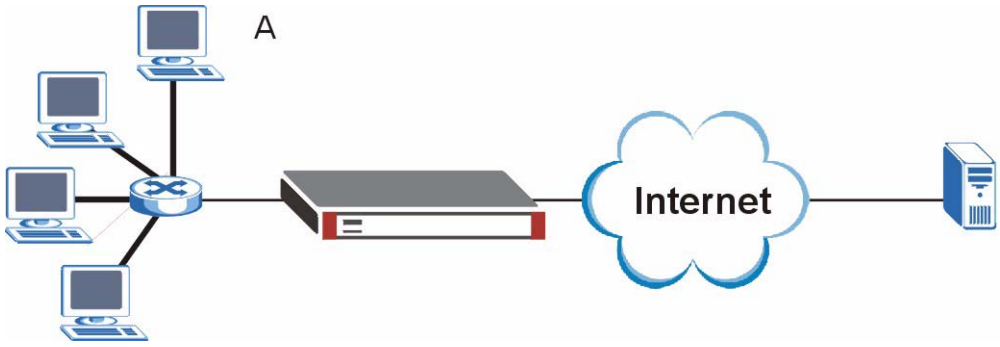
## 22.5 The Port Triggering Screen

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 a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address.

Trigger port forwarding solves this problem by allowing computers on the LAN to dynamically take turns using the service. The ZyWALL records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a "trigger" port). When the ZyWALL's WAN port receives a response with a specific port number and protocol ("incoming" port), the ZyWALL forwards the traffic to the LAN IP address of the computer that sent the request. After that computer’s connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

For example:

**Figure 257** Trigger Port Forwarding Process: Example



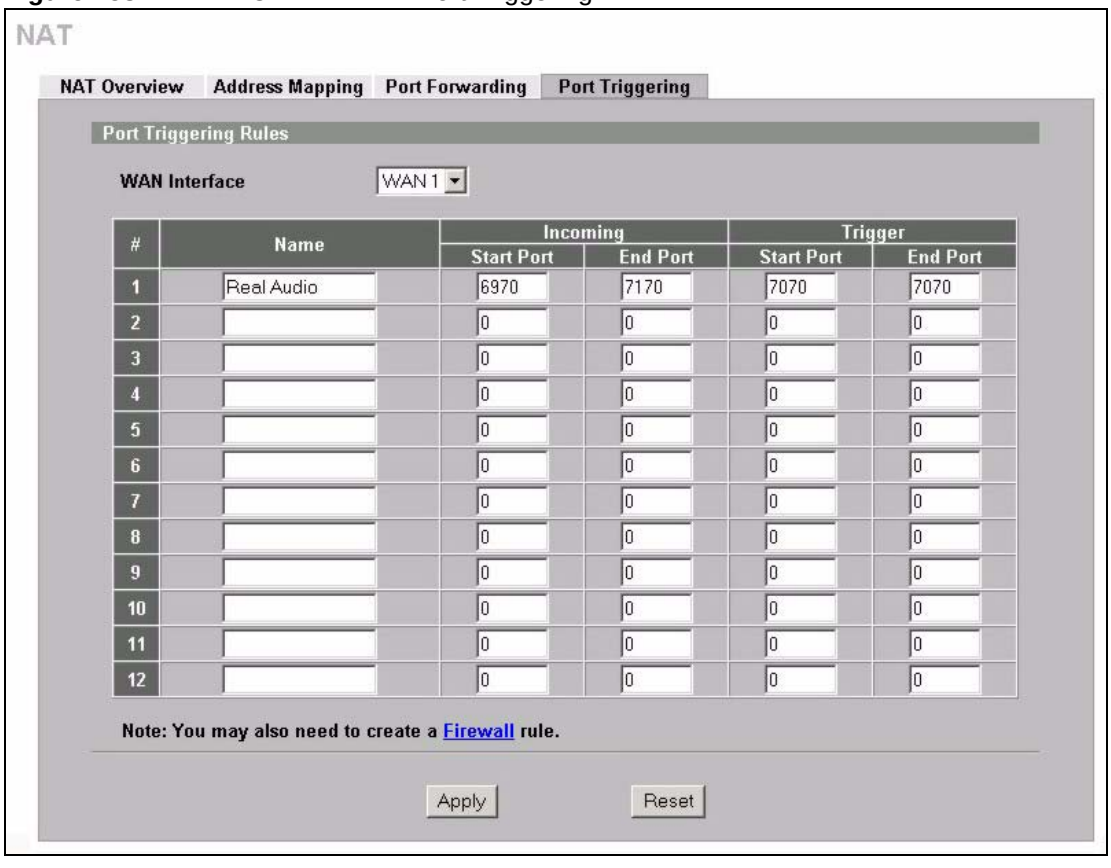

1 Jane (A) requests a file from the Real Audio server (port 7070).

2 Port 7070 is a “trigger” port and causes the ZyWALL to record Jane’s computer IP address. The ZyWALL associates Jane's computer IP address with the "incoming" port range of 6970-7170.
3 The Real Audio server responds using a port number ranging between 6970-7170.
4 The ZyWALL forwards the traffic to Jane’s computer IP address.
5 Only Jane can connect to the Real Audio server until the connection is closed or times out. The ZyWALL times out in three minutes with UDP (User Datagram Protocol) or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

## 22.5.1 Configuring Port Triggering

Click **ADVANCED** > **NAT** > **Port Triggering** to open the following screen. Use this screen to change your ZyWALL’s trigger port settings.

**Figure 258** ADVANCED > NAT > Port Triggering




The following table describes the labels in this screen.

**Table 134** ADVANCED > NAT > Port Triggering

| LABEL | DESCRIPTION |
|---|---|
| WAN Interface | Select the WAN interface for which you want to view or configure address mapping rules. |
| # | This is the rule index number (read-only). |
| Name | Type a unique name (up to 15 characters) for identification purposes. All characters are permitted - including spaces. |

**Table 134** ADVANCED > NAT > Port Triggering

| LABEL | DESCRIPTION |
|---|---|
| Incoming | Incoming is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The ZyWALL forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service. |
| Start Port | Type a port number or the starting port number in a range of port numbers. |
| End Port | Type a port number or the ending port number in a range of port numbers. |
| Trigger | The trigger port is a port (or a range of ports) that causes (or triggers) the ZyWALL to record the IP address of the LAN computer that sent the traffic to a server on the WAN. |
| Start Port | Type a port number or the starting port number in a range of port numbers. |
| End Port | Type a port number or the ending port number in a range of port numbers. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 22.6 Technical Reference

This technical reference contains the following sections:

- Inside/outside and Global/local
- What NAT Does
- How NAT Works
- NAT Application
- Port Restricted Cone NAT

## Inside/outside and Global/local

Inside/outside denotes where a host is located relative to the ZyWALL. For example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router. For example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note that inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side.

# What NAT Does

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

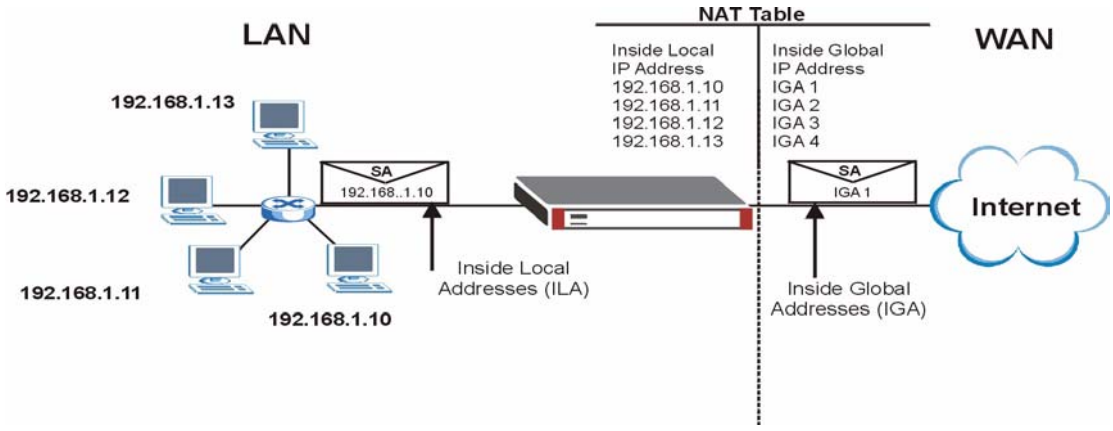
The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers (for example a web server and a telnet server) on your local network and make them accessible to the outside world. Although you can make designated servers on the LAN accessible to the outside world, it is strongly recommended that you attach those servers to the DMZ port instead. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping), NAT offers the additional benefit of firewall protection. With no servers defined, your ZyWALL filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to RFC 1631, The IP Network Address Translator (NAT).

# How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The ZyWALL keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored.

NAT never changes the IP address (either local or global) of an **outside** host.

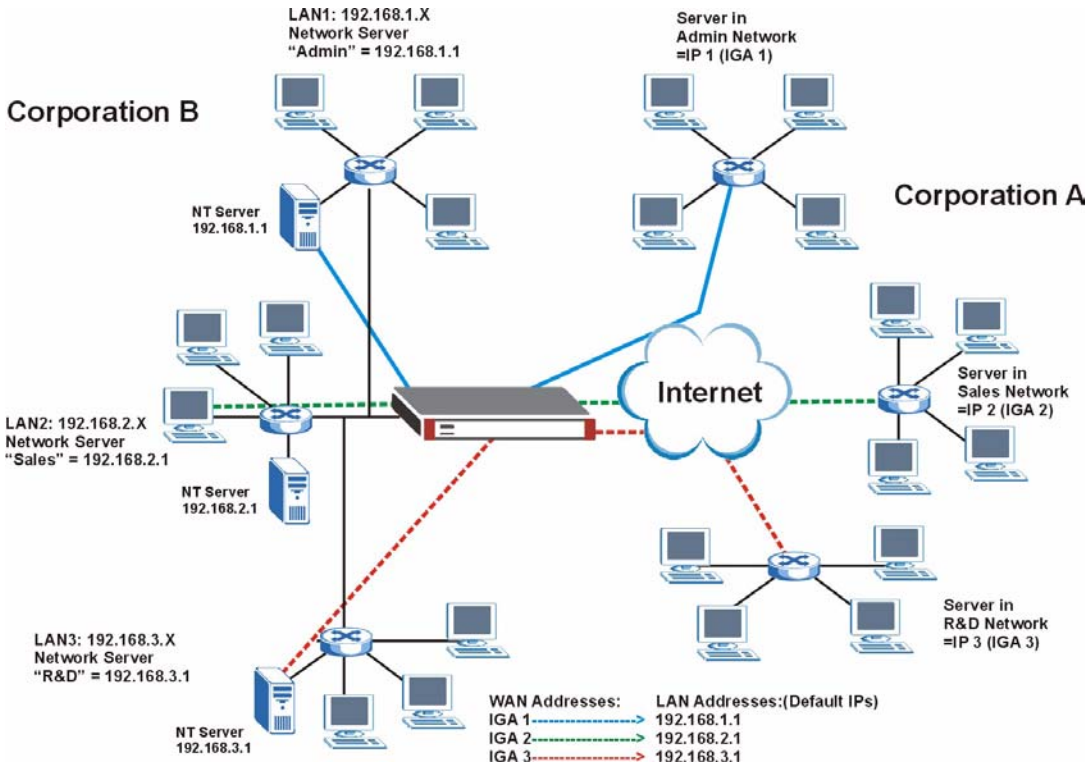
**Figure 259** NAT Overview



# NAT Application

The following figure illustrates a possible NAT application, where three inside LANs (logical LANs using IP Alias) behind the ZyWALL can communicate with three distinct WAN networks. More examples follow at the end of this chapter.

**Figure 260** NAT Application With IP Alias




# Port Restricted Cone NAT

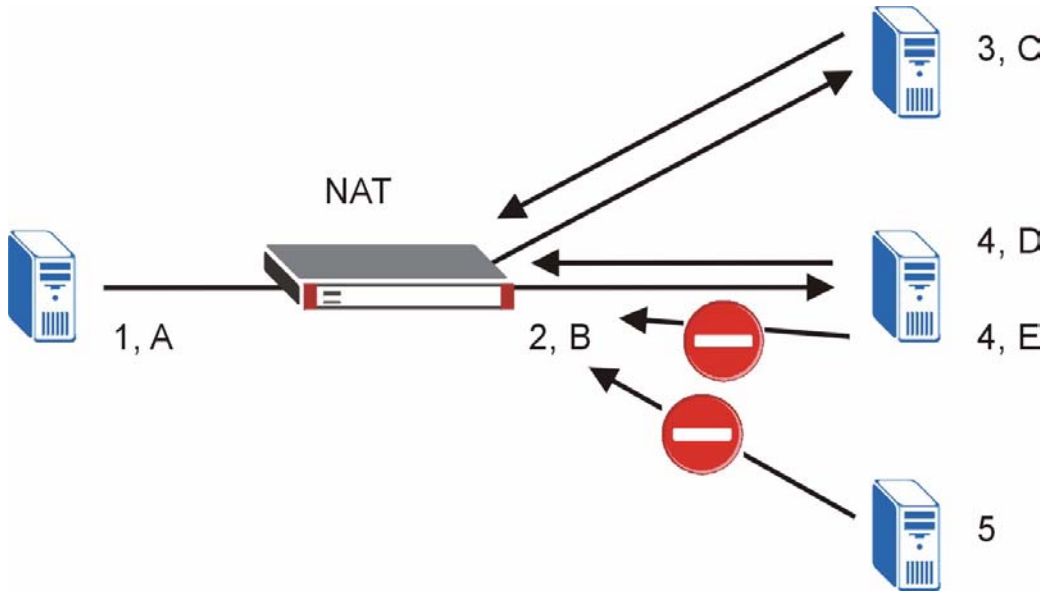
ZyWALL ZyNOS version 4.00 and later uses port restricted cone NAT. Port restricted cone NAT maps all outgoing packets from an internal IP address and port to a single IP address and port on the external network. In the following example, the ZyWALL maps the source address of all packets sent from internal IP address **1** and port **A** to IP address **2** and port **B** on the external network. A host on the external network (IP address **3** and Port **C** for example) can only send packets to the internal host if the internal host has already sent a packet to the external host's IP address and port.

A server with IP address **1** and port **A** sends packets to IP address **3**, port **C** and IP address **4**, port **D**. The ZyWALL changes the server's IP address to **2** and port to **B**.

Since **1**, **A** has already sent packets to **3**, **C** and **4**, **D,** they can send packets back to **2**, **B** and the ZyWALL will perform NAT on them and send them to the server at IP address **1**, port **A**.

Packets have not been sent from **1**, **A** to **4**, **E** or **5**, so they cannot send packets to **1**, **A**.

**Figure 261** Port Restricted Cone NAT Example



# 23

# Static Route Screens

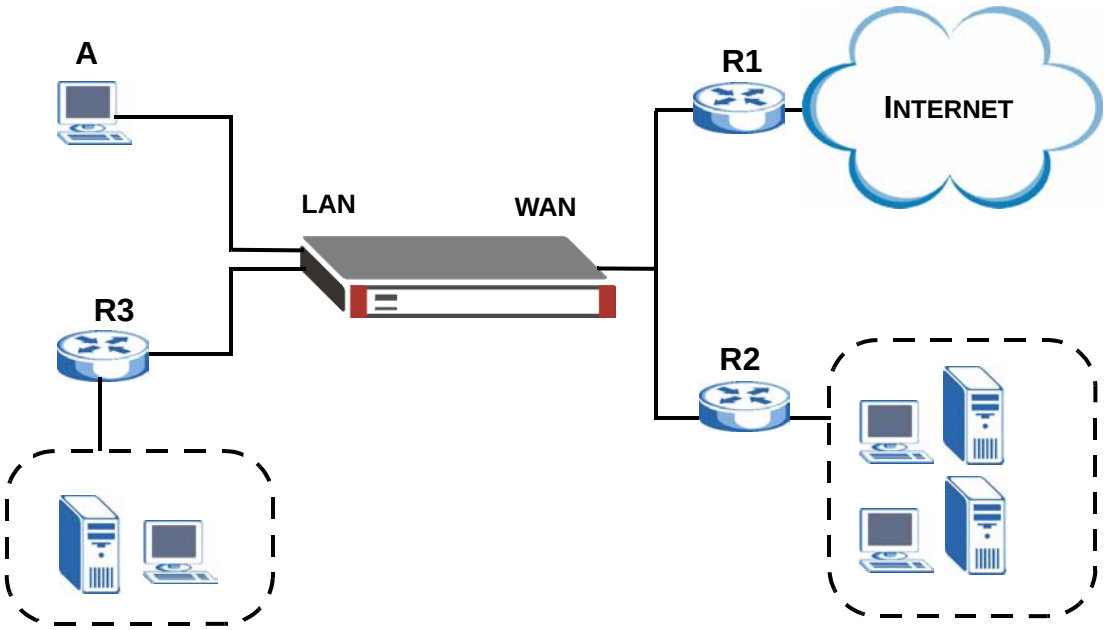
## 23.1 Overview

This chapter shows you how to configure static routes for your ZyWALL.

The ZyWALL usually uses the default gateway to route outbound traffic from local computers to the Internet. To have the ZyWALL send data to devices not reachable through the default gateway, use static routes.

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 default gateway (**R1**). You create one static route to connect to services offered by your ISP behind router **R2**. You create another static route to communicate with a separate network behind a router (**R3**) connected to the LAN.

**Figure 262** Example of Static Routing Topology




### 23.1.1 What You Can Do in the Static Route Screens

- Use the **IP Static Route** screen (Section 23.1.1 on page 451) to display the current static route entries.

- Use the **IP Static Route Edit** screen (Section 23.2.1 on page 454) to configure the required information for a static route.

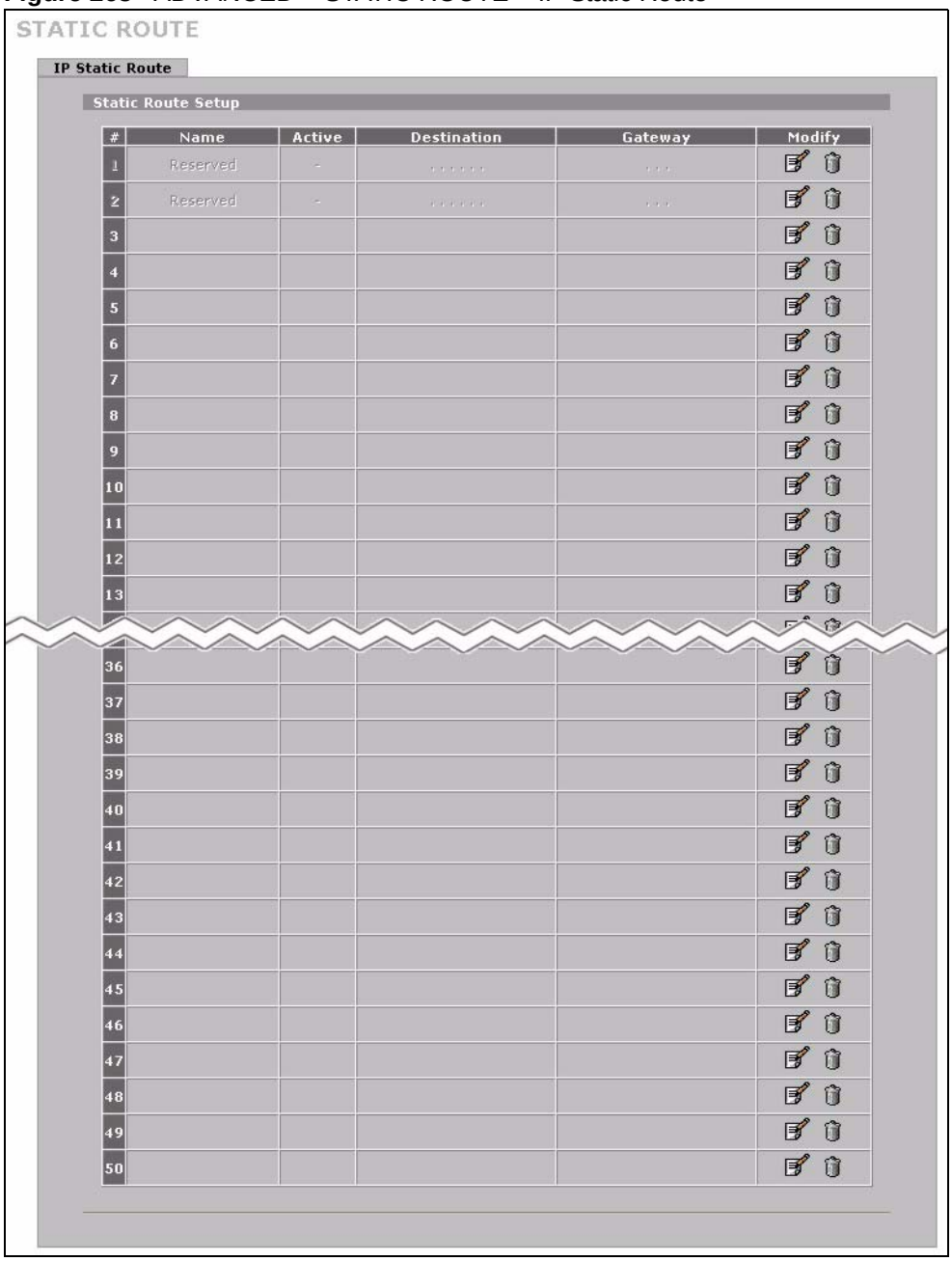
## 23.2 The IP Static Route Screen

Click **ADVANCED** > **STATIC ROUTE** to open the **IP Static Route** screen (some of the screen's blank rows are not shown).

The first two static route entries are for default WAN 1 and WAN 2 routes on a ZyWALL with multiple WAN interfaces. You cannot modify or delete a static default route.

The default route is disabled after you change the static WAN IP address to a dynamic WAN IP address.

**Figure 263** ADVANCED > STATIC ROUTE > IP Static Route




The following table describes the labels in this screen.

**Table 135** ADVANCED > STATIC ROUTE > IP Static Route

| LABEL | DESCRIPTION |
|---|---|
| # | This is the number of an individual static route. |
| Name | This is the name that describes or identifies this route. |
| Active | This field shows whether this static route is active (**Yes**) or not (**No**). |
| Destination | This parameter specifies the IP network address of the final destination. Routing is always based on network number. |

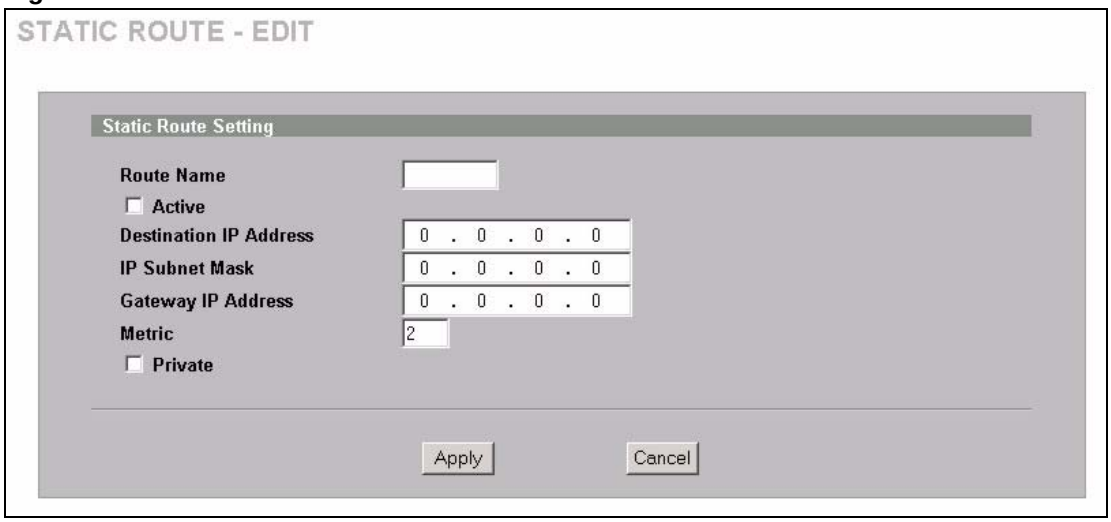
**Table 135** ADVANCED > STATIC ROUTE > IP Static Route

| LABEL | DESCRIPTION |
|---|---|
| Gateway | This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the ZyWALL's interface. The gateway helps forward packets to their destinations. |
| Modify | Click the edit icon to go to the screen where you can set up a static route on the ZyWALL.<br>Click the delete icon to remove a static route from the ZyWALL. A window displays asking you to confirm that you want to delete the route. |

## 23.2.1 The IP Static Route Edit Screen

Click the edit icon in the **IP Static Route** screen. The screen shown next appears. Use this screen to configure the required information for a static route.

**Figure 264** ADVANCED > STATIC ROUTE > IP Static Route > Edit




The following table describes the labels in this screen.

**Table 136** ADVANCED > STATIC ROUTE > IP Static Route > Edit

| LABEL | DESCRIPTION |
|---|---|
| Route Name | Enter the name of the IP static route. Leave this field blank to delete this static route. |
| Active | This field allows you to activate/deactivate this static route. |
| Destination IP Address | 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. |
| IP Subnet Mask | Enter the IP subnet mask here. |
| Gateway IP Address | Enter the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations. |
| 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 between 1 and 15. In practice, 2 or 3 is usually a good number. |

**Table 136** ADVANCED > STATIC ROUTE > IP Static Route > Edit

| LABEL | DESCRIPTION |
|---|---|
| Private | This parameter determines if the ZyWALL will include this route to a remote node in its RIP broadcasts.<br>Select this check box to keep this route private and not included in RIP broadcasts.<br>Clear this check box to propagate this route to other hosts through RIP broadcasts. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# 24

# Policy Route Screens

## 24.1 Overview

This chapter covers setting and applying policies used for IP 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.

### 24.1.1 What You Can Do in the Policy Route Screens

- Use the **Policy Route Summary** screen (Section 24.2 on page 458) to display the current policy route entries.
- Use the **Policy Route Edit** screen (Section 24.2.1 on page 460) to configure a policy route to override the default (shortest path) routing behavior and forward packets based on the criteria you specify.

### 24.1.2 What You Need To Know About Policy Route

#### Benefits

- Source-Based Routing – Network administrators can use policy-based routing to direct traffic from different users through different connections.
- Quality of Service (QoS) – Organizations can differentiate traffic by setting the precedence or ToS (Type of Service) values in the IP header at the periphery of the network to enable the backbone to prioritize traffic.
- 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.

### Routing Policy

Individual routing policies are used as part of the overall IPPR process. A policy 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 include the source address and port, IP protocol (ICMP, UDP, TCP, etc.), destination address and port, ToS and precedence (fields in the IP header) and length. The inclusion of length criterion is to differentiate between interactive and bulk traffic. Interactive applications, e.g., telnet, tend to have short packets, while bulk traffic, e.g., file transfer, tends to have large packets.

The actions that can be taken include:

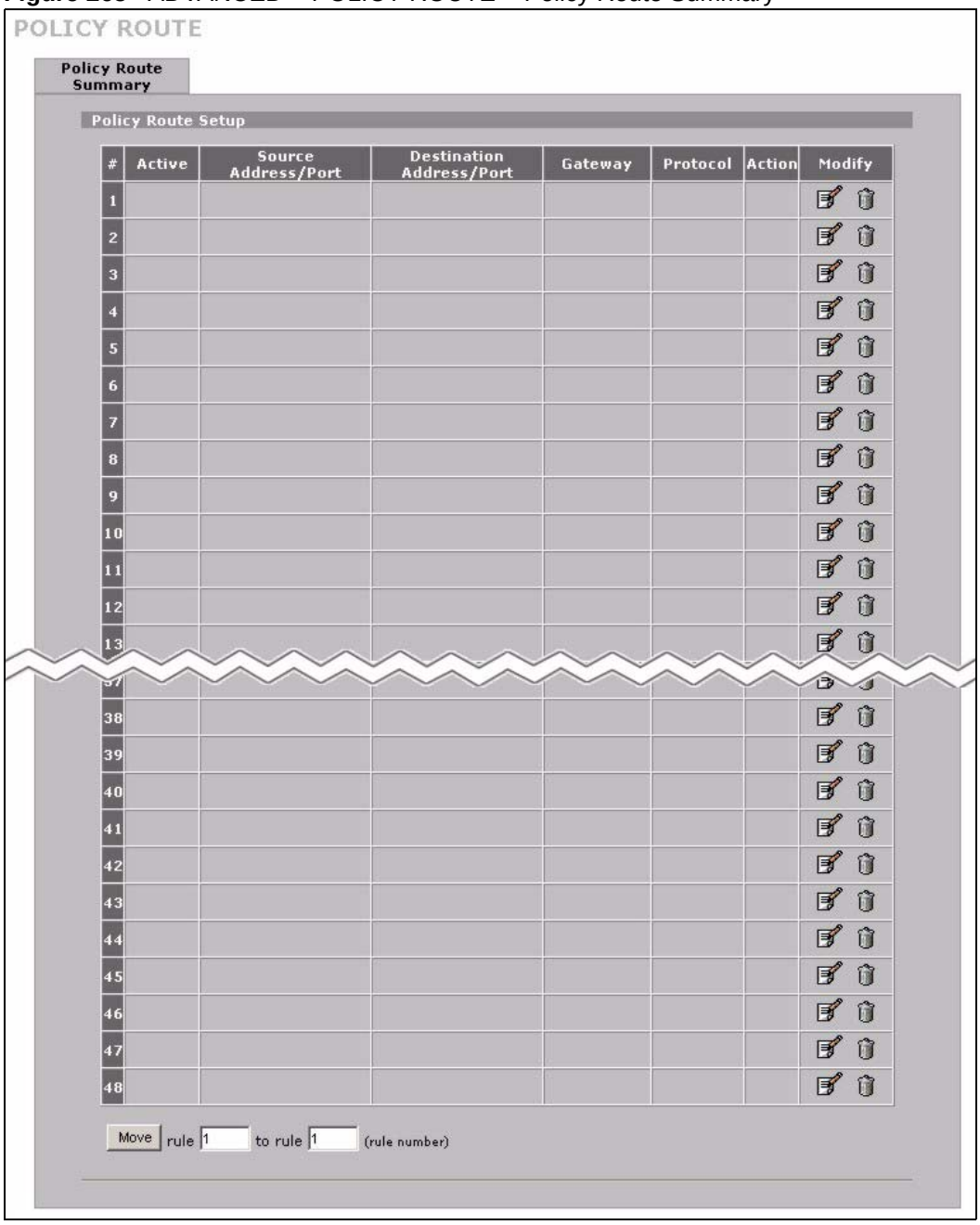
- Routing the packet to a different gateway (and hence the outgoing interface).
- Setting the ToS and precedence fields in the IP header.

IPPR follows the existing packet filtering facility of RAS in style and in implementation.

## 24.2 The Policy Route Summary Screen

Click **ADVANCED > POLICY ROUTE** to open the **Policy Route Summary** screen (some of the screen's blank rows are not shown).

**Figure 265** ADVANCED > POLICY ROUTE > Policy Route Summary




The following table describes the labels in this screen.

**Table 137** ADVANCED > POLICY ROUTE > Policy Route Summary

| LABEL | DESCRIPTION |
|---|---|
| # | This is the number of an individual policy route. |
| Active | This field shows whether the policy is active or inactive. |
| Source Address/Port | This is the source IP address range and/or port number range. |
| Destination Address/Port | This is the destination IP address range and/or port number range. |

**Table 137** ADVANCED > POLICY ROUTE > Policy Route Summary

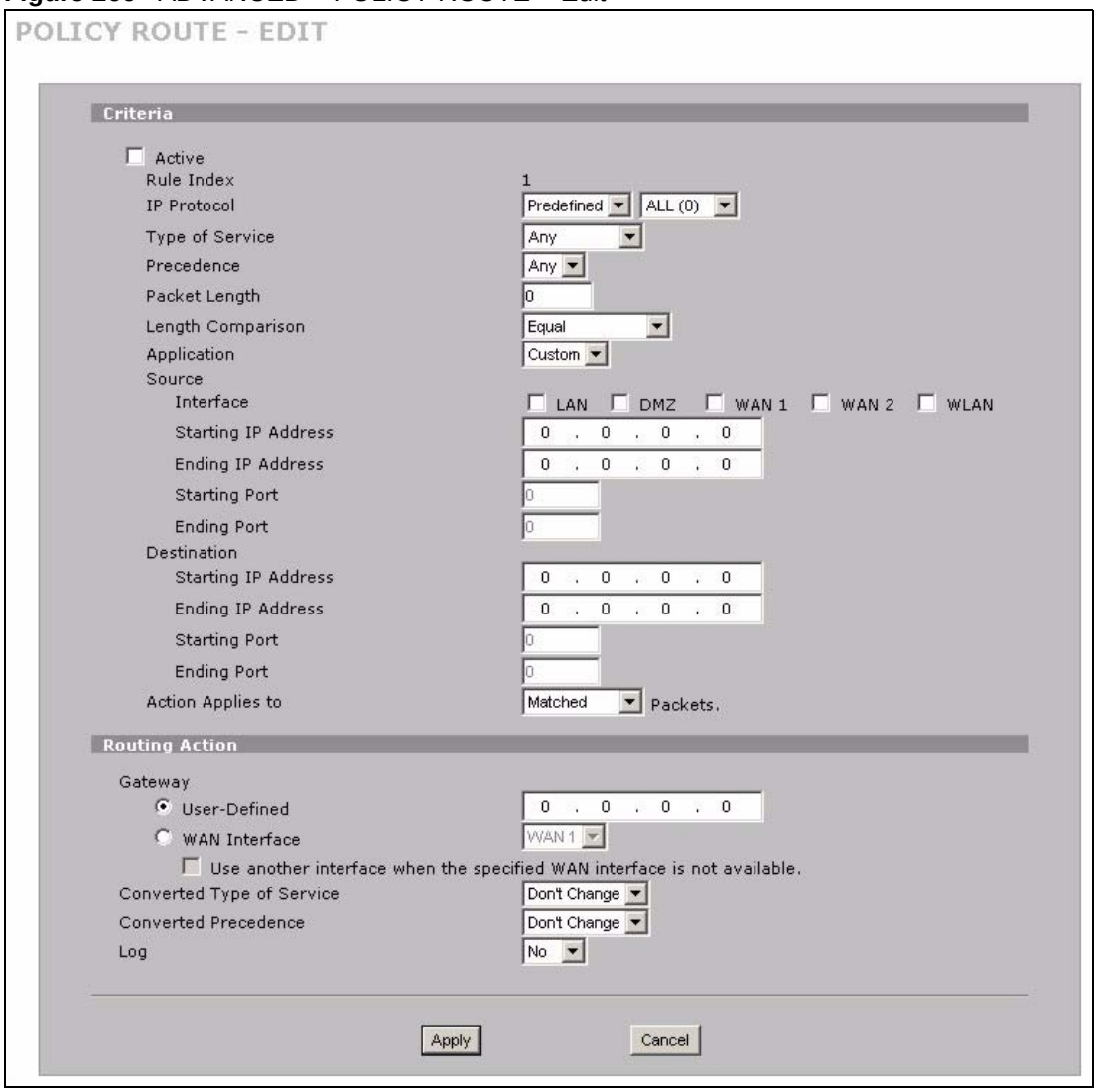
| LABEL | DESCRIPTION |
|---|---|
| Gateway | Enter the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations. |
| Protocol | This is the IP protocol and can be **ALL(0)**, **ICMP(1)**, **IGMP(2)**, **TCP(6)**, **UDP(17)**, **GRE(47)**, **ESP(50)** or **AH(51)**. |
| Action | This field specifies whether action should be taken on criteria **Matched** or **Not Matched**. |
| Modify | Click the edit icon to go to the screen where you can edit the routing policy on the ZyWALL.<br>Click the delete icon to remove an existing routing policy from the ZyWALL. A window display asking you to confirm that you want to delete the routing policy. |
| Move | Type a policy route's index number and the number for where you want to put that rule. Click **Move** 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. |

## 24.2.1 The Policy Route Edit Screen

Click **ADVANCED** > **POLICY ROUTE** to open the **Policy Route Summary** screen. Then click the edit icon to open the **Edit IP Policy Route** screen. WAN 2 refers to either the physical WAN 2 port on the ZyWALL with multiple WAN ports or the 3G card on the supported ZyWALL in router mode. Not all fields are available on all models.

Use this screen to configure a policy route to override the default (shortest path) routing behavior and forward packets based on the criteria you specify. 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. Policy-based routing is applied to incoming packets on a per interface basis before normal routing. The ZyWALL does not perform normal routing on packets that match any of the policy routes.

**Figure 266** ADVANCED > POLICY ROUTE > Edit




The following table describes the labels in this screen.

**Table 138** ADVANCED > POLICY ROUTE > Edit

| LABEL | DESCRIPTION |
|---|---|
| Criteria | |
| Active | Select the check box to activate the policy. |
| Rule Index | This is the index number of the policy route. |
| IP Protocol | Select **Predefined** and then the IP protocol from **ALL(0)**, **ICMP(1)**, **IGMP(2)**, **TCP(6)**, **UDP(17)**, **GRE(47)**, **ESP(50)** or **AH(51)**.<br>Otherwise, select **Custom** and enter a number from 0 to 255. |
| Type of Service | Prioritize incoming network traffic by choosing from **Any**, **Normal**, **Min Delay**, **Max Thruput**, **Max Reliable** or **Mix Cost**. |
| Precedence | Precedence value of the incoming packet. Select a value from **0** to **7** or **Any**. |
| Packet Length | Type a length of packet (in bytes). The operators in the **Length Comparison** field apply to incoming packets of this length. |

**Table 138** ADVANCED > POLICY ROUTE > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Length Comparison | Choose from **Equal**, **Not Equal**, **Less**, **Greater**, **Less or Equal** or **Greater or Equal**. |
| Application | Select a predefined application (**FTP**, **H.323** or **SIP**) for the policy rule. If you do not want to use a predefined application, select **Custom**. You can also configure the source and destination port numbers if you set **IP protocol** to **TCP** or **UDP**.<br>**FTP** (File Transfer Program) is a program to enable fast transfer of files, including large files that may not be possible by e-mail. Select **FTP** to configure the policy rule for TCP packets with a port 21 destination.<br>**H.323** is a protocol used for multimedia communications over networks, for example NetMeeting. Select **H.323** to configure the policy rule for TCP packets with a port 1720 destination.<br>Note: If you select **H.323**, make sure you also use the **ALG** screen to turn on the H.323 ALG.<br>**SIP** (Session Initiation Protocol) is a signaling protocol used in Internet telephony, instant messaging, events notification and conferencing. The ZyWALL supports SIP traffic pass-through. Select **SIP** to configure the policy rule for UDP packets with a port 5060 destination.<br>Note: If you select **SIP**, make sure you also use the **ALG** screen to turn on the SIP ALG. |
| Source | |
| Interface | Use the check box to select **LAN**, **DMZ**, **WAN 1**, **WAN 2** and/or **WLAN**. |
| Starting IP Address | Enter the source starting IP address. |
| Ending IP Address | Enter the source ending IP address. |
| Starting Port | Enter the source starting port number. This field is applicable only when you select **TCP** or **UDP** in the **IP Protocol** field and **Custom** in the **Application** field. |
| Ending Port | Enter the source ending port number. This field is applicable only when you select **TCP** or **UDP** in the **IP Protocol** field and **Custom** in the **Application** field. |
| Destination | |
| Starting IP Address | Enter the destination starting IP address. |
| Ending IP Address | Enter the destination ending IP address. |
| Starting Port | Enter the destination starting port number. This field is applicable only when you select **TCP** or **UDP** in the **IP Protocol** field and **Custom** in the **Application** field. |
| Ending Port | Enter the destination ending port number. This field is applicable only when you select **TCP** or **UDP** in the **IP Protocol** field and **Custom** in the **Application** field. |
| Action Applies to | Specifies whether action should be taken on criteria **Matched** or **Not Matched**. |
| Routing Action | |

**Table 138** ADVANCED > POLICY ROUTE > Edit (continued)

| LABEL | DESCRIPTION |
|---|---|
| Gateway | Select **User-Defined** and enter the IP address of the gateway if you want to specify the IP address of the gateway. The gateway is an immediate neighbor of your ZyWALL that will forward the packet to the destination. The gateway must be a router on the same segment as your ZyWALL's LAN or WAN interface.<br>Select **WAN Interface** to have the ZyWALL send traffic that matches the policy route through a specific WAN interface. Select the WAN interface from the drop-down list box.<br>Select the **Use another interface when the specified WAN interface is not available.** check box to have the ZyWALL send traffic that matches the policy route through the other WAN interface if it cannot send the traffic through the WAN interface you selected. This option is only available when you select **WAN Interface**. |
| Converted Type of Service | Set the new TOS value of the outgoing packet. Prioritize incoming network traffic by choosing **Don't Change**, **Normal**, **Min Delay**, **Max Thruput**, **Max Reliable** or **Min Cost**. |
| Converted Precedence | Set the new outgoing packet precedence value. Values are **0** to **7** or **Don't Change**. |
| Log | Select **Yes** from the drop-down list box to make an entry in the system log when a policy is executed. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving. |

# 25

# Bandwidth Management Screens

## 25.1 Overview

Bandwidth management allows you to allocate an interface's outgoing capacity to specific types of traffic. It can also help you make sure that the ZyWALL forwards certain types of traffic, such as Voice-over-IP (VoIP), with minimum delay.

Bandwidth management addresses questions such as:

- Who gets how much access to specific applications?
- What priority level should you give to each type of traffic?
- Which traffic must have guaranteed delivery?
- How much bandwidth should be allotted to guarantee delivery?

Bandwidth management also allows you to configure the allowed output for an interface to match what the network can handle. This helps reduce delays and dropped packets at the next routing device. For example, you can set the WAN interface speed to 1024 kbps (or less) if the broadband device connected to the WAN port has an upstream speed of 1024 kbps.

### 25.1.1 What You Can Do in the Bandwidth Management Screens

- Use the **Summary** screen (Section 25.2 on page 467) to enable bandwidth management on an interface and set the maximum allowed bandwidth for that interface.
- Use the **Class Setup** screen (Section 25.3 on page 471) to view the configured bandwidth classes by individual interface and to set up a bandwidth class's name, bandwidth allotment, and bandwidth filter.
- Use the **Monitor** screen (Section 25.6 on page 478) to view the device's bandwidth usage and allotments.

### 25.1.2 What You Need to Know About Bandwidth Management

#### Bandwidth Classes and Filters

Use bandwidth classes and sub-classes to allocate specific amounts of bandwidth capacity (bandwidth budgets). Configure a bandwidth filter to define a bandwidth class (or sub-class) based on a specific application and/or subnet.

### Proportional Bandwidth Allocation

Bandwidth management allows you to define how much bandwidth each class gets; however, the actual bandwidth allotted to each class decreases or increases in proportion to actual available bandwidth.

### Application-based Bandwidth Management

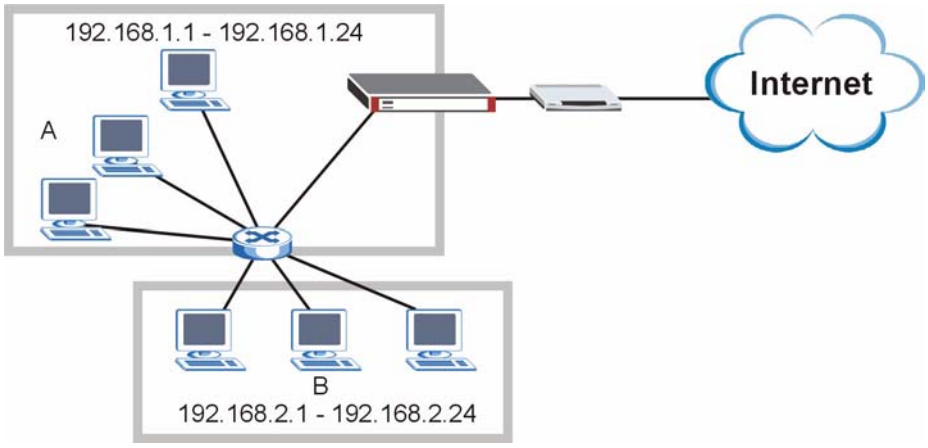
You can create bandwidth classes based on individual applications (like VoIP, Web, FTP, E-mail and Video for example).

### Subnet-based Bandwidth Management

You can create bandwidth classes based on subnets.

The following figure shows LAN subnets. You could configure one bandwidth class for subnet A and another for subnet B.

**Figure 267** Subnet-based Bandwidth Management Example




## 25.1.3 Application and Subnet-based Bandwidth Management Example

You could also create bandwidth classes based on a combination of a subnet and an application. The following example table shows bandwidth allocations for application specific traffic from separate LAN subnets.

**Table 139** Application and Subnet-based Bandwidth Management Example

| TRAFFIC TYPE | FROM SUBNET A | FROM SUBNET B |
|---|---|---|
| VoIP | 64 Kbps | 64 Kbps |
| Web | 64 Kbps | 64 Kbps |
| FTP | 64 Kbps | 64 Kbps |
| E-mail | 64 Kbps | 64 Kbps |
| Video | 64 Kbps | 64 Kbps |

### 25.1.4 Over Allotment of Bandwidth Example

It is possible to set the bandwidth management speed for an interface higher than the interface's actual transmission speed. Higher priority traffic gets to use up to its allocated bandwidth, even if it takes up all of the interface's available bandwidth. This could stop lower priority traffic from being sent. The following is an example.

**Table 140** Over Allotment of Bandwidth Example

| BANDWIDTH CLASSES, ALLOTMENTS | | PRIORITIES |
|---|---|---|
| Actual outgoing bandwidth available on the interface: 1000 kbps | | |
| Root Class: 1500 kbps (same as Speed setting) | VoIP traffic (Service = SIP): 500 Kbps | 7 |
| | OpenPhone traffic (Service = H.323): 500 kbps | 7 |
| | FTP (Service = FTP): 500 Kbps | 3 |

If you use VoIP and OpenPhone at the same time, the device allocates up to 500 Kbps of bandwidth to each of them before it allocates any bandwidth to FTP. As a result, FTP can only use bandwidth when VoIP and OpenPhone do not use all of their allocated bandwidth.

Suppose you try to browse the web too. In this case, VoIP, OpenPhone and FTP all have higher priority, so they get to use the bandwidth first. You can only browse the web when VoIP, OpenPhone, and FTP do not use all 1000 Kbps of available bandwidth.

### 25.1.5 Maximize Bandwidth Usage With Bandwidth Borrowing Example

If you configure both maximize bandwidth usage (on the interface) and bandwidth borrowing (on individual sub-classes), the ZyWALL functions as follows.

1. The ZyWALL sends traffic according to each bandwidth class's bandwidth budget.
2. The ZyWALL assigns a parent class's unused bandwidth to its sub-classes that have more traffic than their budgets and have bandwidth borrowing enabled. The ZyWALL gives priority to sub-classes of higher priority and treats classes of the same priority equally.
3. The ZyWALL assigns any remaining unused or unbudgeted bandwidth on the interface to any class that requires it. The ZyWALL gives priority to classes of higher priority and treats classes of the same level equally.
4. If the bandwidth requirements of all of the traffic classes are met and there is still some unbudgeted bandwidth, the ZyWALL assigns it to traffic that does not match any of the classes.

## 25.2 The Summary Screen

Click **ADVANCED > BW MGMT** to open the **Summary** screen. Use this screen to enable and configure bandwidth management on different bandwidth classes.

#### Bandwidth Class

Enable bandwidth management on an interface and set the maximum allowed bandwidth for that interface.

You can configure up to one bandwidth filter per bandwidth class. You can also configure bandwidth classes without bandwidth filters. However, it is recommended that you configure sub-classes with filters for any classes that you configure without filters. The ZyWALL leaves the bandwidth budget allocated and unused for a class that does not have a filter or sub-classes with filters.

The total of the configured bandwidth budgets for sub-classes cannot exceed the configured bandwidth budget speed of the parent class.

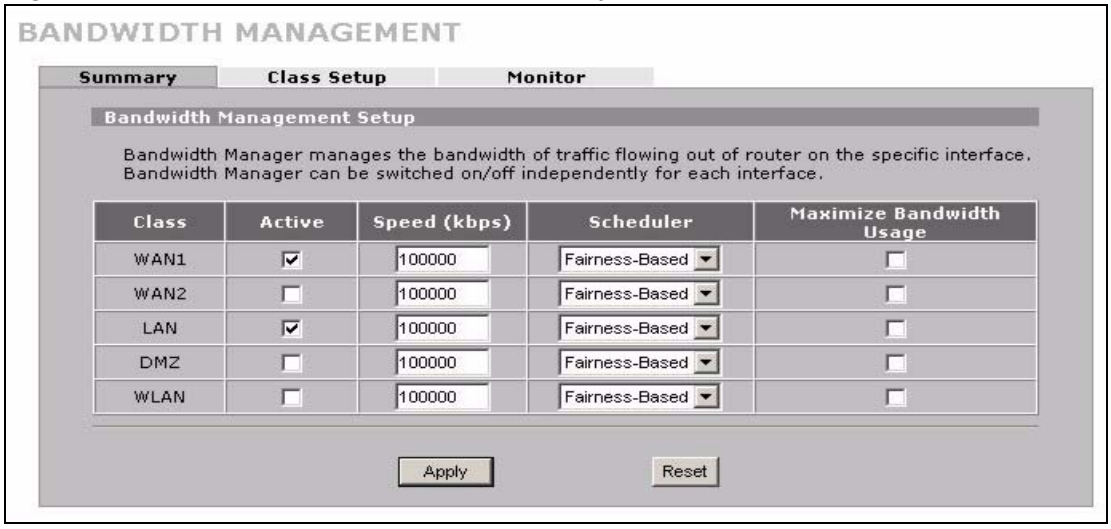
### Maximize Bandwidth Usage

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 class is not using) among the bandwidth classes that require more bandwidth.

When you enable maximize bandwidth usage, the ZyWALL first makes sure that each bandwidth class gets up to its bandwidth allotment. Next, the ZyWALL divides up an interface's available bandwidth (bandwidth that is unbudgeted or unused by the classes) depending on how many bandwidth classes require more bandwidth and on their priority levels. When only one class requires more bandwidth, the ZyWALL gives extra bandwidth to that class.

When multiple classes require more bandwidth, the ZyWALL gives the highest priority classes the available bandwidth first (as much as they require, if there is enough available bandwidth), and then to lower priority classes if there is still bandwidth available. The ZyWALL distributes the available bandwidth equally among classes with the same priority level.

**Figure 268** ADVANCED > BW MGMT > Summary



The following table describes the labels in this screen.

**Table 141** ADVANCED > BW MGMT > Summary

| LABEL | DESCRIPTION |
|---|---|
| Class | These read-only labels represent the physical interfaces. Select an interface's check box to enable bandwidth management on that interface. Bandwidth management applies to all traffic flowing out of the router through the interface, regardless of the traffic's source.<br><br>Note: The WLAN class refers to the Ethernet interfaces in the WLAN port role. The ZyWALL does not apply bandwidth management to an installed wireless card's traffic.<br><br>Traffic redirect or IP alias may cause LAN-to-LAN or DMZ-to-DMZ traffic to pass through the ZyWALL and be managed by bandwidth management. |
| Active | Select an interface's check box to enable bandwidth management on that interface. |
| Speed (kbps) | Enter the amount of bandwidth for this interface that you want to allocate using bandwidth management. This appears as the bandwidth budget of the interface's root class (see Section 25.3 on page 471). The recommendation is to set this speed to match what the device connected to the port can handle. For example, set the WAN interface speed to 1000 kbps if the broadband device connected to the WAN port has an upstream speed of 1000 kbps.<br>The recommendation is to set this speed to match the interface's actual transmission speed. For example, set the WAN interface speed to 1000 kbps if your Internet connection has an upstream transmission speed of 1 Mbps.<br>You can set this number higher than the interface's actual transmission speed. This will stop lower priority traffic from being sent if higher priority traffic uses all of the actual bandwidth.<br>You can also set this number lower than the interface's actual transmission speed. If you do not enable **Max Bandwidth Usage**, this will cause the ZyWALL to not use some of the interface's available bandwidth. |
| Scheduler | Select either **Priority-Based** or **Fairness-Based** from the drop-down menu to control the traffic flow.<br>Select **Priority-Based** to give preference to bandwidth classes with higher priorities. With the priority-based scheduler, the ZyWALL forwards traffic from bandwidth classes according to the priorities that you assign to the bandwidth classes. The larger a bandwidth class's priority number is, the higher the priority. Assign real-time applications (like those using audio or video) a higher priority number to provide smoother operation.<br>Select **Fairness-Based** to treat all bandwidth classes equally. The ZyWALL divides bandwidth equally among bandwidth classes when using the fairness-based scheduler; thus preventing one bandwidth class from using all of the interface's bandwidth. |
| 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 bandwidth classes that require bandwidth. Do not select this if you want to reserve bandwidth for traffic that does not match a bandwidth class (see Section 25.1.5 on page 467) or you want to limit the speed of this interface (see the **Speed** field description). |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 25.2.1 Maximize Bandwidth Usage Example

Here is an example of a ZyWALL that has maximize bandwidth usage enabled on an interface. The following table shows each bandwidth class's bandwidth budget. The classes are set up based on subnets. The interface is set to 10240 kbps. Each subnet is allocated 2048 kbps. The unbudgeted 2048 kbps allows traffic not defined in any of the bandwidth filters to go out when you do not select the maximize bandwidth option.

**Table 142** Maximize Bandwidth Usage Example

| BANDWIDTH CLASSES AND ALLOTMENTS | |
|---|---|
| Root Class: 10240 kbps | Administration: 2048 kbps |
| | Sales: 2048 kbps |
| | Marketing: 2048 kbps |
| | Research: 2048 kbps |

The ZyWALL divides up the unbudgeted 2048 kbps among the classes that require more bandwidth. If the administration department only uses 1024 kbps of the budgeted 2048 kbps, the ZyWALL also divides the remaining 1024 kbps among the classes that require more bandwidth. Therefore, the ZyWALL divides a total of 3072 kbps of unbudgeted and unused bandwidth among the classes that require more bandwidth.

### 25.2.1.1 Priority-based Allotment of Unused and Unbudgeted Bandwidth

The following table shows the priorities of the bandwidth classes and the amount of bandwidth that each class gets.

**Table 143** Priority-based Allotment of Unused and Unbudgeted Bandwidth Example

| BANDWIDTH CLASSES, PRIORITIES AND ALLOTMENTS | |
|---|---|
| Root Class: 10240 kbps | Administration: Priority 4, 1024 kbps |
| | Sales: Priority 6, 3584 kbps |
| | Marketing: Priority 6, 3584 kbps |
| | Research: Priority 5, 2048 kbps |

Suppose that all of the classes except for the administration class need more bandwidth.

- Each class gets up to its budgeted bandwidth. The administration class only uses 1024 kbps of its budgeted 2048 kbps.
- The sales and marketing are first to get extra bandwidth because they have the highest priority (6). If they each require 1536 kbps or more of extra bandwidth, the ZyWALL divides the total 3072 kbps total of unbudgeted and unused bandwidth equally between the sales and marketing departments (1536 kbps extra to each for a total of 3584 kbps for each) because they both have the highest priority level.
- Research requires more bandwidth but only gets its budgeted 2048 kbps because all of the unbudgeted and unused bandwidth goes to the higher priority sales and marketing classes.

#### 25.2.1.2 Fairness-based Allotment of Unused and Unbudgeted Bandwidth

The following table shows the amount of bandwidth that each class gets.

**Table 144** Fairness-based Allotment of Unused and Unbudgeted Bandwidth Example

| BANDWIDTH CLASSES AND ALLOTMENTS | |
|---|---|
| Root Class: 10240 kbps | Administration: 1024 kbps |
| | Sales: 3072 kbps |
| | Marketing: 3072 kbps |
| | Research: 3072 kbps |

Suppose that all of the classes except for the administration class need more bandwidth.

- Each class gets up to its budgeted bandwidth. The administration class only uses 1024 kbps of its budgeted 2048 kbps.
- The ZyWALL divides the total 3072 kbps total of unbudgeted and unused bandwidth equally among the other classes. 1024 kbps extra goes to each so the other classes each get a total of 3072 kbps.

### 25.2.2 Reserving Bandwidth for Non-Bandwidth Class Traffic

Do the following three steps to configure the ZyWALL to allow bandwidth for traffic that is not defined in a bandwidth filter.

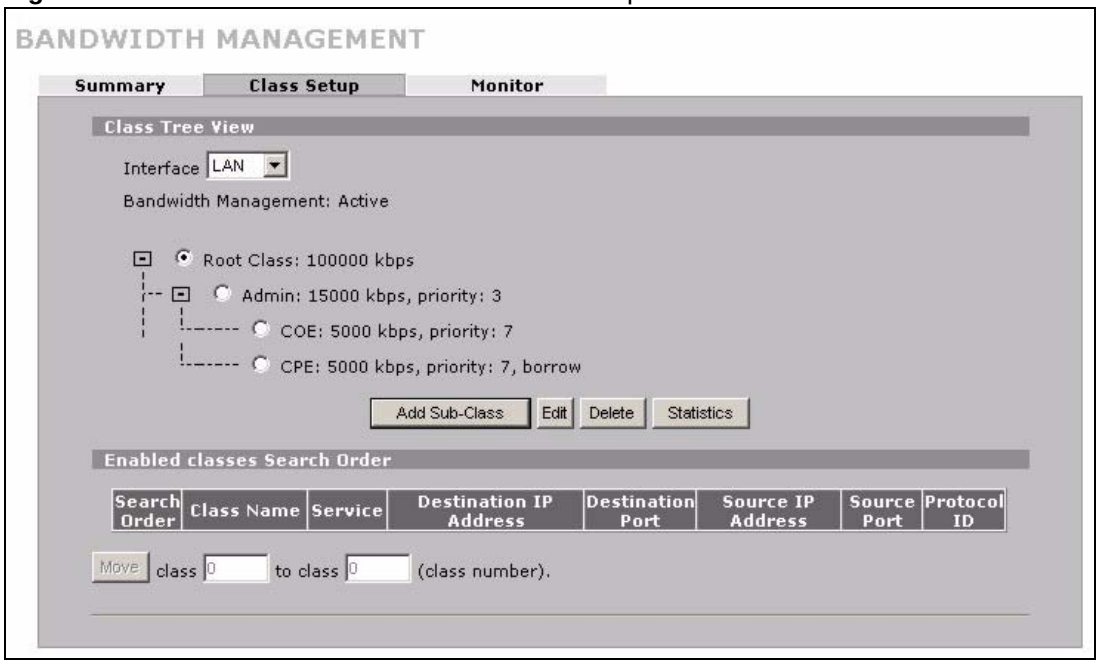
1. Leave some of the interface's bandwidth unbudgeted.
2. Do not enable the interface's **Maximize Bandwidth Usage** option.
3. Do not enable bandwidth borrowing on the sub-classes that have the root class as their parent (see Section 25.3 on page 471).

## 25.3 The Class Setup Screen

The **Class Setup** screen displays the configured bandwidth classes by individual interface. Select an interface and click the buttons to perform the actions described next. Click "+" to expand the class tree or click "-" to collapse the class tree. Each interface has a permanent root class. The bandwidth budget of the root class is equal to the speed you configured on the interface (see Section 25.2 on page 467 to configure the speed of the interface). Configure sub-class layers for the root class.

To add or delete child classes on an interface, click **ADVANCED** > **BW MGMT** > **Class Setup**. The screen is shown here with example classes.

**Figure 269** ADVANCED > BW MGMT > Class Setup




The following table describes the labels in this screen.

**Table 145** ADVANCED > BW MGMT > Class Setup

| LABEL | DESCRIPTION |
|---|---|
| Interface | Select an interface for which you want to set up bandwidth management classes.<br>Bandwidth management controls outgoing traffic on an interface, not incoming. So, in order to limit the download bandwidth of the LAN users, set the bandwidth management class on the LAN. In order to limit the upload bandwidth, set the bandwidth management class on the corresponding WAN interface. |
| Bandwidth Management | This field displays whether bandwidth management on the interface you selected in the field above is enabled (**Active**) or not (**Inactive**). |
| | After you select an interface, the bandwidth management classes configured for the interface display. The name, bandwidth and priority display for each class. “borrow” also displays if the class is set to use bandwidth from its parent class if the parent class is not using up its bandwidth budget. |
| Add Sub-Class | Click **Add Sub-class** to add a sub-class. |
| Edit | Click **Edit** to configure the selected class. You cannot edit the root class. |
| Delete | Click **Delete** to delete the class and all its sub-classes. You cannot delete the root class. |
| Statistics | Click **Statistics** to display the status of the selected class. |
| Enabled classes Search Order | This list displays the interface’s active bandwidth management classes (the ones that have the bandwidth filter enabled). The ZyWALL applies the classes in the order that they appear here. Once a connection matches a bandwidth management class, the ZyWALL applies the class’s rules and does not check the connection against any other bandwidth management classes. |
| Search Order | This is the index number of an individual bandwidth management class. |
| Class Name | This is the name that identifies a bandwidth management class. |
| Service | This is the service that this bandwidth management class is configured to manage. |
| Destination IP Address | This is the destination IP address for connections to which this bandwidth management class applies. |

**Table 145** ADVANCED > BW MGMT > Class Setup (continued)

| LABEL | DESCRIPTION |
|---|---|
| Destination Port | This is the destination port for connections to which this bandwidth management class applies. |
| Source IP Address | This is the source IP address for connections to which this bandwidth management class applies. |
| Source Port | This is the source port for connections to which this bandwidth management class applies. |
| Protocol ID | This is the protocol ID (service type) number for connections to which this bandwidth management class applies. For example: 1 for ICMP, 6 for TCP or 17 for UDP. |
| Move | Type a class's index number and the number for where you want to put that class. Click **Move** to move the class to the number that you typed. The ordering of your classes is important as they are applied in order of their numbering. |

## 25.4 Bandwidth Manager Class Configuration

Configure a bandwidth management class in the **Class Setup** screen. You must use the **Summary** screen to enable bandwidth management on an interface before you can configure classes for that interface.

### Bandwidth Borrowing

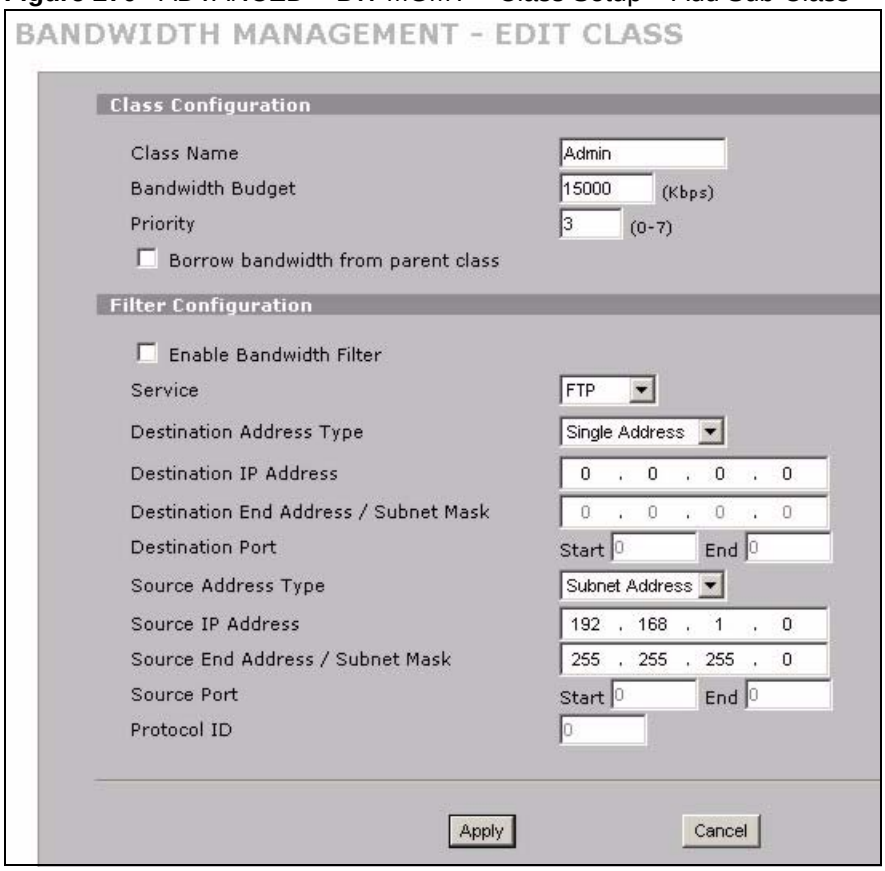
Bandwidth borrowing allows a sub-class to borrow unused bandwidth from its parent class, whereas maximize bandwidth usage allows bandwidth classes to borrow any unused or unbudgeted bandwidth on the whole interface.

Enable bandwidth borrowing on a sub-class to allow the sub-class to use its parent class's unused bandwidth. A parent class's unused bandwidth is given to the highest priority sub-class first. The sub-class can also borrow bandwidth from a higher parent class (grandparent class) if the sub-class's parent class is also configured to borrow bandwidth from its parent class. This can go on for as many levels as are configured to borrow bandwidth from their parent class (see Section 25.4.1 on page 476).

The total of the bandwidth allotments for sub-classes cannot exceed the bandwidth allotment of their parent class. The ZyWALL uses the scheduler to divide a parent class's unused bandwidth among the sub-classes.

Click **ADVANCED** > **BW MGMT** > **Class Setup** > **Add Sub-Class** or **Edit** to open the following screen. Use this screen to add a child class.

**Figure 270** ADVANCED > BW MGMT > Class Setup > Add Sub-Class




The following table describes the labels in this screen.

**Table 146** ADVANCED > BW MGMT > Class Setup > Add Sub-Class

| LABEL | DESCRIPTION |
|---|---|
| Class Configuration | |
| Class Name | Use the auto-generated name or enter a descriptive name of up to 20 alphanumeric characters, including spaces. |
| Bandwidth Budget (kbps) | Specify the maximum bandwidth allowed for the class in kbps. The recommendation is a setting between 20 kbps and 20000 kbps for an individual class. |
| Priority | Enter a number between 0 and 7 to set the priority of this class. The higher the number, the higher the priority. The default setting is 3. |
| Borrow bandwidth from parent class | Select this option to allow a sub-class to borrow bandwidth from its parent class if the parent class is not using up its bandwidth budget.<br>Bandwidth borrowing is governed by the priority of the sub-classes. That is, a sub-class with the highest priority (7) is the first to borrow bandwidth from its parent class.<br>Do not select this for the classes directly below the root class if you want to leave bandwidth available for other traffic types (see Section 25.1.5 on page 467) or you want to set the interface's speed to match what the next device in network can handle (see the **Speed** field description in Table 141 on page 469). |
| Filter Configuration | |

**Table 146** ADVANCED > BW MGMT > Class Setup > Add Sub-Class (continued)

| LABEL | DESCRIPTION |
|---|---|
| Enable Bandwidth Filter | Select **Enable Bandwidth Filter** to have the ZyWALL use this bandwidth filter when it performs bandwidth management.<br>You must enter a value in at least one of the following fields (other than the **Subnet Mask** fields which are only available when you enter the destination or source IP address). |
| Service | This field simplifies bandwidth class configuration by allowing you to select a predefined application. When you select a predefined application, you do not configure the rest of the bandwidth filter fields (other than enabling or disabling the filter).<br>**FTP** (File Transfer Program) is a program to enable fast transfer of files, including large files that may not be possible by e-mail. Select FTP from the drop-down list box to configure the bandwidth filter for TCP packets with a port 21 destination.<br>**H.323** is a protocol used for multimedia communications over networks, for example OpenPhone. Select **H.323** from the drop-down list box to configure the bandwidth filter for TCP packets with a port 1720 destination.<br>Note: At the time of writing, bandwidth management only supports H.323 applications using the fast connect procedure. H.323 applications using the normal connect procedure are not applicable to bandwidth management.<br>Note: If you select **H.323**, make sure you also use the **ALG** screen to turn on the H.323 ALG.<br>**SIP** (Session Initiation Protocol) is a signaling protocol used in Internet telephony, instant messaging, events notification and conferencing. The ZyWALL supports SIP traffic pass-through. Select **SIP** from the drop-down list box to configure this bandwidth filter for UDP packets with a port 5060 destination. This option makes it easier to manage bandwidth for SIP traffic and is useful for example when there is a VoIP (Voice over Internet Protocol) device on your LAN.<br>Note: If you select **SIP**, make sure you also use the **ALG** screen to turn on the SIP ALG.<br>Select **Custom** from the drop-down list box if you do not want to use a predefined application for the bandwidth class. When you select **Custom**, you need to configure at least one of the following fields (other than the **Subnet Mask** fields which you only enter if you also enter a corresponding destination or source IP address). |
| Destination Address Type | Do you want your rule to apply to packets coming going to a particular (single) IP, a range of IP addresses (for example 192.168.1.10 to 192.169.1.50) or a subnet? Select **Single Address, Range Address** or **Subnet Address**. |
| Destination IP Address | Enter the single IP address or the starting IP address in a range here. |
| Destination End Address **/** Subnet Mask | If you are configuring a range of IP addresses, enter the ending IP address here. If you are configuring a subnet of addresses, enter the subnet mask here. Refer to Appendix E on page 817 for more information on IP subnetting. |
| Destination Port | Enter the starting and ending destination port numbers. Enter the same port number in both fields to specify a single port number. See Appendix B on page 783 for a table of services and port numbers. |

**Table 146** ADVANCED > BW MGMT > Class Setup > Add Sub-Class (continued)

| LABEL | DESCRIPTION |
|---|---|
| Source Address Type | Do you want your rule to apply to packets coming from a particular (single) IP, a range of IP addresses (for example 192.168.1.10 to 192.169.1.50) or a subnet? Select **Single Address, Range Address** or **Subnet Address**. |
| Source IP Address | Enter the single IP address or the starting IP address in a range here. |
| Source End Address / Subnet Mask | If you are configuring a range of IP addresses, enter the ending IP address here. If you are configuring a subnet of addresses, enter the subnet mask here. Refer to Appendix E on page 817 for more information on IP subnetting. |
| Source Port | Enter the starting and ending destination port numbers. Enter the same port number in both fields to specify a single port number. See Appendix B on page 783 for a table of services and port numbers. |
| Protocol ID | Enter the protocol ID (service type) number, for example: 1 for ICMP, 6 for TCP or 17 for UDP. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving. |

## 25.4.1 Bandwidth Borrowing Example

Here is an example of bandwidth management with classes configured for bandwidth borrowing. The classes are set up based on departments and individuals within certain departments.

Refer to the product specifications chapter to see how many class levels you can configure on your ZyWALL.

**Table 147** Bandwidth Borrowing Example

| BANDWIDTH CLASSES AND BANDWIDTH BORROWING SETTINGS | | | |
|---|---|---|---|
| Root Class: | Administration: Borrowing Enabled | | |
| | Sales: Borrowing Disabled | Sales USA: Borrowing Enabled | Bill: Borrowing Enabled |
| | | | Amy: Borrowing Disabled |
| | | Sales Asia: Borrowing Disabled | Tina: Borrowing Enabled |
| | | | Fred: Borrowing Disabled |
| | Marketing: Borrowing Enabled | | |
| | Research: Borrowing Enabled | Software: Borrowing Enabled | |
| | | Hardware: Borrowing Enabled | |

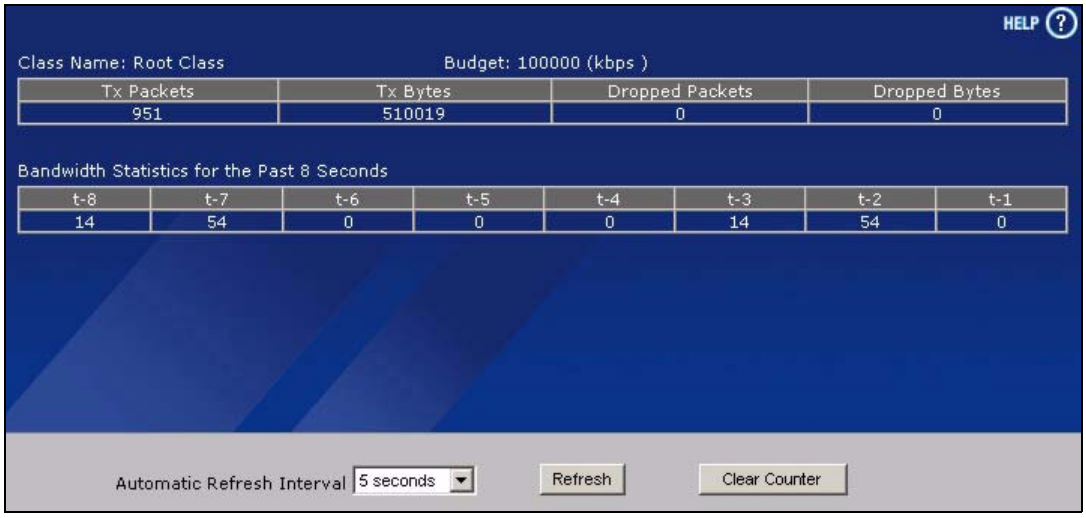
- The Bill class can borrow unused bandwidth from the Sales USA class because the Bill class has bandwidth borrowing enabled.
- The Bill class can also borrow unused bandwidth from the Sales class because the Sales USA class also has bandwidth borrowing enabled.
- The Bill class cannot borrow unused bandwidth from the Root class because the Sales class has bandwidth borrowing disabled.
- The Amy class cannot borrow unused bandwidth from the Sales USA class because the Amy class has bandwidth borrowing disabled.

- The Research Software and Hardware classes can both borrow unused bandwidth from the Research class because the Research Software and Hardware classes both have bandwidth borrowing enabled.
- The Research Software and Hardware classes can also borrow unused bandwidth from the Root class because the Research class also has bandwidth borrowing enabled.

## 25.5 Bandwidth Management Statistics

Click **ADVANCED** > **BW MGMT** > **Class Setup** > **Statistics** to open the **Bandwidth Management Statistics** screen. This screen displays the selected bandwidth class's bandwidth usage and allotments.

**Figure 271** ADVANCED > BW MGMT > Class Setup > Statistics



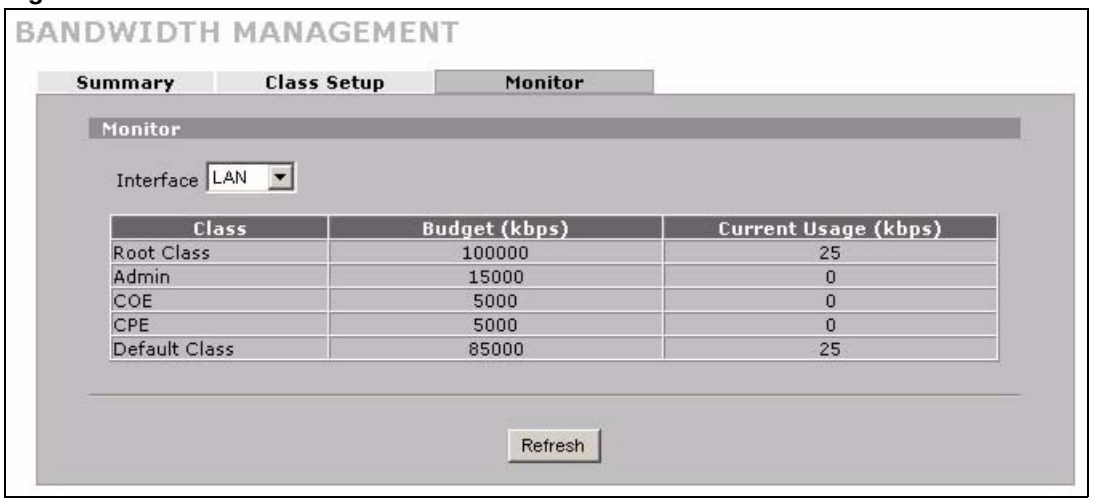

The following table describes the labels in this screen.

| LABEL | DESCRIPTION |
|---|---|
| Class Name | This field displays the name of the class the statistics page is showing. |
| Budget (kbps) | This field displays the amount of bandwidth allocated to the class. |
| Tx Packets | This field displays the total number of packets transmitted. |
| Tx Bytes | This field displays the total number of bytes transmitted. |
| Dropped Packets | This field displays the total number of packets dropped. |
| Dropped Bytes | This field displays the total number of bytes dropped. |
| Bandwidth Statistics for the Past 8 Seconds (t-8 to t-1) | |
| This field displays the bandwidth statistics (in bps) for the past one to eight seconds. For example, t-1 means one second ago. | |
| Automatic Refresh Interval | Select a number of seconds or **None** from the drop-down list box to update all screen statistics automatically at the end of every time interval or to not update the screen statistics. |
| Refresh | Click this button to update the screen's statistics immediately. |
| Clear Counter | Click **Clear Counter** to clear all of the bandwidth management statistics. |

## 25.6 The Monitor Screen

Click **ADVANCED** > **BW MGMT** > **Monitor** to open the following screen. Use this screen to view the device's bandwidth usage and allotments.

**Figure 272** ADVANCED > BW MGMT > Monitor




The following table describes the labels in this screen.

| LABEL | DESCRIPTION |
|---|---|
| Interface | Select an interface from the drop-down list box to view the bandwidth usage of its bandwidth classes. |
| Class | This field displays the name of the bandwidth class.<br>A **Default Class** automatically displays for all the bandwidth in the **Root Class** that is not allocated to bandwidth classes. If you do not enable maximize bandwidth usage on an interface, the ZyWALL uses the bandwidth in this default class to send traffic that does not match any of the bandwidth classes.[A] |
| Budget (kbps) | This field displays the amount of bandwidth allocated to the bandwidth class. |
| Current Usage (kbps) | This field displays the amount of bandwidth that each bandwidth class is using. |
| Refresh | Click **Refresh** to update the page. |

A.

# 26

# DNS Screens

## 26.1 Overview

This chapter shows you how to configure the DNS screens.

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. The ZyWALL uses a system DNS server (in the order you specify in the **DNS System** screen) to resolve domain names, for example, VPN, DDNS and the time server.

### 26.1.1 What You Can Do in the DNS Screens

- Use the **System** screen (Section 26.2 on page 481) to configure the ZyWALL to use a DNS server to resolve domain names for ZyWALL system features like VPN, DDNS and the time server.
  - Use the **Add Address Record** screen (Section 26.2.1 on page 483) to add an address record.
  - Use the **Insert Name Server Record** screen (Section 26.2.2 on page 484) to insert a name server record.
- Use the **Cache** screen (Section 26.3 on page 485) to configure the ZyWALL's DNS caching settings.
- Use the **DHCP** screen (Section 26.4 on page 487) to configure the DNS server information that the ZyWALL sends to its LAN, DMZ or WLAN DHCP clients.
- Use the **DDNS** screen (Section 26.5 on page 488) to change your ZyWALL's DDNS (Dynamic DNS) settings.

### 26.1.2 What You Need To Know About DNS

#### DNS Server Address Assignment

The ZyWALL can get the DNS server addresses in the following ways.

1. 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.
2. 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.

3 You can manually enter the IP addresses of other DNS servers. These servers can be public or private. A DNS server could even be behind a remote IPSec router (see Section on page 480).

### 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 and includes the top-level domain. For example, www.zyxel.com.tw is a fully qualified domain name, where “www” is the host, “zyxel” is the second-level domain, and “com.tw” is the top level domain. mail.myZyXEL.com.tw is also a FQDN, where "mail" is the host, "myZyXEL" is the second-level domain, and "com.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.

### DNS Wildcard

Enabling the wildcard feature for your host causes *.yourhost.com to be aliased to the same IP address as yourhost.com. This feature is useful if you want to be able to use, for example, www.yourhost.com and still reach your hostname.

### Name Server Record

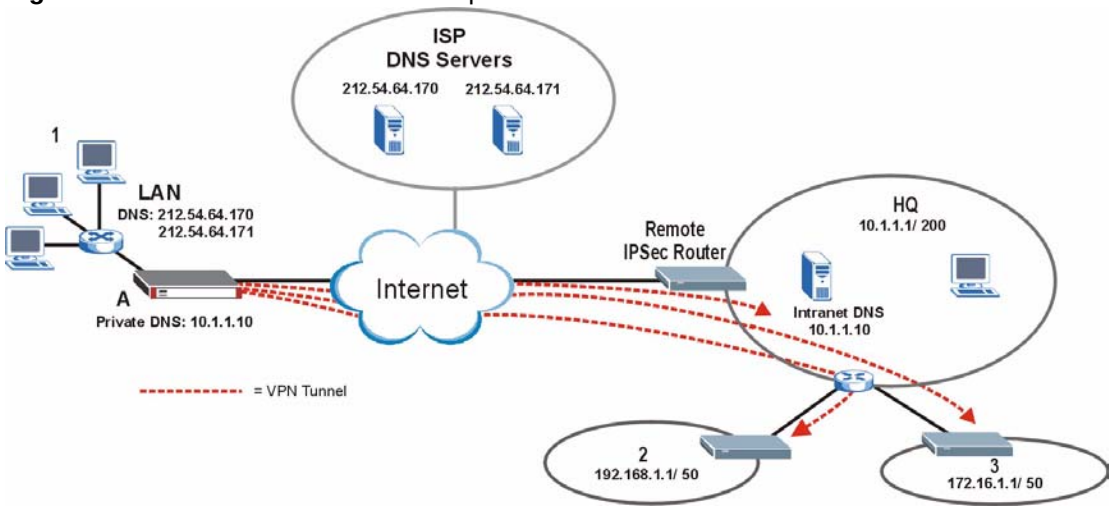
A name server record contains a DNS server’s IP address. The ZyWALL can query the DNS server to resolve domain names for features like VPN, DDNS and the time server. A domain zone may also be included. A domain zone is a fully qualified domain name without the host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name.

### Private DNS Server

In cases where you want to use domain names to access Intranet servers on a remote private network that has a DNS server, you must identify that DNS server. You cannot use DNS servers on the LAN or from the ISP since these DNS servers cannot resolve domain names to private IP addresses on the remote private network.

The following figure depicts an example where three VPN tunnels are created from ZyWALL A; one to branch office **2**, one to branch office **3** and another to headquarters (**HQ**). In order to access computers that use private domain names on the **HQ** network, the ZyWALL at branch office **1** uses the Intranet DNS server in headquarters.

**Figure 273** Private DNS Server Example




If you do not specify an Intranet DNS server on the remote network, then the VPN host must use IP addresses to access the computers on the remote private network.

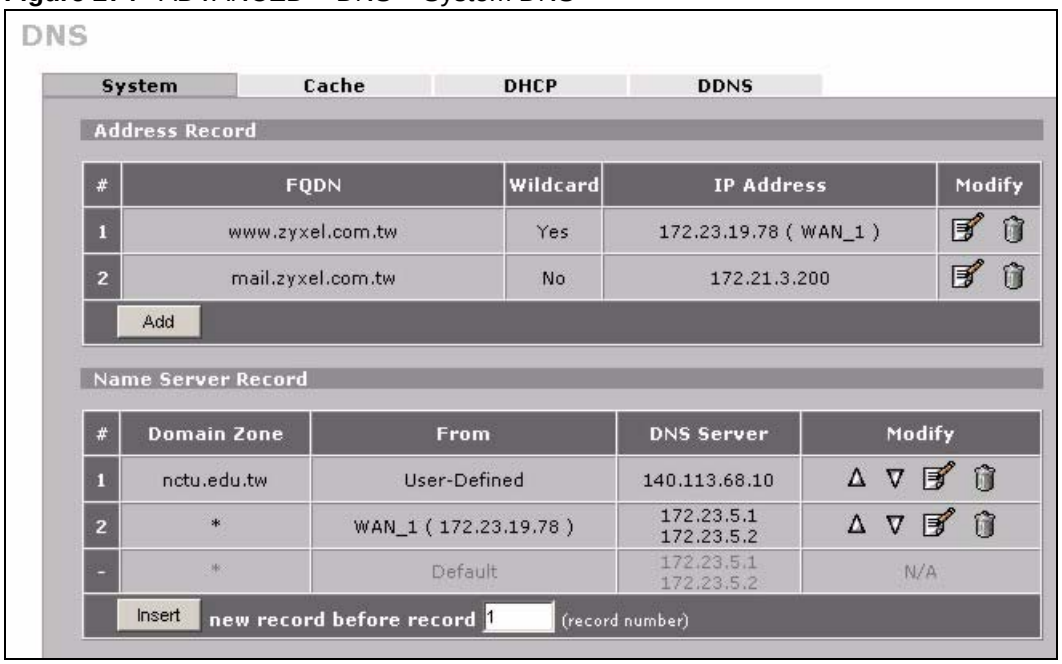
### DDNS

DDNS (Dynamic DNS) allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

## 26.2 The System Screen

Click **ADVANCED** > **DNS** to display the following screen. Use this screen to configure your ZyWALL's DNS address and name server records.

**Figure 274** ADVANCED > DNS > System DNS




The following table describes the labels in this screen.

| LABEL | DESCRIPTION |
|---|---|
| Address Record | An address record specifies the mapping of a fully qualified domain name (FQDN) to an IP address. An FQDN consists of a host and domain name and includes the top-level domain. For example, www.zyxel.com.tw is a fully qualified domain name, where “www” is the host, “zyxel” is the second-level domain, and “com.tw” is the top level domain. |
| # | This is the index number of the address record. |
| FQDN | This is a host’s fully qualified domain name. |
| Wildcard | This column displays whether or not the DNS wildcard feature is enabled for this domain name. |
| IP Address | This is the IP address of a host. |
| Modify | Click the edit icon to go to the screen where you can edit the record.<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. |
| Add | Click **Add** to open a screen where you can add a new address record. Refer to Table 148 on page 484 for information on the fields. |
| Name Server Record | A name server record contains a DNS server’s IP address. The ZyWALL can query the DNS server to resolve domain names for features like VPN, DDNS and the time server.<br>When the ZyWALL needs to resolve a domain name, it checks it against the name server record entries in the order that they appear in this list.<br>A “*” indicates a name server record without a domain zone. The default record is grayed out. The ZyWALL uses this default record if the domain name that needs to be resolved does not match any of the other name server records.<br>A name server record with a domain zone is always put before a record without a domain zone. |
| # | This is the index number of the name server record. |

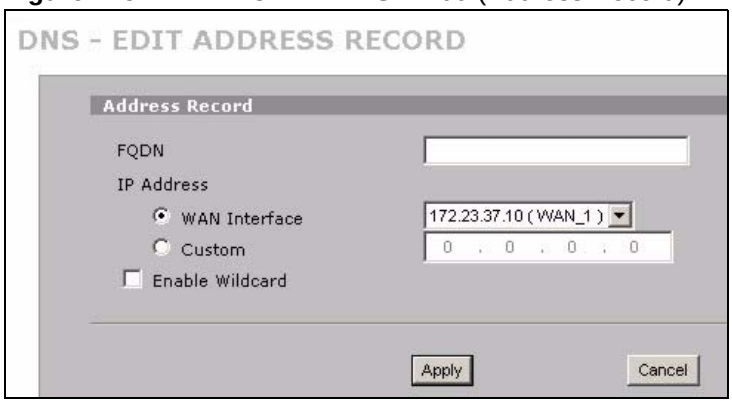
| LABEL | DESCRIPTION |
|---|---|
| Domain Zone | A domain zone is a fully qualified domain name without the host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name. |
| From | This field displays whether the IP address of a DNS server is from a WAN interface (and which it is) or specified by the user. |
| DNS Server | This is the IP address of a DNS server. |
| Modify | Click a triangle icon to move the record up or down in the list.<br>Click the edit icon to go to the screen where you can edit the record.<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. |
| Insert | Click **Insert** to open a screen where you can insert a new name server record. Refer to Table 152 on page 485 for information on the fields. |

## 26.2.1 The Add Address Record Screen

Click **Add** in the **System** screen to open this screen. Use this screen to add an address record.

An address record contains the mapping of a fully qualified domain name (FQDN) to an IP address. Configure address records about the ZyWALL itself or another device to 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. See Section 26.1.2 on page 479 for more on address records.

**Figure 275** ADVANCED > DNS > Add (Address Record)



The following table describes the labels in this screen.

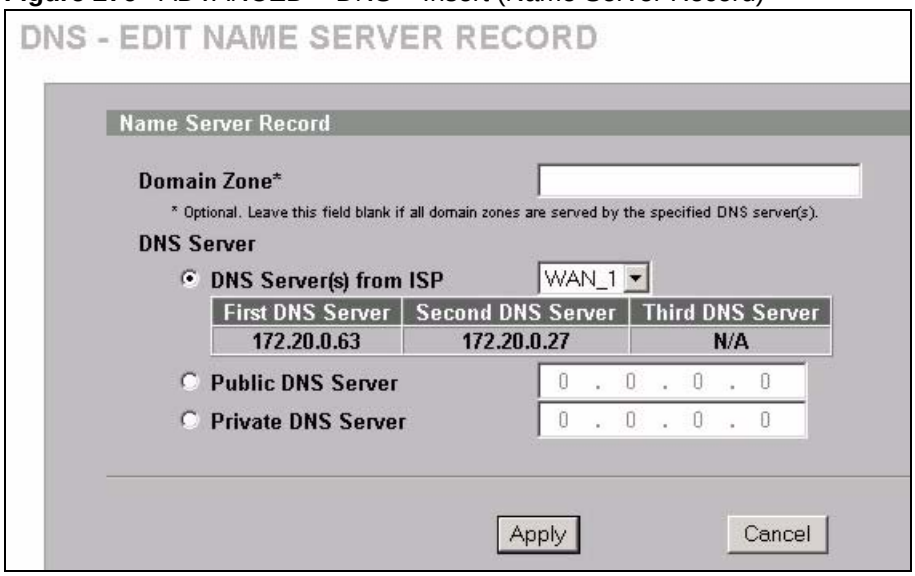
**Table 148** ADVANCED > DNS > Add (Address Record)

| 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 second-level domain, and “com.tw” is the top level domain. |
| IP Address | If this entry is for one of the WAN ports on a ZyWALL with multiple WAN ports, select **WAN Interface** and select WAN 1 or WAN 2 from the drop-down list box.<br>If this entry is for the WAN port on a ZyWALL with a single WAN port, select **WAN Interface**.<br>For entries that are not for the WAN port(s), select **Custom** and enter the IP address of the host in dotted decimal notation. |
| Enable Wildcard | Select the check box to enable DNS wildcard. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving. |

## 26.2.2 The Insert Name Server Record Screen

Click **Insert** in the **System** screen to open this screen. Use this screen to insert a name server record.A name server record contains a DNS server’s IP address. The ZyWALL can query the DNS server to resolve domain names for features like VPN, DDNS and the time server. A domain zone may also be included. 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.

**Figure 276** ADVANCED > DNS > Insert (Name Server Record)



The following table describes the labels in this screen.

| LABEL | DESCRIPTION |
|---|---|
| Domain Zone | This field is optional.<br>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>Leave this field blank if all domain zones are served by the specified DNS server(s). |
| DNS Server | Select the **DNS Server(s) from ISP** radio button 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 as 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. **N/A** displays for all of the DNS server IP address fields if the ZyWALL has a fixed WAN IP address.<br>Select **Public DNS Server** if you have the IP address of a DNS server. The IP address must be public or a private address on your local LAN. Enter the DNS server's IP address in the field to the right.<br>**Public DNS Server** entries with the IP address set to 0.0.0.0 are not allowed.<br>Select **Private DNS Server** if the DNS server has a private IP address and is located behind a VPN peer. Enter the DNS server's IP address in the field to the right.<br>With a private DNS server, you must also configure the first DNS server entry for the LAN, DMZ and/or WLAN in the **DNS DHCP** screen to use **DNS Relay**.<br>You must also configure a VPN rule since the ZyWALL uses a VPN tunnel when it relays DNS queries to the private DNS server. The rule must include the LAN IP address of the ZyWALL as a local IP address and the IP address of the DNS server as a remote IP address.<br>**Private DNS Server** entries with the IP address set to 0.0.0.0 are not allowed. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Cancel | Click **Cancel** to exit this screen without saving. |

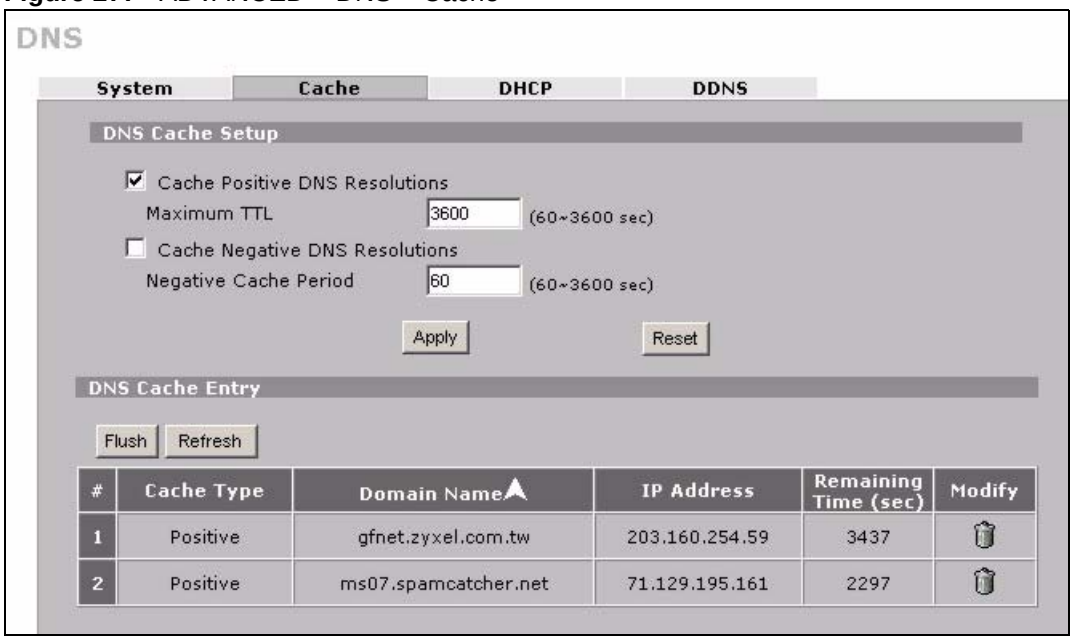
## 26.3 The DNS Cache Screen

DNS cache is the temporary storage area where a router stores responses from DNS servers. When the ZyWALL receives a positive or negative response for a DNS query, it records the response in the DNS cache. A positive response means that the ZyWALL received the IP address for a domain name that it checked with a DNS server within the five second DNS timeout period. A negative response means that the ZyWALL did not receive a response for a query it sent to a DNS server within the five second DNS timeout period.

When the ZyWALL receives DNS queries, it compares them against the DNS cache before querying a DNS server. If the DNS query matches a positive entry, the ZyWALL responses with the IP address from the entry. If the DNS query matches a negative entry, the ZyWALL replies that the DNS query failed.

To configure your ZyWALL's DNS caching, click **ADVANCED** > **DNS** > **Cache**. The screen appears as shown.

**Figure 277** ADVANCED > DNS > Cache




The following table describes the labels in this screen.

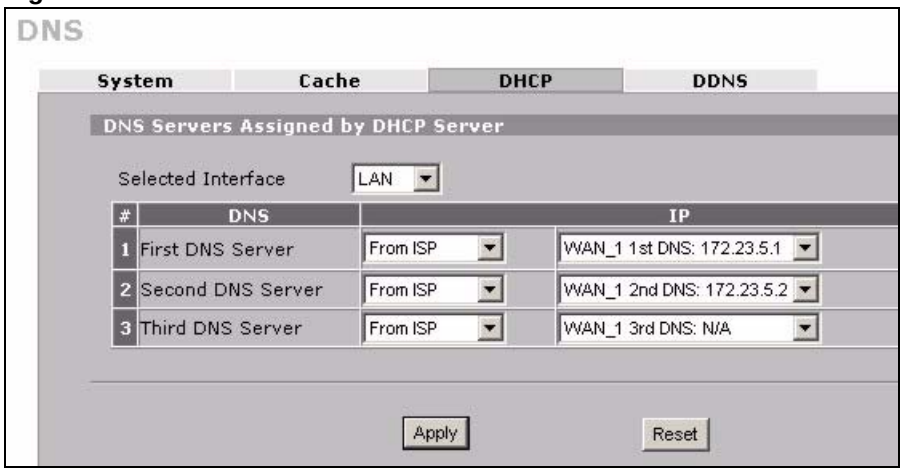
| LABEL | DESCRIPTION |
|---|---|
| DNS Cache Setup | |
| Cache Positive DNS Resolutions | Select the check box to record the positive DNS resolutions in the cache. Caching positive DNS resolutions helps speed up the ZyWALL's processing of commonly queried domain names and reduces the amount of traffic that the ZyWALL sends out to the WAN. |
| Maximum TTL | Type the maximum time to live (TTL) (60 to 3600 seconds). This sets how long the ZyWALL is to allow a positive resolution entry to remain in the DNS cache before discarding it. |
| Cache Negative DNS Resolutions | Caching negative DNS resolutions helps speed up the ZyWALL's processing of commonly queried domain names (for which DNS resolution has failed) and reduces the amount of traffic that the ZyWALL sends out to the WAN. |
| Negative Cache Period | Type the time (60 to 3600 seconds) that the ZyWALL is to allow a negative resolution entry to remain in the DNS cache before discarding it. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |
| DNS Cache Entry | |
| Flush | Click this button to clear the cache manually. After you flush the cache, the ZyWALL must query the DNS servers again for any domain names that had been previously resolved. |
| Refresh | Click this button to reload the cache. |
| # | This is the index number of a record. |
| Cache Type | This displays whether the response for the DNS request is positive or negative. |
| Domain Name | This is the domain name of a host. |
| IP Address | This is the (resolved) IP address of a host. This field displays **0.0.0.0** for negative DNS resolution entries. |

| LABEL | DESCRIPTION |
|---|---|
| Remaining Time (sec) | This is the number of seconds left before the DNS resolution entry is discarded from the cache. |
| Modify | Click the delete icon to remove the DNS resolution entry from the cache. |

## 26.4 The DHCP Screen

Click **ADVANCED** > **DNS** > **DHCP** to open the **DNS DHCP** screen shown next. Use this screen to configure the DNS server information that the ZyWALL sends to its LAN, DMZ or WLAN DHCP clients.

**Figure 278** ADVANCED > DNS > DHCP




The following table describes the labels in this screen.

| LABEL | DESCRIPTION |
|---|---|
| DNS Servers Assigned by DHCP Server | The ZyWALL passes a DNS (Domain Name System) server IP address to the DHCP clients. |
| Selected Interface | Select an interface from the drop-down list box to configure the DNS servers for the specified interface. |
| DNS | These read-only labels represent the DNS servers. |

| LABEL | DESCRIPTION |
|---|---|
| IP | Select **From ISP** if your ISP dynamically assigns DNS server information (and the ZyWALL's WAN IP address). Use the drop-down list box to select a DNS server IP address that the ISP assigns in the field to the right.<br>Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**.<br>Select **DNS Relay** to have the ZyWALL act as a DNS proxy. The ZyWALL's LAN, DMZ or WLAN IP address displays in the field to the right (read-only). The ZyWALL tells the DHCP clients on the LAN, DMZ or WLAN that the ZyWALL itself is the DNS server. When a computer on the LAN, DMZ or WLAN sends a DNS query to the ZyWALL, the ZyWALL forwards the query to the ZyWALL's system DNS server (configured in the **DNS System** screen) and relays the response back to the computer. You can only select **DNS Relay** for one of the three servers; if you select DNS Relay for a second or third DNS server, that choice changes to **None** after you click **Apply**.<br>Select **None** if you do not want to configure DNS servers. You must have another DHCP sever on your LAN, or else the computers must have their DNS server addresses manually configured. If you do not configure a DNS server, you must know the IP address of a computer in order to access it. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 26.5 The DDNS Screen

First of all, you need to have registered a dynamic DNS account with www.dyndns.com. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

You must go to the Dynamic DNS service provider’s website and register a user account and a domain name before you can use the Dynamic DNS service with your ZyWALL.

### DYNDNS Wildcard

Enabling the wildcard feature for your host causes *.yourhost.dyndns.com to be aliased to the same IP address as yourhost.dyndns.com. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.com and still reach your hostname.

If you have a private WAN IP address, then you cannot use Dynamic DNS.

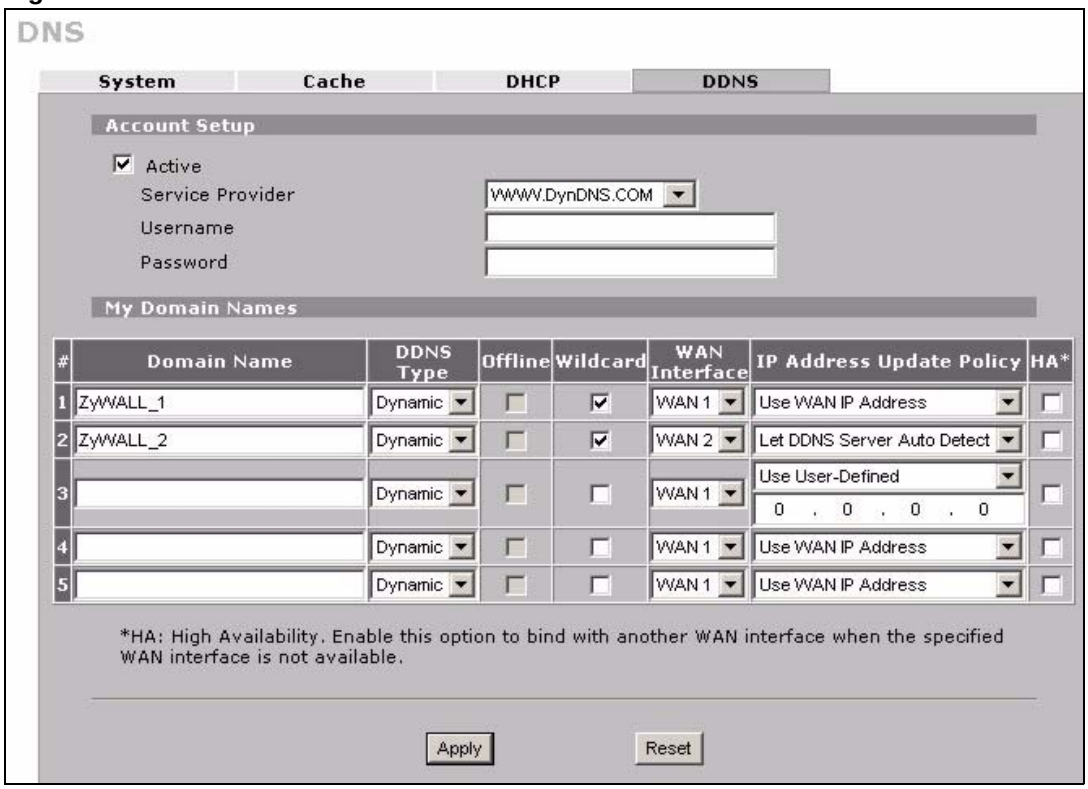
### High Availability

A DNS server maps a domain name to a port's IP address. If that WAN port loses its connection, high availability allows the router to substitute another port's IP address for the domain name mapping.

## 26.6 Configuring the Dynamic DNS Screen

To change your ZyWALL's DDNS, click **ADVANCED** > **DNS** > **DDNS**. The screen appears as shown.

**Figure 279** ADVANCED > DNS > DDNS




The following table describes the labels in this screen.

| LABEL | DESCRIPTION |
|---|---|
| Account Setup | |
| Active | Select this check box to use dynamic DNS. |
| Service Provider | This is the name of your Dynamic DNS service provider. |
| Username | Enter your user name. You can use up to 31 alphanumeric characters (and the underscore). Spaces are not allowed. |
| Password | Enter the password associated with the user name above. You can use up to 31 alphanumeric characters (and the underscore). Spaces are not allowed. |
| Token | If you have selected **WWW.REGFISH.COM** as your DNS service provider you can use a token instead of a user name and password. This token is provided automatically for a domain when activating DynDNS with RegFish. |
| My Domain Names | |

| LABEL | DESCRIPTION |
|---|---|
| Domain Name 1~5 | Enter the host names in these fields. |
| DDNS Type | Select the type of service that you are registered for from your Dynamic DNS service provider if you have selected **WWW.DynDNS.COM**.<br>Select **Dynamic** if you have the Dynamic DNS service.<br>Select **Static** if you have the Static DNS service.<br>Select **Custom** if you have the Custom DNS service. |
| Offline | This option is available when **Custom** is selected in the **DDNS Type** field. Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line. |
| Wildcard | Select the check box to enable DYNDNS Wildcard. |
| WAN Interface | Select the WAN interface to use for updating the IP address of the domain name. |
| IP Address Update Policy | Select **Use WAN IP Address** to have the ZyWALL update the domain name with the WAN interface's IP address.<br>Select **Use User-Defined** and enter the IP address if you have a static IP address.<br>Select **Let DDNS Server Auto Detect** only when there are one or more NAT routers between the ZyWALL and the DDNS server. This feature has the DDNS server automatically detect and use the IP address of the NAT router that has a public IP address.<br><br>Note: The DDNS server may not be able to detect the proper IP address if there is an HTTP proxy server between the ZyWALL and the DDNS server. |
| HA | Select this check box to enable the high availability (HA) feature. High availability has the ZyWALL update a domain name with another interface's IP address when the normal WAN interface does not have a connection.<br>If the WAN interface specified in the **WAN Interface** field does not have a connection, the ZyWALL will attempt to use the IP address of another WAN interface to update the domain name.<br>When the WAN interfaces are in the active/passive operating mode, the ZyWALL will update the domain name with the IP address of whichever WAN interface has a connection, regardless of the setting in the **WAN Interface** field.<br>Disable this feature and the ZyWALL will only update the domain name with an IP address of the WAN interface specified in the **WAN Interface** field. If that WAN interface does not have a connection, the ZyWALL will not update the domain name with another port's IP address.<br><br>Note: If you enable high availability, DDNS can also function when the ZyWALL uses the dial backup port. DDNS does not function when the ZyWALL uses traffic redirect. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# 27

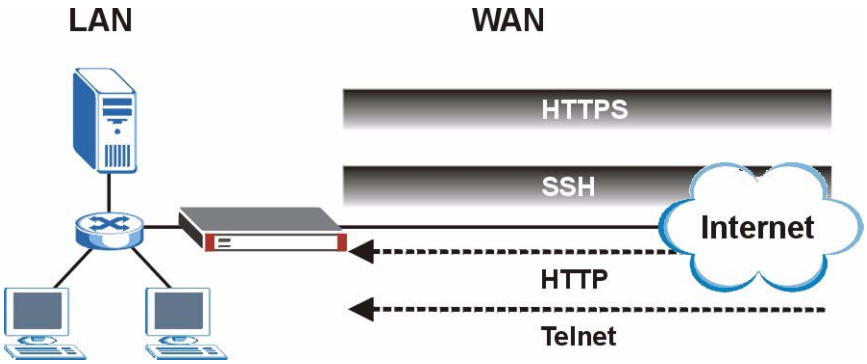
# Remote Management Screens

## 27.1 Overview

This chapter provides information on the remote management screens. Remote management allows you to determine which services/protocols can access which ZyWALL interface (if any) from which computers.

The following figure shows secure and insecure management of the ZyWALL coming in from the WAN. HTTPS and SSH access are secure. HTTP and Telnet access are not secure.

**Figure 280** Secure and Insecure Remote Management From the WAN




### 27.1.1 What You Can Do in the Remote Management Screens

- Use the **WWW** screen (Section 27.3 on page 504) to configure the ZyWALL's HTTP and HTTPS management settings.
- Use the **SSH** screen (Section 27.5 on page 507) to configure the ZyWALL's Secure Shell settings.
- Use the **Telnet** screen (Section 27.7 on page 508) to specify which interfaces allow Telnet access and from which IP address the access can come.
- Use the **FTP** screen (Section 27.8 on page 509) to specify which interfaces allow FTP access and from which IP address the access can come.
- Use the **SNMP** screen (Section 27.9 on page 510) to configure the ZyWALL's SNMP settings.
- Use the **DNS** screen (Section 27.10 on page 513) to set from which IP address the ZyWALL will accept DNS queries and on which interface it can send them your ZyWALL's DNS settings.
- Use the **CNM** screen (Section 27.11 on page 514) to configure the ZyWALL's CNM settings.

## 27.1.2 What You Need To Know About Remote Management

### Firewall Rules

When you configure remote management to allow management from any network except the LAN, you still need to configure a firewall rule to allow access. See Chapter 13 on page 251 for details on configuring firewall rules.

You can also disable a service on the ZyWALL by not allowing access for the service/protocol through any of the ZyWALL interfaces.

### Remote Management Sessions

You may only have one remote management session running at a time. The ZyWALL automatically disconnects a remote management session of lower priority when another remote management session of higher priority starts. The priorities for the different types of remote management sessions are as follows.

1. Console port
2. SSH
3. Telnet
4. HTTPS and HTTP

### Remote Management Limitations

Remote management does not work when:

1. You have not enabled that service on the interface in the corresponding remote management screen.
2. You have disabled that service in one of the remote management screens.
3. The IP address in the **Secure Client IP Address** field does not match the client IP address. If it does not match, the ZyWALL will disconnect the session immediately.
4. There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.
5. There is a firewall rule that blocks it.
6. A filter is applied (through the SMT or the commands) to block a Telnet, FTP or Web service.

### System Timeout

There is a default system management idle timeout of five minutes (three hundred seconds). 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. You can change the timeout period in the **MAINTENANCE** > **General** screen.

### Finding Out More

For more advanced information regarding Remote Management refer to Section 27.13 on page 516.

The next section covers remote management examples. If you would prefer to find out how to configure the screens then proceed to Section 27.3 on page 504.

## 27.2 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.

### 27.2.1 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 281** Security Alert Dialog Box (Internet Explorer)


### 27.2.2 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 282** Security Certificate 1 (Netscape)

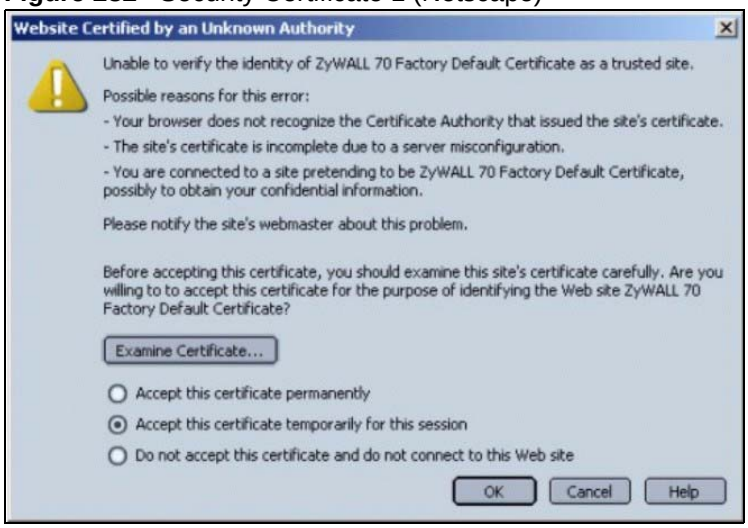



**Figure 283** Security Certificate 2 (Netscape)


## 27.2.3 Avoiding the Browser Warning Messages

The following describes the main reasons that 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 J on page 861 for details.
- The actual IP address of the HTTPS server (the IP address of the ZyWALL's port that you are trying to access) does not match the common name specified in the ZyWALL's HTTPS server certificate that your browser received. Do the following to check the common name specified in the certificate that your ZyWALL sends to HTTPS clients.

**6a** Click **REMOTE MGMT**. Write down the name of the certificate displayed in the **Server Certificate** field.

**6b** Click **CERTIFICATES**. Find the certificate and check its **Subject** column. **CN** stands for certificate's common name (see Figure 286 on page 496 for an example).

Use this procedure to have the ZyWALL use a certificate with a common name that matches the ZyWALL's actual IP address. You cannot use this procedure if you need to access the WAN port and it uses a dynamically assigned IP address.

**6a** Create a new certificate for the ZyWALL that uses the IP address (of the ZyWALL's port that you are trying to access) as the certificate's common name. For example, to use HTTPS to access a LAN port with IP address 192.168.1.1, create a certificate that uses 192.168.1.1 as the common name.

**6b** Go to the remote management **WWW** screen and select the newly created certificate in the **Server Certificate** field. Click **Apply**.

## 27.2.4 Login Screen

After you accept the certificate, the ZyWALL login screen appears. The lock displayed in the bottom right of the browser status bar denotes a secure connection.

**Figure 284** Example: Lock Denoting a Secure Connection

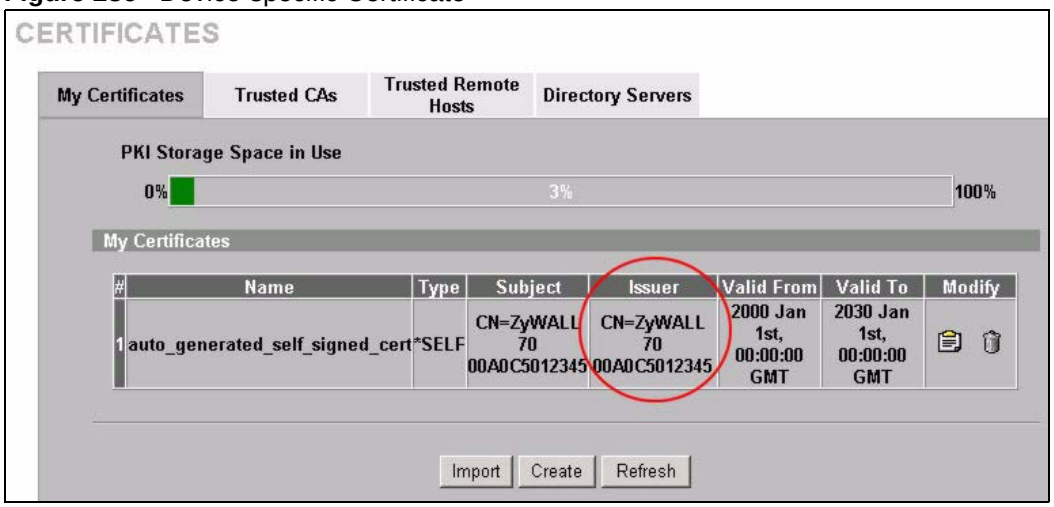

Click **Login** and you then see the next screen.

The factory default certificate is a common default certificate for all ZyWALL models.

**Figure 285** Replace Certificate

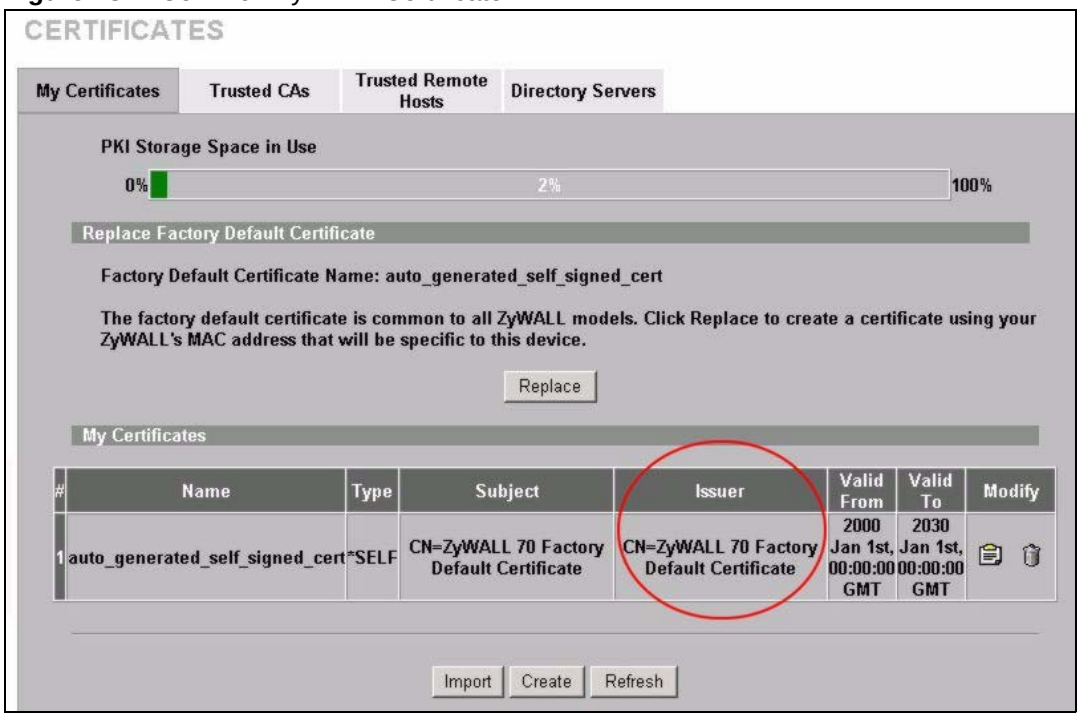

Click **Apply** in the **Replace Certificate** screen to create a certificate using your ZyWALL's MAC address that will be specific to this device. Click **CERTIFICATES** to open the **My Certificates** screen. You will see information similar to that shown in the following figure.

**Figure 286** Device-specific Certificate




Click **Ignore** in the **Replace Certificate** screen to use the common ZyWALL certificate. You will then see this information in the **My Certificates** screen.

**Figure 287** Common ZyWALL Certificate



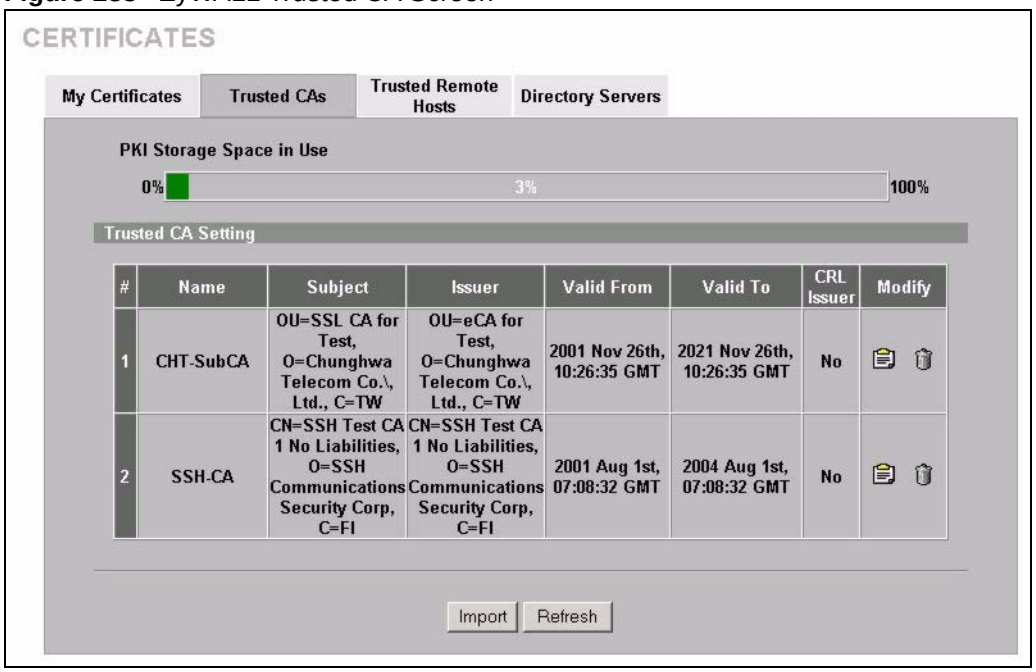

## 27.2.5 Enrolling and Importing SSL Client Certificates (Example)

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 288** ZyWALL Trusted CA Screen

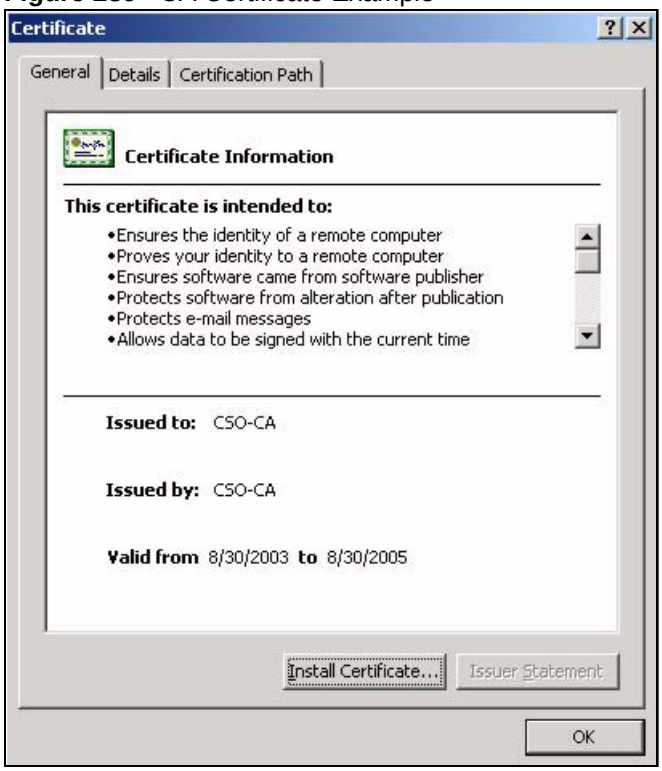



The CA sends you a package containing the CA's trusted certificate(s), your personal certificate(s) and a password to install the personal certificate(s).

## 27.2.6 Installing the CA's Certificate (Example)

**1** Double click the CA's trusted certificate to produce a screen similar to the one shown next.

**Figure 289** CA Certificate Example




2 Click **Install Certificate** and follow the wizard as shown earlier in this appendix.

## 27.2.7 Installing Your Personal Certificate(s) (Example)

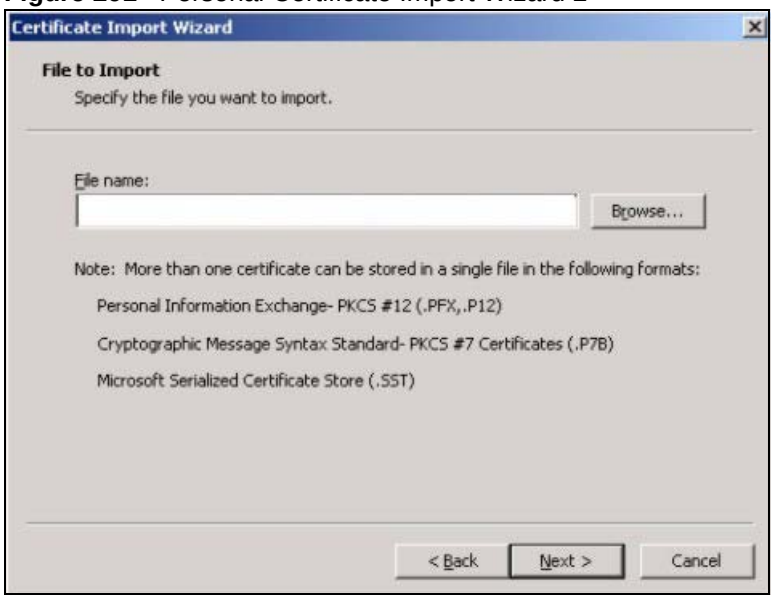
You need a password in advance. The CA may issue the password or you may have to specify it during the enrollment. Double-click the personal certificate given to you by the CA to produce a screen similar to the one shown next

1 Click **Next** to begin the wizard.

**Figure 290** 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 291** Personal Certificate Import Wizard 2

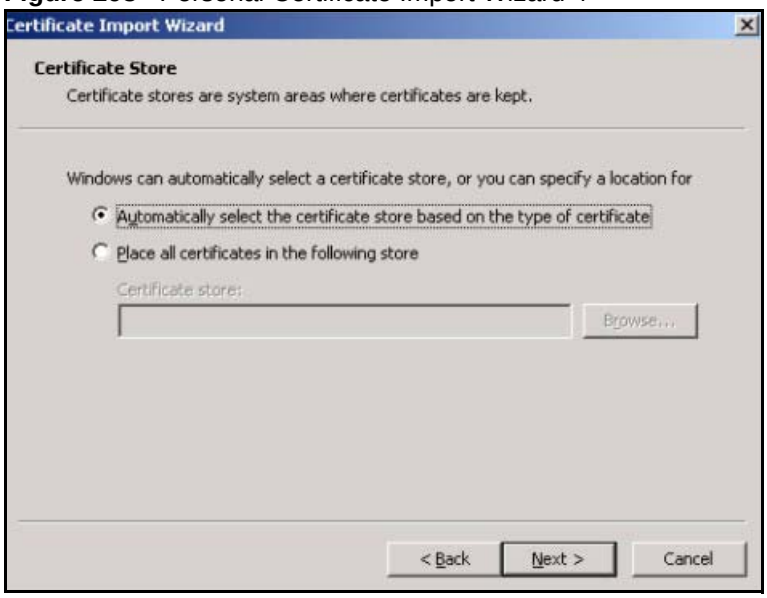



**3** Enter the password given to you by the CA.

**Figure 292** Personal Certificate Import Wizard 3

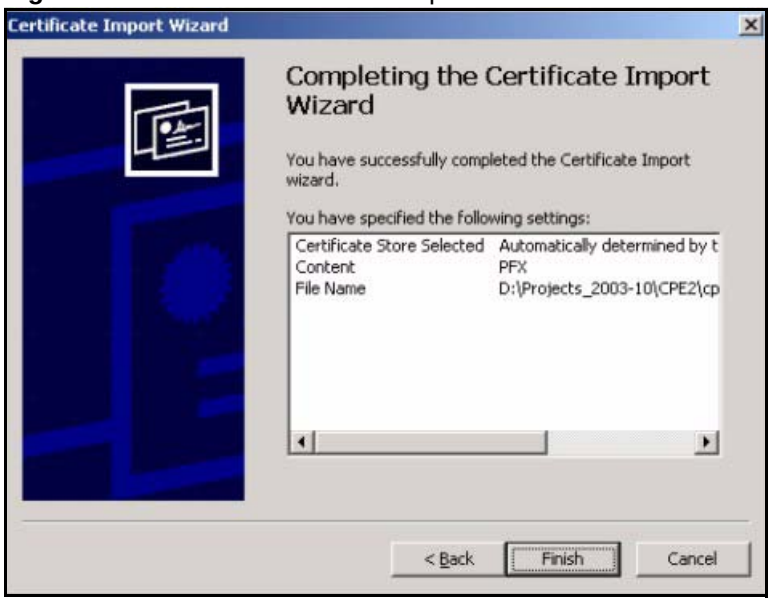

**4** Have the wizard determine where the certificate should be saved on your computer or select **Place all certificates in the following store** and choose a different location.

**Figure 293** Personal Certificate Import Wizard 4




**5** Click **Finish** to complete the wizard and begin the import process.

**Figure 294** Personal Certificate Import Wizard 5




**6** You should see the following screen when the certificate is correctly installed on your computer.

**Figure 295** Personal Certificate Import Wizard 6


## 27.2.8 Using a Certificate When Accessing the ZyWALL (Example)

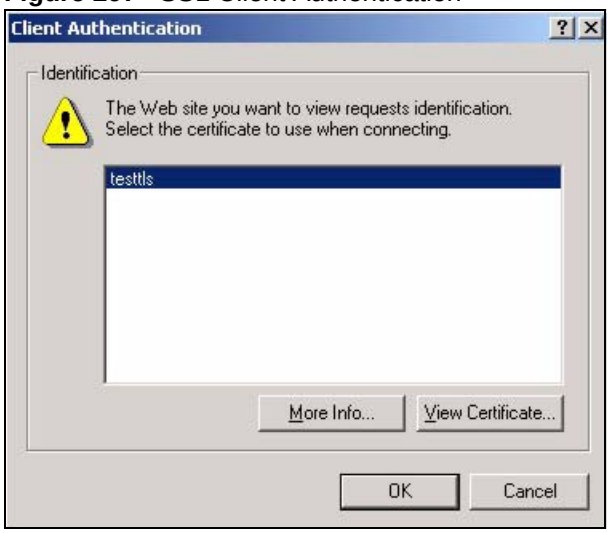
Use the following procedure to access the ZyWALL via HTTPS.

**1** Enter 'https://ZyWALL IP Address/ in your browser's web address field.

**Figure 296** 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 297** SSL Client Authentication




**3** You next see the web configurator login screen.

**Figure 298** Secure Web Configurator Login Screen


## 27.2.9 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.

### 27.2.9.1 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 or device name) 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 299** SSH Example 1: Store Host Key


Enter the password to log in to the ZyWALL. The SMT main menu displays next.

### 27.2.9.2 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 300** 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 301** 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 SMT main menu displays next.

#### 27.2.9.3 Secure FTP Using SSH Example

This section shows an example on file transfer using the OpenSSH client program. The configuration and connection steps are similar for other SSH client programs. Refer to your SSH client program user's guide.

1 Enter "`sftp -1 192.168.1.1`". This command forces your computer to connect to the ZyWALL for secure file transfer 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].
2 Enter the password to login to the ZyWALL.
3 Use the "`put`" command to upload a new firmware to the ZyWALL.

**Figure 302** Secure FTP: Firmware Upload Example

```
$ sftp -1 192.168.1.1
Connecting to 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:
sftp> put firmware.bin ras
Uploading firmware.bin to /ras
Read from remote host 192.168.1.1: Connection reset by peer
Connection closed
$
```

## 27.3 The WWW Screen

Use this screen to configure the ZyWALL's HTTP and HTTPS management settings.

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 20 on page 399 for more information).

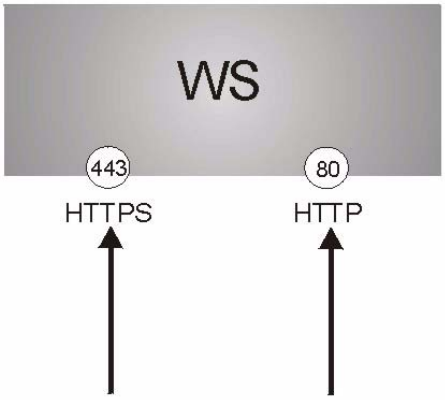
HTTPS on the ZyWALL is used so that you may securely access the ZyWALL using the web configurator. The SSL protocol specifies that the SSL server (the ZyWALL) must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the ZyWALL), whereas the SSL client only should authenticate itself when the SSL server

requires it to do so (select **Authenticate Client Certificates** in the **REMOTE MGMT** > **WWW** screen). **Authenticate Client Certificates** is optional and if selected means the SSL-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 WS (web server).
2. HTTP connection requests from a web browser go to port 80 (by default) on the ZyWALL's WS (web server).

**Figure 303** HTTPS Implementation




If you disable the **HTTP** service in the **REMOTE MGMT > WWW** screen, then the ZyWALL blocks all HTTP connection attempts.

## 27.4 Configuring the WWW Screen

Click **ADVANCED** > **REMOTE MGMT** to open the **WWW** screen.

**Figure 304** ADVANCED > REMOTE MGMT > WWW


The following table describes the labels in this screen.

**Table 149** ADVANCED > REMOTE MGMT > WWW

| LABEL | DESCRIPTION |
|---|---|
| HTTPS | |
| Server Certificate | Select the **Server Certificate** that the ZyWALL will use to identify itself. The ZyWALL is the SSL server and must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the ZyWALL). |
| 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 27.2.5 on page 496 on importing certificates for details). |
| Server Port | The HTTPS proxy server listens on port 443 by default. If you change the HTTPS proxy 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. |
| Server Access | Select the interface(s) through which a computer may access the ZyWALL using this service.<br>You can allow only secure web configurator access by clearing all of the interface check boxes in the **HTTP Server Access** field and setting the **HTTPS Server Access** field to an interface(s). |
| Secure Client IP Address | A secure client is a "trusted" computer that is allowed to communicate with the ZyWALL using this service.<br>Select **All** to allow any computer to access the ZyWALL using this service.<br>Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyWALL using this service. |
| HTTP | |
| 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. |

**Table 149** ADVANCED > REMOTE MGMT > WWW (continued)

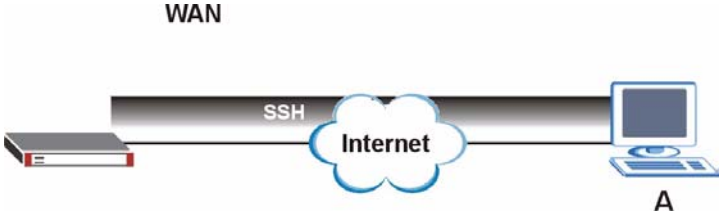
| LABEL | DESCRIPTION |
|---|---|
| Server Access | Select the interface(s) through which a computer may access the ZyWALL using this service. |
| Secure Client IP Address | A secure client is a “trusted” computer that is allowed to communicate with the ZyWALL using this service.<br>Select **All** to allow any computer to access the ZyWALL using this service.<br>Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyWALL using this service. |
| Apply | Click **Apply** to save your customized settings and exit this screen. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# 27.5 The SSH Screen

You can use SSH (Secure SHell) to securely access the ZyWALL’s SMT or command line interface. Specify which interfaces allow SSH access and from which IP address the access can come.

Unlike Telnet or FTP, which transmit data in plaintext (clear or unencrypted text), 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 305** SSH Communication Over the WAN Example




## SSH Implementation on the ZyWALL

Your ZyWALL supports SSH version 1.5 using RSA authentication and three encryption methods (DES, 3DES and Blowfish). The SSH server is implemented on the ZyWALL for remote SMT management and file transfer on port 22. Only one SSH connection is allowed at a time.

## Requirements for Using SSH

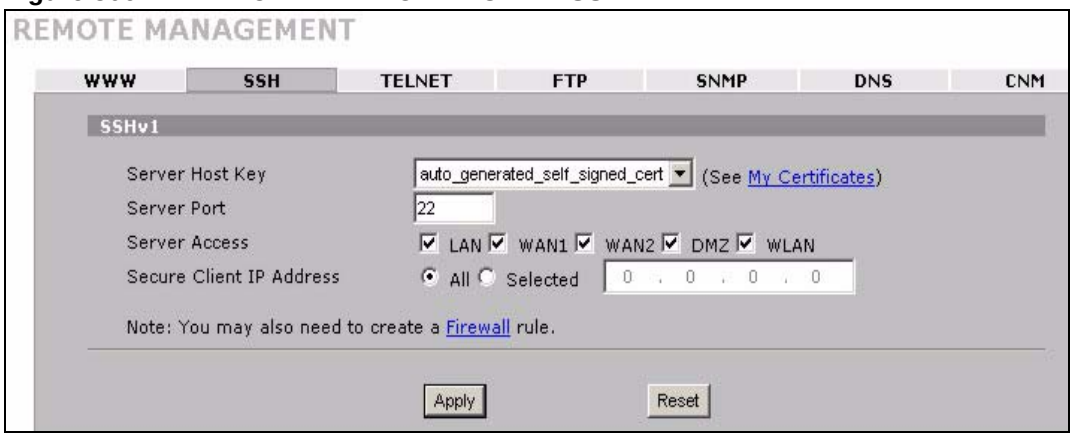
You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to the ZyWALL over SSH.

# 27.6 Configuring the SSH Screen

Click **ADVANCED** > **REMOTE MGMT** > **SSH** to change your ZyWALL’s Secure Shell settings.

It is recommended that you disable Telnet and FTP when you configure SSH for secure connections.

**Figure 306** ADVANCED > REMOTE MGMT > SSH




The following table describes the labels in this screen.

**Table 150** ADVANCED > REMOTE MGMT > SSH

| LABEL | DESCRIPTION |
|---|---|
| Server Host Key | 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 20 on page 399 for details). |
| 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 Access | Select the interface(s) through which a computer may access the ZyWALL using this service. |
| Secure Client IP Address | A secure client is a “trusted” computer that is allowed to communicate with the ZyWALL using this service.<br>Select **All** to allow any computer to access the ZyWALL using this service.<br>Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyWALL using this service. |
| Apply | Click **Apply** to save your customized settings and exit this screen. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

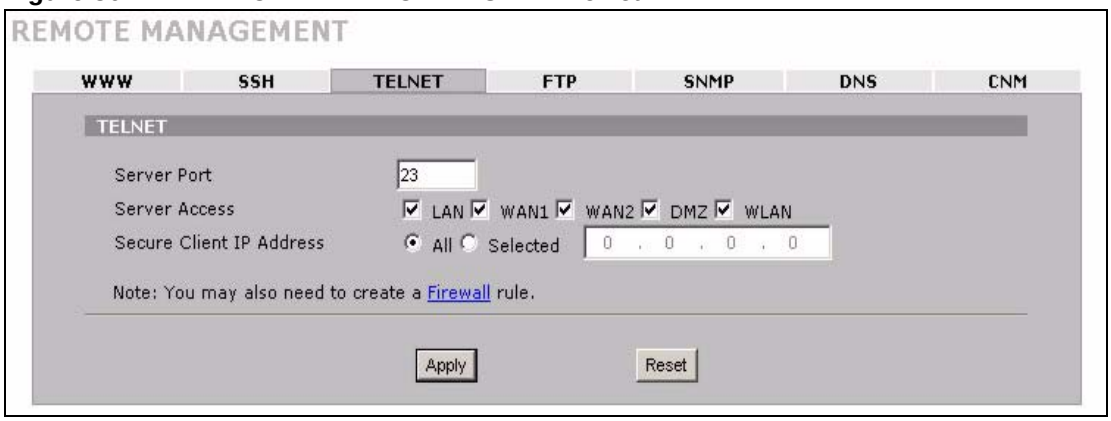
## 27.7 The Telnet Screen

You can use Telnet to access the ZyWALL’s SMT or command line interface. Specify which interfaces allow Telnet access and from which IP address the access can come.

Click **ADVANCED** > **REMOTE MGMT** > **TELNET** to open the following screen. Use this screen to specify which interfaces allow Telnet access and from which IP address the access can come.

It is recommended that you disable Telnet and FTP when you configure SSH for secure connections.

**Figure 307** ADVANCED > REMOTE MGMT > Telnet




The following table describes the labels in this screen.

**Table 151** ADVANCED > REMOTE MGMT > Telnet

| LABEL | DESCRIPTION |
|---|---|
| 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 Access | Select the interface(s) through which a computer may access the ZyWALL using this service. |
| Secure Client IP Address | A secure client is a “trusted” computer that is allowed to communicate with the ZyWALL using this service.<br>Select **All** to allow any computer to access the ZyWALL using this service.<br>Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyWALL using this service. |
| Apply | Click **Apply** to save your customized settings and exit this screen. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

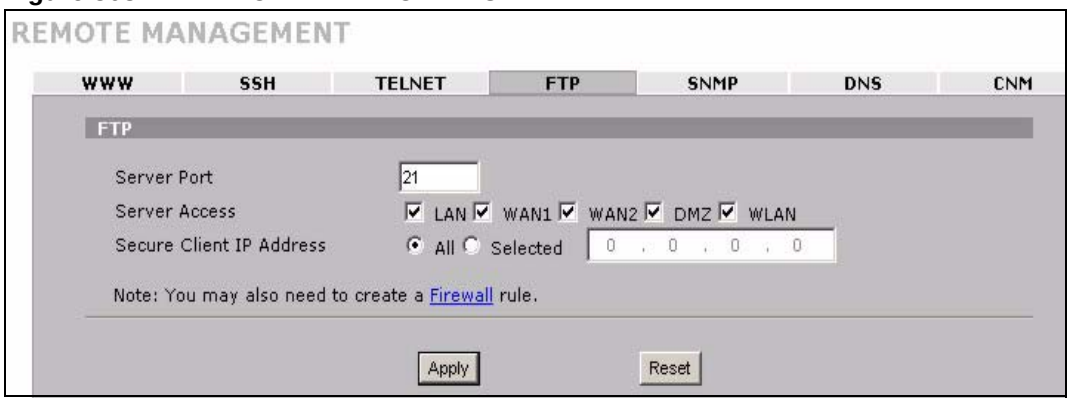
## 27.8 The FTP Screen

You can use FTP (File Transfer Protocol) to upload and download the ZyWALL’s firmware and configuration files, please see Chapter 49 on page 725 on firmware and configuration file maintenance for details. To use this feature, your computer must have an FTP client.

To change your ZyWALL’s FTP settings, click **ADVANCED** > **REMOTE MGMT** > **FTP**. The screen appears as shown. Use this screen to specify which interfaces allow FTP access and from which IP address the access can come.

It is recommended that you disable Telnet and FTP when you configure SSH for secure connections.

**Figure 308** ADVANCED > REMOTE MGMT > FTP




The following table describes the labels in this screen.

**Table 152** ADVANCED > REMOTE MGMT > FTP

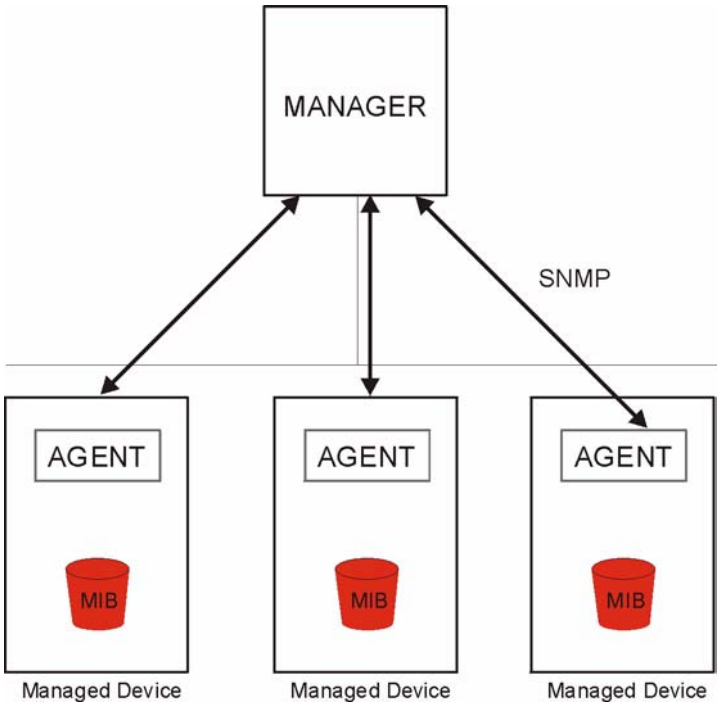
| LABEL | DESCRIPTION |
|---|---|
| Server Port | You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management. |
| Server Access | Select the interface(s) through which a computer may access the ZyWALL using this service. |
| Secure Client IP Address | A secure client is a “trusted” computer that is allowed to communicate with the ZyWALL using this service.<br>Select **All** to allow any computer to access the ZyWALL using this service.<br>Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyWALL using this service. |
| Apply | Click **Apply** to save your customized settings. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 27.9 The SNMP Screen

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. 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). The next figure illustrates an SNMP management operation.

SNMP is only available if TCP/IP is configured.

**Figure 309** 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.

### Supported MIBs

The ZyWALL supports MIB II that is defined in RFC-1213 and RFC-1215. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance.

### SNMP Traps

The ZyWALL will send traps to the SNMP manager when any one of the following events occurs:

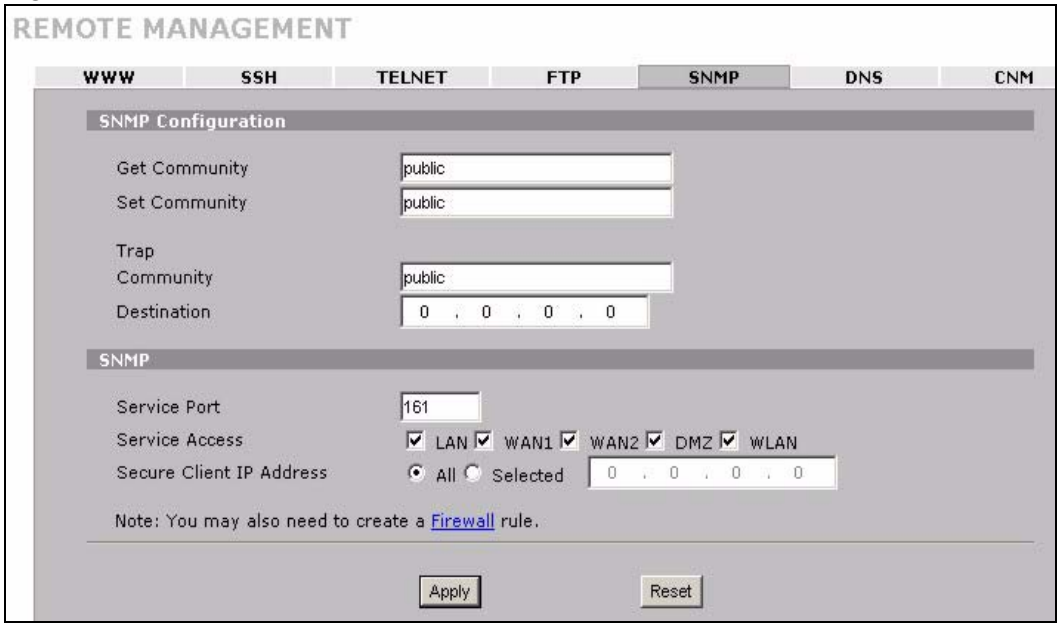
**Table 153** SNMP Traps

| TRAP # | TRAP NAME | DESCRIPTION |
|---|---|---|
| 0 | coldStart (defined in *RFC-1215*) | A trap is sent after booting (power on). |
| 1 | warmStart (defined in *RFC-1215*) | A trap is sent after booting (software reboot). |
| 4 | authenticationFailure (defined in *RFC-1215*) | A trap is sent to the manager when receiving any SNMP get or set requirements with the wrong community (password). |
| 6 | whyReboot (defined in ZYXEL-MIB) | A trap is sent with the reason of restart before rebooting when the system is going to restart (warm start). |
| 6a | For intentional reboot : | A trap is sent with the message "System reboot by user!" if reboot is done intentionally, (for example, download new files, CI command "sys reboot", etc.). |
| 6b | For fatal error : | A trap is sent with the message of the fatal code if the system reboots because of fatal errors. |

## 27.9.1 Configuring the SNMP Screen

To change your ZyWALL's SNMP settings, click **ADVANCED** > **REMOTE MGMT** > **SNMP**. The screen appears as shown.

**Figure 310** ADVANCED > REMOTE MGMT > SNMP



The following table describes the labels in this screen.

**Table 154** ADVANCED > REMOTE MGMT > SNMP

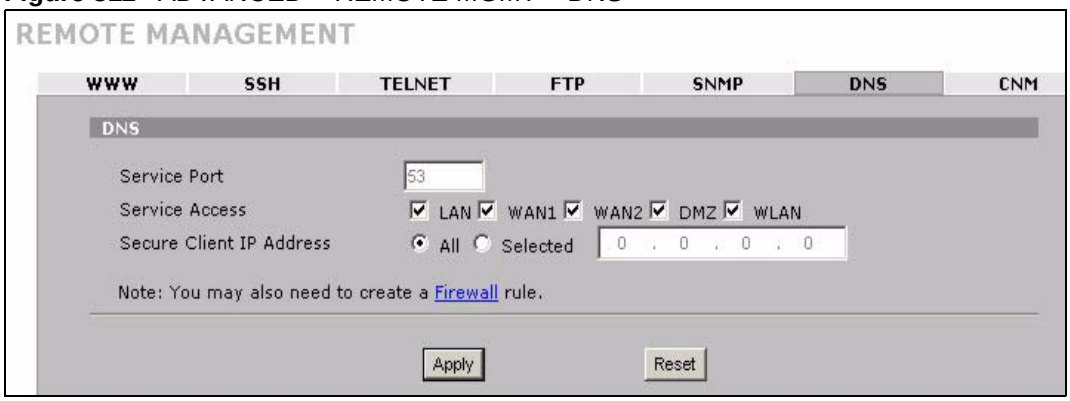
| LABEL | DESCRIPTION |
|---|---|
| SNMP Configuration | |
| Get Community | Enter the **Get Community**, which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests. |
| Set Community | Enter the **Set community**, which is the password for incoming Set requests from the management station. The default is public 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. |
| SNMP | |
| Service 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 Access | Select the interface(s) through which a computer may access the ZyWALL using this service. |
| Secure Client IP Address | A secure client is a “trusted” computer that is allowed to communicate with the ZyWALL using this service.<br>Select **All** to allow any computer to access the ZyWALL using this service.<br>Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyWALL using this service. |
| Apply | Click **Apply** to save your customized settings. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 27.10 The DNS Screen

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa. Refer to Chapter 9 on page 169 for more information.

Click **ADVANCED** > **REMOTE MGMT** > **DNS** to change your ZyWALL’s DNS settings. Use this screen to set from which IP address the ZyWALL will accept DNS queries and on which interface it can send them your ZyWALL’s DNS settings. This feature is not available when the ZyWALL is set to bridge mode.

**Figure 311** ADVANCED > REMOTE MGMT > DNS




The following table describes the labels in this screen.

**Table 155** ADVANCED > REMOTE MGMT > DNS

| LABEL | DESCRIPTION |
|---|---|
| Server Port | The DNS service port number is 53 and cannot be changed here. |
| Service Access | Select the interface(s) through which a computer may send DNS queries to the ZyWALL. |
| Secure Client IP Address | A secure client is a “trusted” computer that is allowed to send DNS queries to the ZyWALL.<br>Select **All** to allow any computer to send DNS queries to the ZyWALL.<br>Choose **Selected** to just allow the computer with the IP address that you specify to send DNS queries to the ZyWALL. |
| Apply | Click **Apply** to save your customized settings. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 27.11 The CNM Screen

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, SMT menus or commands) without notifying the Vantage CNM administrator.

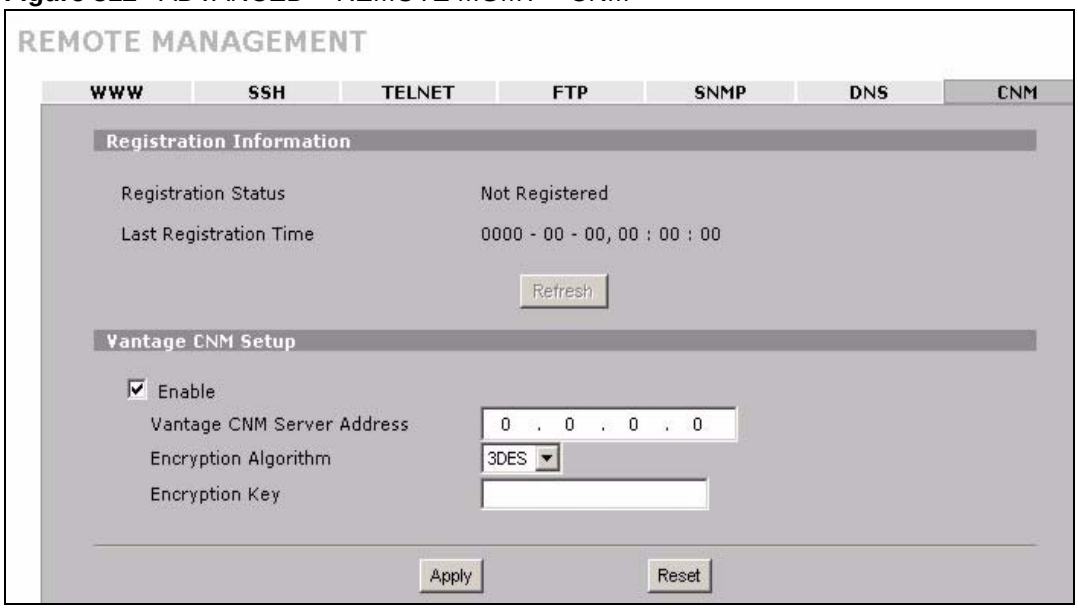
### Additional Configuration for Vantage CNM

If you have NAT routers or firewalls between the ZyWALL and the Vantage CNM server, you must configure them to forward TCP ports 8080 (HTTP), 443 (HTTPS) and 20 and 21 (FTP). They must also forward UDP ports 1864 and 1865.

## 27.12 Configuring the CNM Screen

Vantage CNM is disabled on the device by default. Click **ADVANCED** > **REMOTE MGMT** > **CNM** to configure your device’s Vantage CNM settings.

**Figure 312** ADVANCED > REMOTE MGMT > CNM




The following table describes the labels in this screen.

**Table 156** ADVANCED > REMOTE MGMT > CNM

| LABEL | DESCRIPTION |
|---|---|
| Registration Information | |
| Registration Status | This read only field displays **Not Registered** when **Enable** is not selected.<br>It displays **Registering** when the ZyWALL first connects with the Vantage CNM server and then **Registered** after it has been successfully registered with the Vantage CNM server. It will continue to display **Registering** until it successfully registers with the Vantage CNM server. It will not be able to register with the Vantage CNM server if:<br>The Vantage CNM server is down.<br>The Vantage CNM server IP address is incorrect.<br>The Vantage CNM server is behind a NAT router or firewall that does not forward packets through to the Vantage CNM server.<br>The encryption algorithms and/or encryption keys do not match between the ZyWALL and the Vantage CNM server. |
| Last Registration Time | This field displays the last date (year-month-date) and time (hours-minutes-seconds) that the ZyWALL registered with the Vantage CNM server. It displays all zeroes if it has not yet registered with the Vantage CNM server. |
| Refresh | Click **Refresh** to update the registration status and last registration time. |
| Vantage CNM Setup | |
| Enable | Select this check box to allow Vantage CNM to manage your ZyWALL. |
| Vantage CNM Server Address | If the Vantage server is on the same subnet as the ZyXEL device, enter the private or public IP address of the Vantage server.<br>If the Vantage CNM server is on a different subnet to the ZyWALL, enter the public IP address of the Vantage server.<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. |

**Table 156** ADVANCED > REMOTE MGMT > CNM (continued)

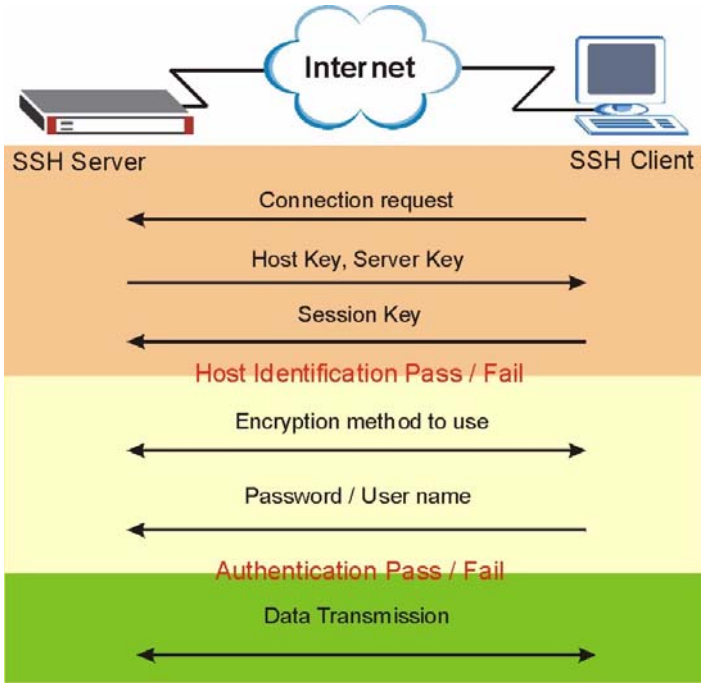
| LABEL | DESCRIPTION |
|---|---|
| Encryption Algorithm | The **Encryption Algorithm** field is used to encrypt communications between the ZyWALL and the Vantage CNM server. Choose from **None** (no encryption), **DES** or **3DES**. The **Encryption Key** field appears when you select **DES** or **3DES**. The ZyWALL must use the same encryption algorithm as the Vantage CNM server. |
| Encryption Key | Type eight alphanumeric characters ("0" to "9", "a" to "z" or "A" to "Z") when you choose the **DES** encryption algorithm and 24 alphanumeric characters ("0" to "9", "a" to "z" or "A" to "Z") when you choose the **3DES** encryption algorithm. The ZyWALL must use the same encryption key as the Vantage CNM server. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 27.13 Remote Management Technical Reference

## How SSH Works

The following table summarizes how a secure connection is established between two remote hosts.

**Figure 313** How SSH Works




**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.

# 28

# UPnP Screens

## 28.1 Overview

This chapter introduces the Universal Plug and Play feature. This chapter is only applicable when the ZyWALL is in router mode.

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

### 28.1.1 What You Can Do in the UPnP Screens

- Use the **UPnP** screen (Section 28.3 on page 526) to configure the ZyWALL's UPnP settings.
- Use the **UPnP Ports** screen (Section 28.4 on page 527) to view the NAT port mapping rules that UPnP creates on the ZyWALL.

### 28.1.2 What You Need To Know About UPnP

#### How Do I Know If I'm Using UPnP?

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

#### NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

- Dynamic port mapping
- Learning public IP addresses
- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

See Chapter 22 on page 436 for further information about NAT.

### Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

When a UPnP device joins a network, it announces its presence with a multicast message. For security reasons, the ZyWALL allows multicast messages on the LAN only.

All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

### UPnP and ZyXEL

ZyXEL has achieved UPnP certification from the Universal Plug and Play Forum UPnP™ Implementers Corp. (UIC). ZyXEL's UPnP implementation supports IGD 1.0 (Internet Gateway Device).

See the following sections for examples of installing and using UPnP.

## 28.2 UPnP Examples

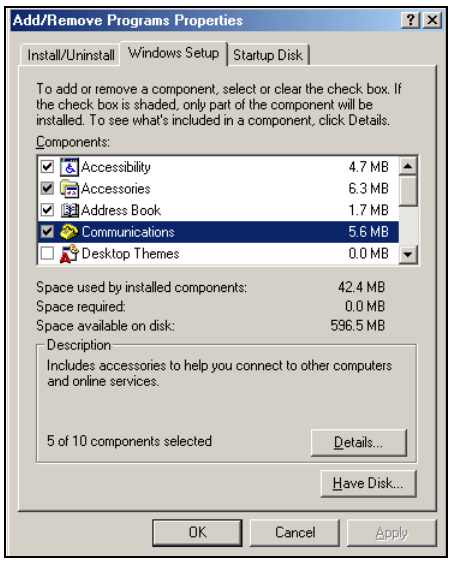
### 28.2.1 Installing UPnP in Windows Example

This section shows how to install UPnP in Windows Me and Windows XP.

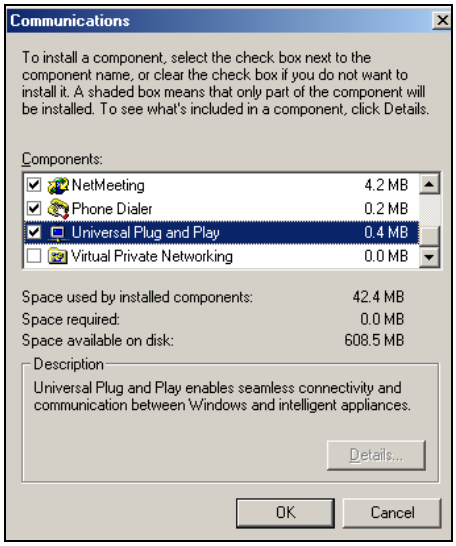
#### 28.2.1.1 Installing UPnP in Windows Me

Follow the steps below to install UPnP in Windows Me.

1. Click **Start**, **Settings** and **Control Panel**. Double-click **Add/Remove Programs**.
2. Click on the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.



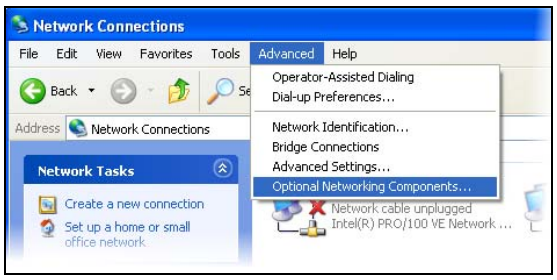

3. In the **Communications** window, select the **Universal Plug and Play** check box in the **Components** selection box.
4. Click **OK** to go back to the **Add/Remove Programs Properties** window and click **Next**.
5. Restart the computer when prompted.



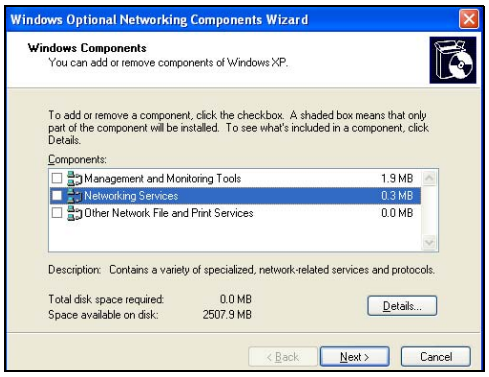
### 28.2.1.2 Installing UPnP in Windows XP

Follow the steps below to install UPnP in Windows XP.

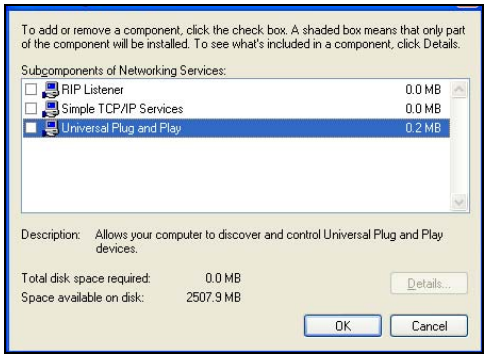
1. Click **Start**, **Settings** and **Control Panel**.
2. Double-click **Network Connections**.
3. In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ….**
   The **Windows Optional Networking Components Wizard** window displays.




4. Select **Networking Service** in the **Components** selection box and click **Details**.




5. In the **Networking Services** window, select the **Universal Plug and Play** check box.
6. Click **OK** to go back to the **Windows Optional Networking Component Wizard** window and click **Next**.



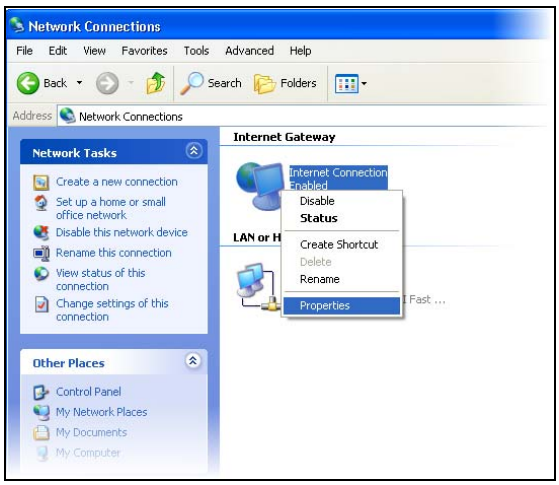

## 28.2.2 Using UPnP in Windows XP Example

This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the ZyXEL device.

Make sure the computer is connected to a LAN port of the ZyXEL device. Turn on your computer and the ZyXEL device.

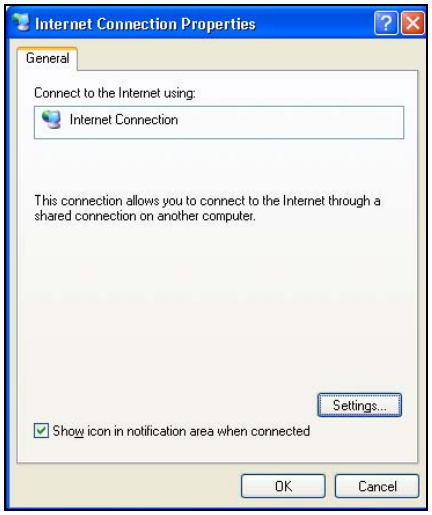
### 28.2.2.1 Auto-discover Your UPnP-enabled Network Device

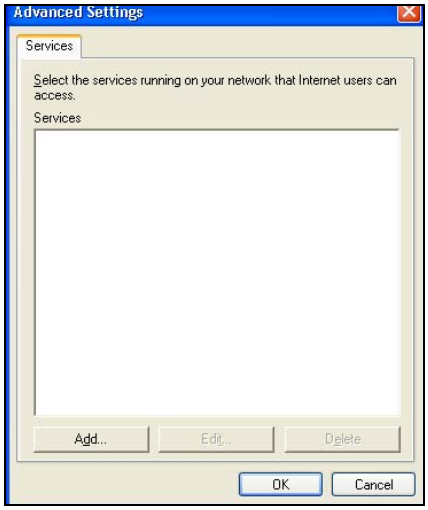
1. Click **Start** and **Control Panel**. Double-click **Network Connections**. An icon displays under **Internet Gateway**.
2. Right-click the icon and select **Properties**.

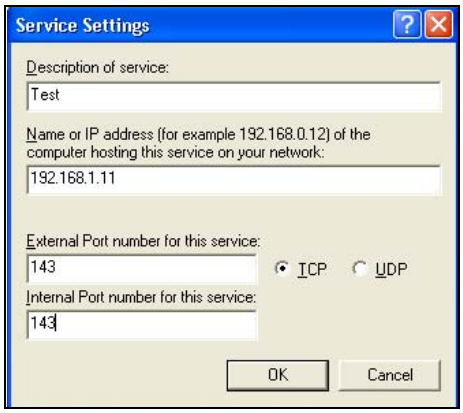



3. In the **Internet Connection Properties** window, click **Settings** to see the port mappings that were automatically created.

You may edit or delete the port mappings or click **Add** to manually add port mappings.






When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

4 Select the **Show icon in notification area when connected** check box and click **OK**. An icon displays in the system tray.

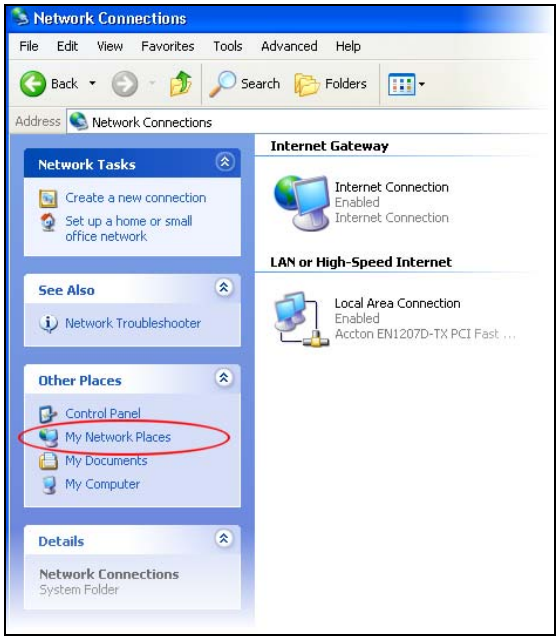

5 Double-click the icon to display your current Internet connection status.


### 28.2.2.2 Web Configurator Easy Access

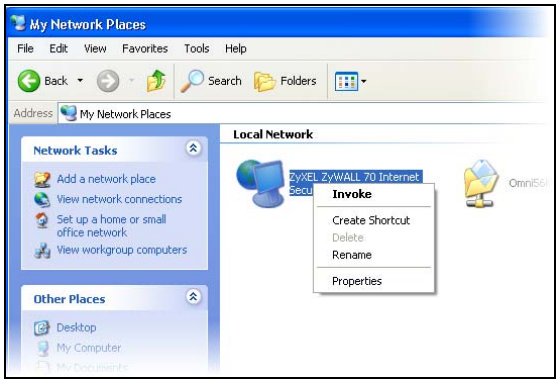
With UPnP, you can access the web-based configurator on the ZyXEL device without finding out the IP address of the ZyXEL device first. This is helpful if you do not know the IP address of the ZyXEL device.

Follow the steps below to access the web configurator.

1. Click **Start** and then **Control Panel**.
2. Double-click **Network Connections**.
3. Select **My Network Places** under **Other Places**.




4. An icon with the description for each UPnP-enabled device displays under **Local Network**.
5. Right-click the icon for your ZyXEL device and select **Invoke**. The web configurator login screen displays.



6 Right-click the icon for your ZyXEL device and select **Properties**. A properties window displays with basic information about the ZyXEL device.


## 28.3 The UPnP Screen

Click **ADVANCED** > **UPnP** to display the **UPnP** screen.

**Figure 314** ADVANCED > UPnP


The following table describes the fields in this screen.

**Table 157** ADVANCED > UPnP

| LABEL | DESCRIPTION |
|---|---|
| UPnP Setup | |
| Device Name | This identifies the ZyXEL device in UPnP applications. |
| Enable the Universal Plug and Play (UPnP) feature | Select this check box to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the ZyWALL's IP address (although you must still enter the password to access the web configurator). |

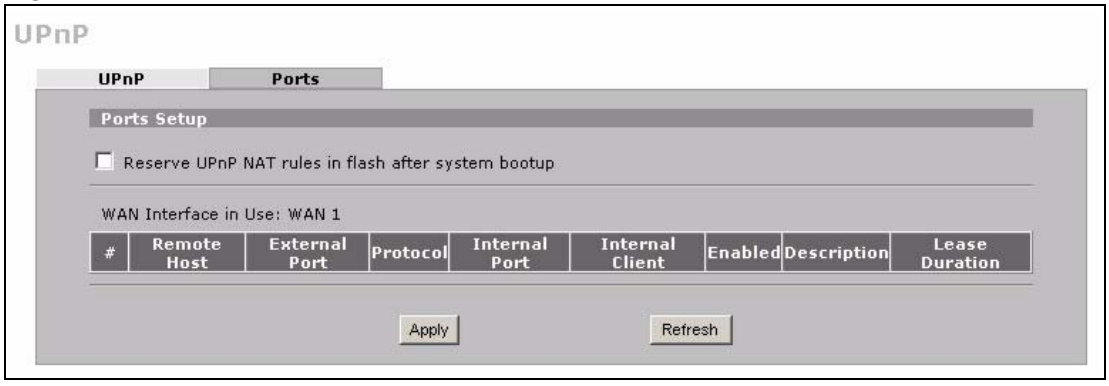
**Table 157** ADVANCED > UPnP

| LABEL | DESCRIPTION |
|---|---|
| Allow users to make configuration changes through UPnP | Select this check box to allow UPnP-enabled applications to automatically configure the ZyWALL so that they can communicate through the ZyWALL, for example by using NAT traversal, UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application. |
| Allow UPnP to pass through Firewall | Select this check box to allow traffic from UPnP-enabled applications to bypass the firewall.<br>Clear this check box to have the firewall block all UPnP application packets (for example, MSN packets). |
| Outgoing WAN Interface | Select through which WAN port you want to send out traffic from UPnP-enabled applications. If the WAN port you select loses its connection, the ZyWALL attempts to use the other WAN port. If the other WAN port also does not work, the ZyWALL drops outgoing packets from UPnP-enabled applications. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 28.4 The Ports Screen

Click **ADVANCED** > **UPnP** > **Ports** to display the UPnP Ports screen. Use this screen to view the NAT port mapping rules that UPnP creates on the ZyWALL.

**Figure 315** ADVANCED > UPnP > Ports




The following table describes the labels in this screen.

**Table 158** ADVANCED > UPnP > Ports

| LABEL | DESCRIPTION |
|---|---|
| Reserve UPnP NAT rules in flash after system bootup | Select this check box to have the ZyWALL retain UPnP created NAT rules even after restarting. If you use UPnP and you set a port on your computer to be fixed for a specific service (for example FTP for file transfers), this option allows the ZyWALL to keep a record when your computer uses UPnP to create a NAT forwarding rule for that service. |
| WAN Interface in Use | This field displays through which WAN interface the ZyWALL is currently sending out traffic from UPnP-enabled applications. This field displays **None** when UPnP is disabled or neither of the WAN ports has a connection. |
| The following read-only table displays information about the UPnP-created NAT mapping rule entries in the ZyWALL's NAT routing table. | |

**Table 158** ADVANCED > UPnP > Ports (continued)

| LABEL | DESCRIPTION |
|---|---|
| # | This is the index number of the UPnP-created NAT mapping rule entry. |
| Remote Host | This field displays the source IP address (on the WAN) of inbound IP packets. Since this is often a wildcard, the field may be blank. When the field is blank, the ZyWALL forwards all traffic sent to the **External Port** on the WAN interface to the **Internal Client** on the **Internal Port**. When this field displays an external IP address, the NAT rule has the ZyWALL forward inbound packets to the **Internal Client** from that IP address only. |
| External Port | This field displays the port number that the ZyWALL “listens” on (on the WAN port) for connection requests destined for the NAT rule’s **Internal Port** and **Internal Client**. The ZyWALL forwards incoming packets (from the WAN) with this port number to the **Internal Client** on the **Internal Port** (on the LAN). If the field displays “0”, the ZyWALL ignores the **Internal Port** value and forwards requests on all external port numbers (that are otherwise unmapped) to the **Internal Client**. |
| Protocol | This field displays the protocol of the NAT mapping rule (TCP or UDP). |
| Internal Port | This field displays the port number on the **Internal Client** to which the ZyWALL should forward incoming connection requests. |
| Internal Client | This field displays the DNS host name or IP address of a client on the LAN. Multiple NAT clients can use a single port simultaneously if the internal client field is set to 255.255.255.255 for UDP mappings. |
| Enabled | This field displays whether or not this UPnP-created NAT mapping rule is turned on. The UPnP-enabled device that connected to the ZyWALL and configured the UPnP-created NAT mapping rule on the ZyWALL determines whether or not the rule is enabled. |
| Description | This field displays a text explanation of the NAT mapping rule. |
| Lease Duration | This field displays a dynamic port-mapping rule’s time to live (in seconds). It displays “0” if the port mapping is static. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Refresh | Click **Refresh** update the screen’s table. |

# 29

# Custom Application Screen

## 29.1 Overview

Use custom application to have the ZyWALL's ALG, anti-spam, anti-virus, and content filtering features monitor traffic on custom ports, in addition to the default ports.

### 29.1.1 What You Can Do in the Custom Application Screen

Use the **Custom App** screen (Section 29.2 on page 529) to configure custom application settings on the ZyWALL.

### 29.1.2 What You Need to Know About Custom Application

#### Default ports

By default, these ZyWALL features monitor traffic for the following protocols on these port numbers.

- FTP: 21
- SIP: 5060
- H.323: 1720
- SMTP: 25
- POP3: 110
- HTTP: 80

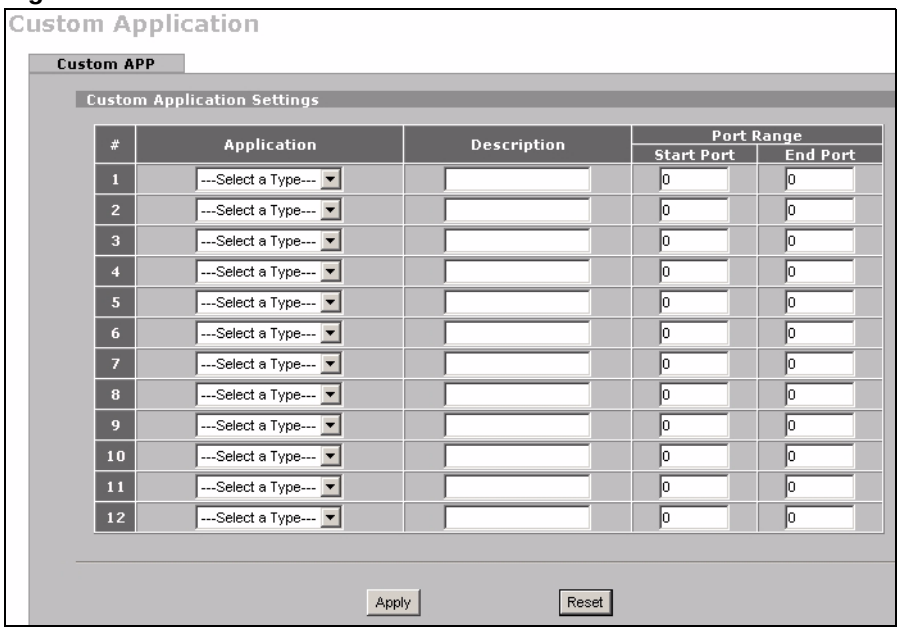
## 29.2 The Custom Application Screen

Click **ADVANCED > Custom APP** to open the **Custom Application** screen. Use this screen to configure port(s) that the ZyWALL monitors for application-specific traffic.

This screen only specifies what port numbers the ZyWALL checks for specific protocol traffic. Use other screens to enable or disable the monitoring of the protocol traffic.

Changes in the **Custom APP** screen do not apply to the firewall.

**Figure 316** ADVANCED > Custom APP




The following table describes the labels in this screen.

**Table 159** ADVANCED > Custom APP

| LABEL | DESCRIPTION |
|---|---|
| Application | Select the application for which you want the ZyWALL to monitor specific ports. You can use the same application in more than one entry. To remove an entry, select **Select a Type**. |
| Description | Enter information about the reason for monitoring custom port numbers for this protocol. |
| Start Port | Enter the starting port for the range that the ZyWALL is to monitor for this application. If you are only entering a single port number, enter it here. |
| End Port | Enter the ending port for the range that the ZyWALL is to monitor for this application. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# 30

# ALG Screen

## 30.1 Overview

This chapter covers how to use the ZyWALL's ALG feature to allow certain applications to pass through the ZyWALL.

An Application Layer Gateway (ALG) manages a specific protocol (such as SIP, H.323 or FTP) at the application layer. The ZyWALL can function as an ALG to allow certain NAT un-friendly applications (such as SIP) to operate properly through the ZyWALL.

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 data stream. When a device behind the ZyWALL uses an application for which the ZyWALL has ALG service 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 dynamically creates implicit NAT port forwarding and firewall rules for the application's traffic to come in from the WAN to the LAN.

To configure the ALG screen proceed to Section 30.2 on page 535.

See Section 29.2 on page 529 if you need to use the ALG for SIP, H.323 or FTP traffic on custom ports.

### 30.1.1 What You Need to Know About ALG

#### ALG and NAT

The ZyWALL dynamically creates an implicit NAT session for the application's traffic from the WAN to the LAN.

The ALG on the ZyWALL supports all NAT mapping types, including **One to One**, **Many to One**, **Many to Many Overload** and **Many One to One**.

### ALG and the Firewall

The ZyWALL uses the dynamic port that the session uses for data transfer in creating an implicit temporary firewall rule for the session's traffic. The firewall rule only allows the session's traffic to go through in the direction that the ZyWALL determines from its inspection of the data payload of the application's packets. The firewall rule is automatically deleted after the application's traffic has gone through.

### ALG and Multiple WAN

When the ZyWALL has two WAN interfaces and uses the second highest priority WAN interfaces as a back up, traffic cannot pass through when the primary WAN connection fails. The ZyWALL does not automatically change the connection to the secondary WAN interfaces.

If the primary WAN connection fails, the client needs to re-initialize the connection through the secondary WAN interfaces to have the connection go through the secondary WAN interfaces.

When the ZyWALL uses both of the WAN interfaces at the same time, you can configure routing policies to specify the WAN interfaces that the connection's traffic is to use.

### 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.

If the FTP server is located on the LAN, you must also configure NAT port forwarding and firewall rules if you want to allow access to the server from the WAN.

### 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.

### RTP

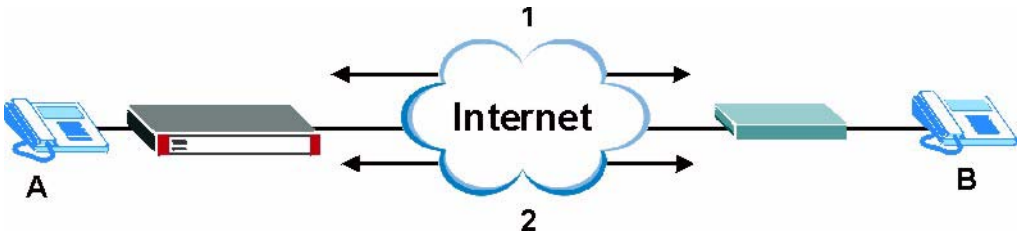
When you make a VoIP call using H.323 or SIP, the RTP (Real time Transport Protocol) is used to handle voice data transfer. See RFC 1889 for details on RTP.

### H.323 ALG Details

- 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.

- You must configure the firewall and port forwarding to allow incoming (peer-to-peer) calls from the WAN to a private IP address on the LAN, DMZ or WLAN. The following example shows H.323 signaling (1) and audio (2) sessions between H.323 devices A and B.

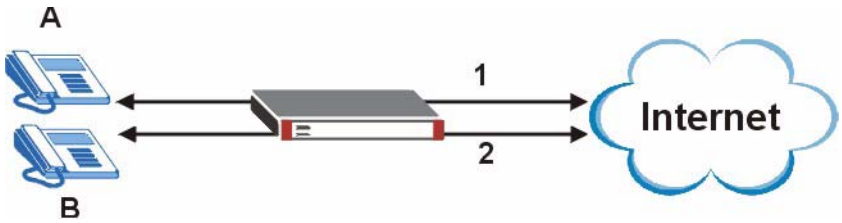
**Figure 317** H.323 ALG Example




- With multiple WAN IP addresses on the ZyWALL, you can configure different firewall and port forwarding rules to allow incoming calls from each WAN IP address to go to a specific IP address on the LAN, DMZ or WLAN. Use policy routing to have the H.323 calls from each of those LAN, DMZ or WLAN 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 port forwarding 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**.

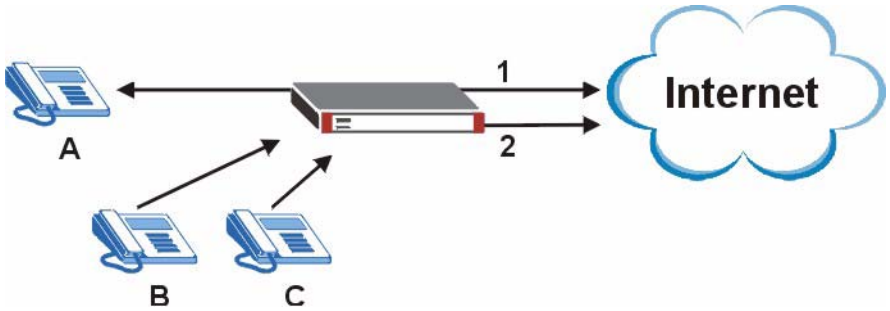
**Figure 318** H.323 with Multiple WAN IP Addresses




- When you configure the firewall and 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 calls from other LAN, DMZ or WLAN 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, DMZ or WLAN IP addresses.

  For example, you configure the firewall and port forwarding 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 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 319** H.323 Calls from the WAN with Multiple Outgoing Calls




- The H.323 ALG operates on TCP packets with a port 1720 destination.
- The ZyWALL allows H.323 audio connections.
- The ZyWALL can also apply bandwidth management to traffic that goes through the H.323 ALG.

### 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.

### STUN

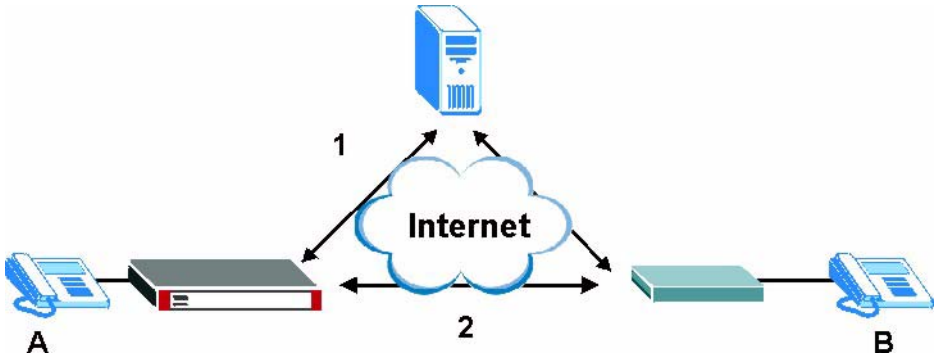
STUN (Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators) allows the VoIP device to find the presence and types of NAT routers and/or firewalls between it and the public Internet. STUN also allows the VoIP device to find the public IP address that NAT assigned, so the VoIP device can embed it in the SIP data stream. See RFC 3489 for details on STUN. You do not need to use STUN for devices behind the ZyWALL if you enable the SIP ALG.

### SIP ALG Details

- SIP clients can be connected to the LAN, WLAN or DMZ. A SIP server must be on the WAN.
- You can make and receive calls between the LAN and the WAN, between the WLAN and the WAN and/or between the DMZ and the WAN. You cannot make a call between the LAN and the LAN, between the LAN and the DMZ, between the LAN and the WLAN, between the DMZ and the DMZ, and so on.
- The SIP ALG allows UDP packets with a port 5060 destination to pass through.
- The ZyWALL allows SIP audio connections.

The following example shows SIP signaling (**1**) and audio (**2**) sessions between SIP clients **A** and **B** and the SIP server.

**Figure 320** SIP ALG Example




### SIP Signaling Session Timeout

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.

If the SIP client does not have this mechanism and makes no calls during the ZyWALL SIP timeout default (60 minutes), the ZyWALL SIP ALG drops any incoming calls after the timeout period.

### SIP Audio Session Timeout

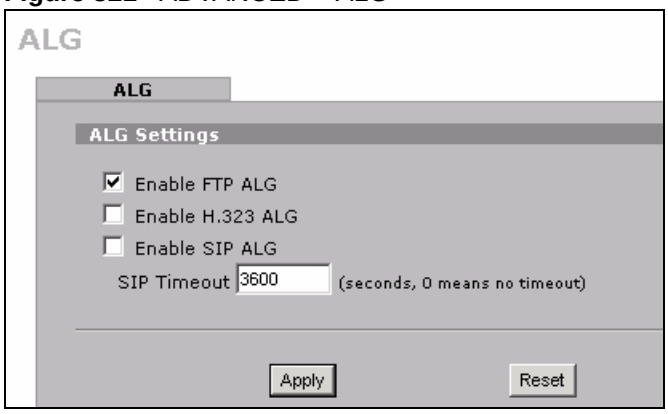
If no voice packets go through the SIP ALG before the timeout period (default 5 minutes) expires, the SIP ALG does not drop the call but blocks all voice traffic and deletes the audio session. You cannot hear anything and you will need to make a new call to continue your conversation.

## 30.2 The ALG Screen

Click **ADVANCED** > **ALG** to open the **ALG** screen. Use the **ALG** screen to turn individual ALGs off or on and set the SIP timeout.

If the ZyWALL provides an ALG for a service, you must enable the ALG in order to perform bandwidth management on that service’s traffic.

**Figure 321** ADVANCED > ALG




The following table describes the labels in this screen.

**Table 160** ADVANCED > ALG

| LABEL | DESCRIPTION |
|---|---|
| Enable FTP ALG | Select this check box to allow FTP sessions to pass through the ZyWALL. FTP (File Transfer Program) is a program that enables fast transfer of files, including large files that may not be possible by e-mail. |
| Enable H.323 ALG | Select this check box to allow H.323 sessions to pass through the ZyWALL. H.323 is a protocol used for audio communications over networks. |
| Enable SIP ALG | Select this check box to allow SIP sessions to pass through the ZyWALL. SIP is a signaling protocol used in VoIP (Voice over IP), the sending of voice signals over Internet Protocol. |
| SIP Timeout | 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>If the SIP client does not have this mechanism and makes no calls during the ZyWALL SIP timeout (default 60 minutes), the ZyWALL SIP ALG drops any incoming calls after the timeout period. Enter the SIP signaling session timeout value. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# PART V
# Reports, Logs and Maintenance

# 31

# Reports Screens

## 31.1 Overview

The **Reports** screens display statistics about network usage and IDP, anti-virus and anti-spam statistics. You can also configure how reports are emailed.

### 31.1.1 What You Can Do in the Reports Screens

- Use the **Traffic Statistics** screen (Section 31.2 on page 539) to view statistics on traffic on an interface.
- Use the **IDP** screen (Section 31.3 on page 545) to view statistics on intrusion detection.
- Use the **Anti-Virus** screen (Section 31.4 on page 547) to view antivirus statistics.
- Use the **Anti-Spam** screen (Section 31.5 on page 549) to view antispam statistics.
- Use the **E-mail Report** screen (Section 31.6 on page 551) to configure the ZyWALL to email a report including statistics provided in the report screens.

#### Finding Out More

See the chapters about content filtering, anti-virus, anti-spam and IDP for more information on these features.

## 31.2 The Traffic Statistics Screen

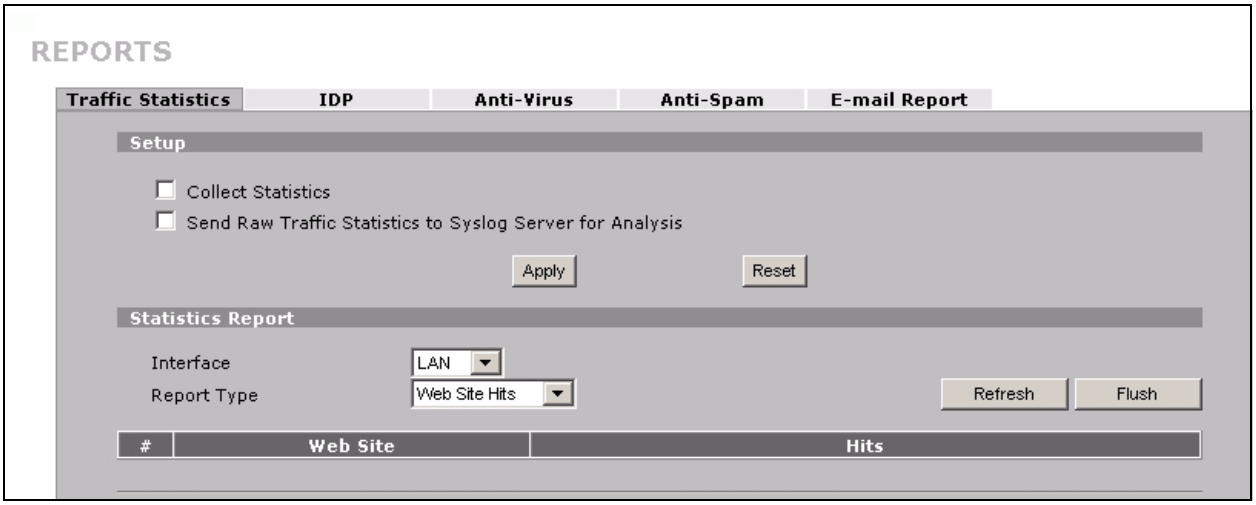
Click **REPORTS** to display the following screen.

The **Traffic Statistics** screen displays which local computers send and receive the most traffic, what kinds of traffic are used the most and which web sites are visited the most often. The ZyWALL can record and display the following network usage details:

- Web sites visited the most often
- Number of times the most visited web sites were visited
- The most-used protocols or service ports
- The amount of traffic for the most used protocols or service ports
- The LAN, DMZ or WLAN IP addresses to and/or from which the most traffic has been sent
- How much traffic has been sent to and from the LAN, DMZ or WLAN IP addresses to and/or from which the most traffic has been sent.

The web site hit count may not be 100% accurate because sometimes when an individual web page loads, it may contain references to other web sites that also get counted as hits.

**Figure 322** REPORTS > Traffic Statistics




Enabling the ZyWALL's reporting function decreases the overall throughput by about 1 Mbps.

The following table describes the labels in this screen.

**Table 161** REPORTS > Traffic Statistics

| LABEL | DESCRIPTION |
|---|---|
| Collect Statistics | Select the check box and click **Apply** to have the ZyWALL record report data. |
| Send Raw Traffic Statistics to Syslog Server for Analysis | Select the check box and click **Apply** to have the ZyWALL send unprocessed traffic statistics to a syslog server for analysis.<br>You must have the syslog server already configured in the **Log Settings** screen. |
| Apply | Click **Apply** to save your changes to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |
| Interface | Select on which interface (**LAN**, **DMZ** or **WLAN**) the logs will be collected. The logs on the DMZ, LAN or WLAN IP alias 1 and 2 are also recorded. |

**Table 161** REPORTS > Traffic Statistics

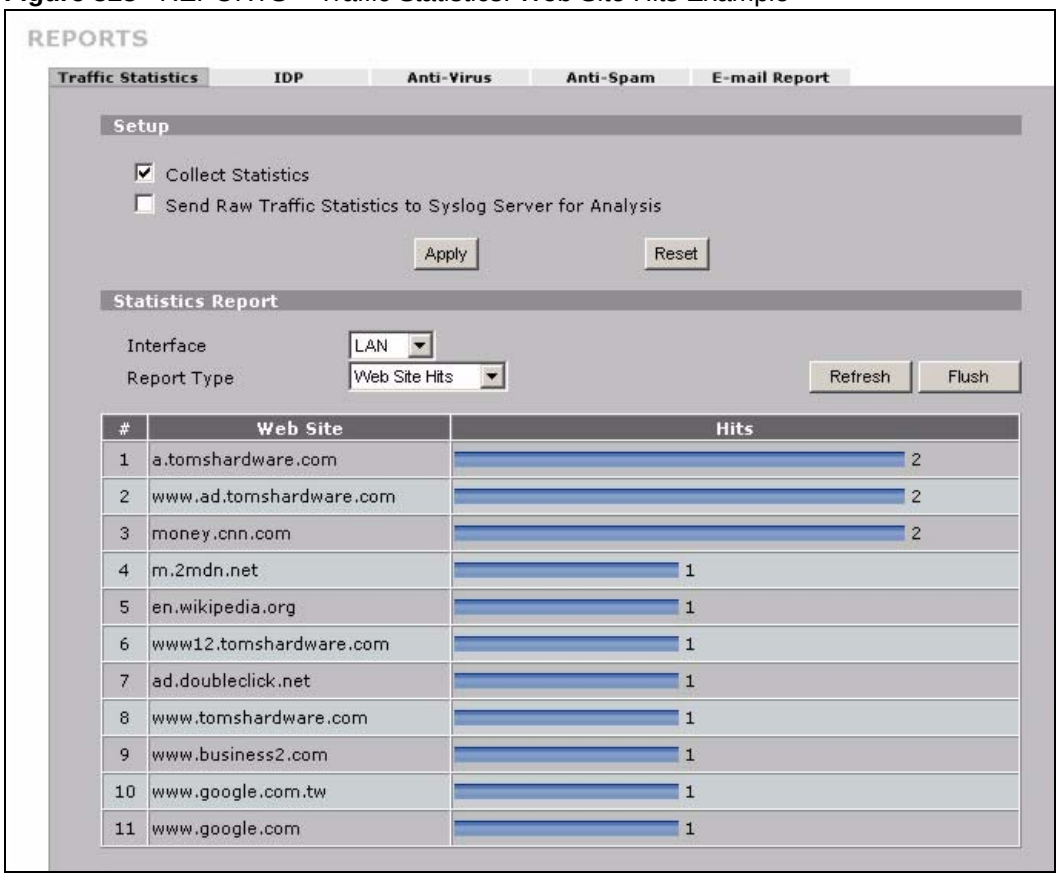
| LABEL | DESCRIPTION |
|---|---|
| Report Type | Use the drop-down list box to select the type of reports to display.<br>**Web Site Hits** displays the web sites that have been visited the most often from the LAN and how many times they have been visited.<br>**Protocol/Port** displays the protocols or service ports that have been used the most and the amount of traffic for the most used protocols or service ports.<br>**Host IP Address** displays the LAN, DMZ or WLAN IP addresses to and /or from which the most traffic has been sent and how much traffic has been sent to and from those IP addresses. |
| Refresh | Click **Refresh** to update the report display. The report also refreshes automatically when you close and reopen the screen. |
| Flush | Click **Flush** to discard the old report data and update the report display. |

All of the recorded reports data is erased when you turn off the ZyWALL.

## 31.2.1 Viewing Web Site Hits

In the **Reports** screen, select **Web Site Hits** from the **Report Type** drop-down list box to have the ZyWALL record and display which web sites have been visited the most often and how many times they have been visited.

**Figure 323** REPORTS > Traffic Statistics: Web Site Hits Example




The following table describes the label in this screen.

**Table 162** REPORTS > Traffic Statistics: Web Site Hits Report

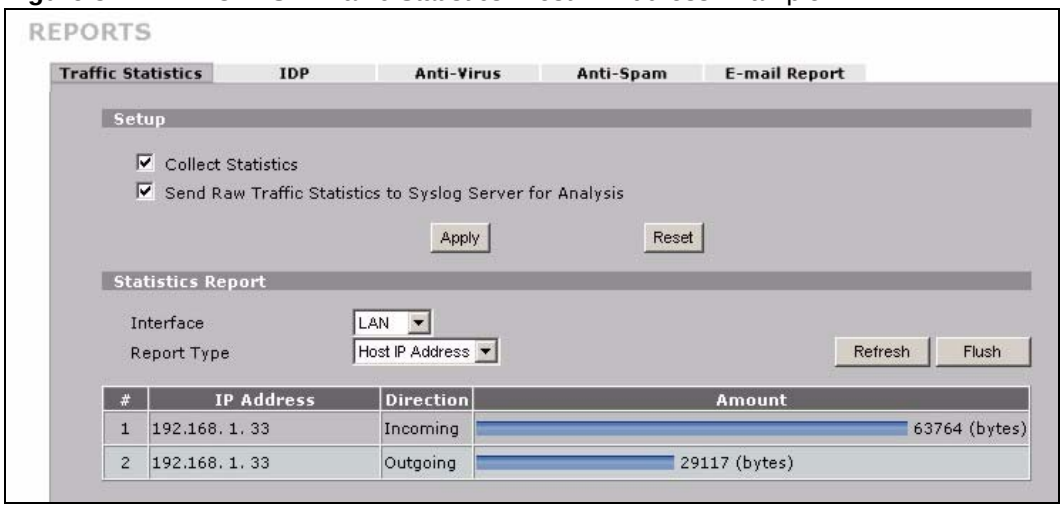
| LABEL | DESCRIPTION |
|---|---|
| Web Site | This column lists the domain names of the web sites visited most often from computers on the LAN, DMZ or WLAN. The names are ranked by the number of visits to each web site and listed in descending order with the most visited web site listed first. The ZyWALL counts each page viewed in a web site as another hit on the web site. |
| Hits | This column lists how many times each web site has been visited. The count starts over at 0 if a web site passes the hit count limit (see Table 165 on page 545). |

## 31.2.2 Viewing Host IP Address

In the **Reports** screen, select **Host IP Address** from the **Report Type** drop-down list box to have the ZyWALL record and display the LAN, DMZ or WLAN IP addresses that the most traffic has been sent to and/or from and how much traffic has been sent to and/or from those IP addresses.

Computers take turns using dynamically assigned LAN, DMZ or WLAN IP addresses. The ZyWALL continues recording the bytes sent to or from a LAN, DMZ or WLAN IP address when it is assigned to a different computer.

**Figure 324** REPORTS > Traffic Statistics: Host IP Address Example




The following table describes the labels in this screen.

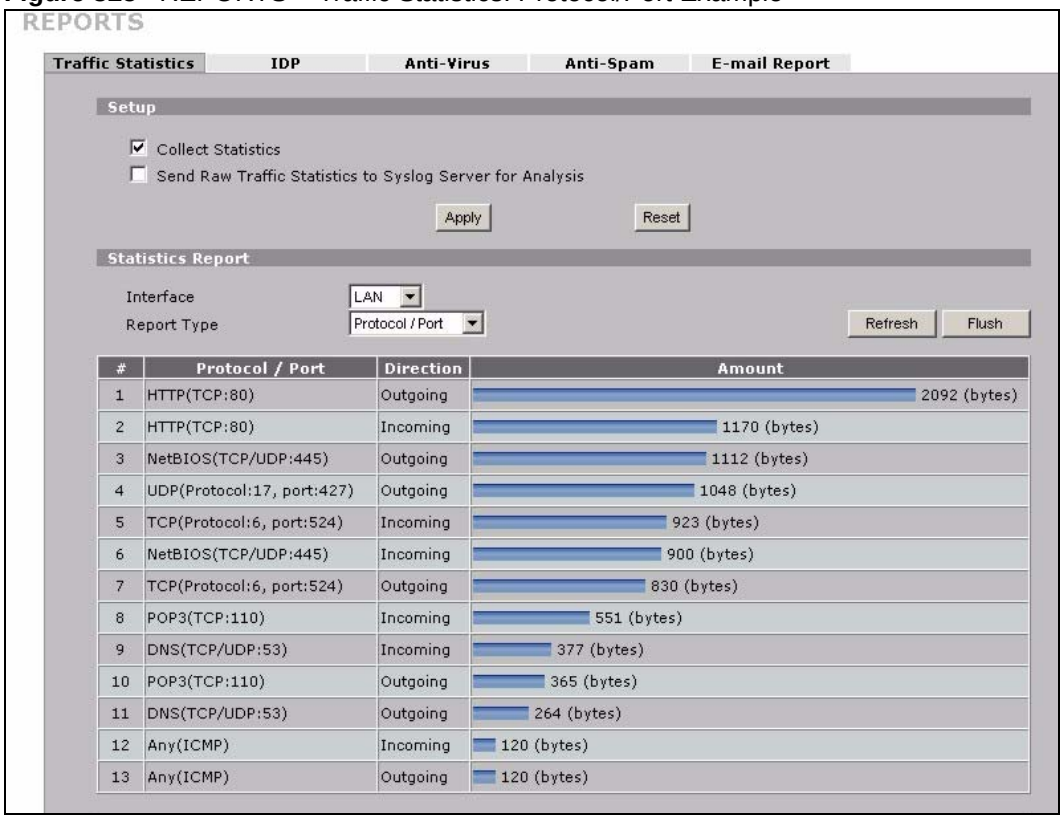
**Table 163** REPORTS > Traffic Statistics: Host IP Address

| LABEL | DESCRIPTION |
|---|---|
| IP Address | This column lists the LAN, DMZ or WLAN IP addresses to and/or from which the most traffic has been sent. The LAN, DMZ or WLAN IP addresses are listed in descending order with the LAN, DMZ or WLAN IP address to and/or from which the most traffic was sent listed first. |
| Direction | This field displays **Incoming** to denote traffic that is coming in from the WAN to the LAN, DMZ or WLAN. This field displays **Outgoing** to denote traffic that is going out from the LAN, DMZ or WLAN to the WAN. |
| Amount | This column displays how much traffic has gone to and from the listed LAN, DMZ or WLAN IP addresses. The measurement unit shown (bytes, Kbytes, Mbytes or Gbytes) varies with the amount of traffic sent to and from the LAN, DMZ or WLAN IP address. The count starts over at 0 if the total traffic sent to and from a LAN, DMZ or WLAN IP passes the bytes count limit (see Table 165 on page 545). |

## 31.2.3 Viewing Protocol/Port

In the **Reports** screen, select **Protocol/Port** from the **Report Type** drop-down list box to have the ZyWALL record and display which protocols or service ports have been used the most and the amount of traffic for the most used protocols or service ports.

**Figure 325** REPORTS > Traffic Statistics: Protocol/Port Example




The following table describes the labels in this screen.

**Table 164** REPORTS > Traffic Statistics: Protocol/ Port

| LABEL | DESCRIPTION |
|---|---|
| Protocol/Port | This column lists the protocols or service ports for which the most traffic has gone through the ZyWALL. The protocols or service ports are listed in descending order with the most used protocol or service port listed first. |
| Direction | This field displays **Incoming** to denote traffic that is coming in from the WAN to the LAN, DMZ or WLAN. This field displays **Outgoing** to denote traffic that is going out from the LAN, DMZ or WLAN to the WAN. |
| Amount | This column lists how much traffic has been sent and/or received for each protocol or service port. The measurement unit shown (bytes, Kbytes, Mbytes or Gbytes) varies with the amount of traffic for the particular protocol or service port. The count starts over at 0 if a protocol or port passes the bytes count limit (see Table 165 on page 545). |

### 31.2.4 System Reports Specifications

The following table lists detailed specifications on the reports feature.

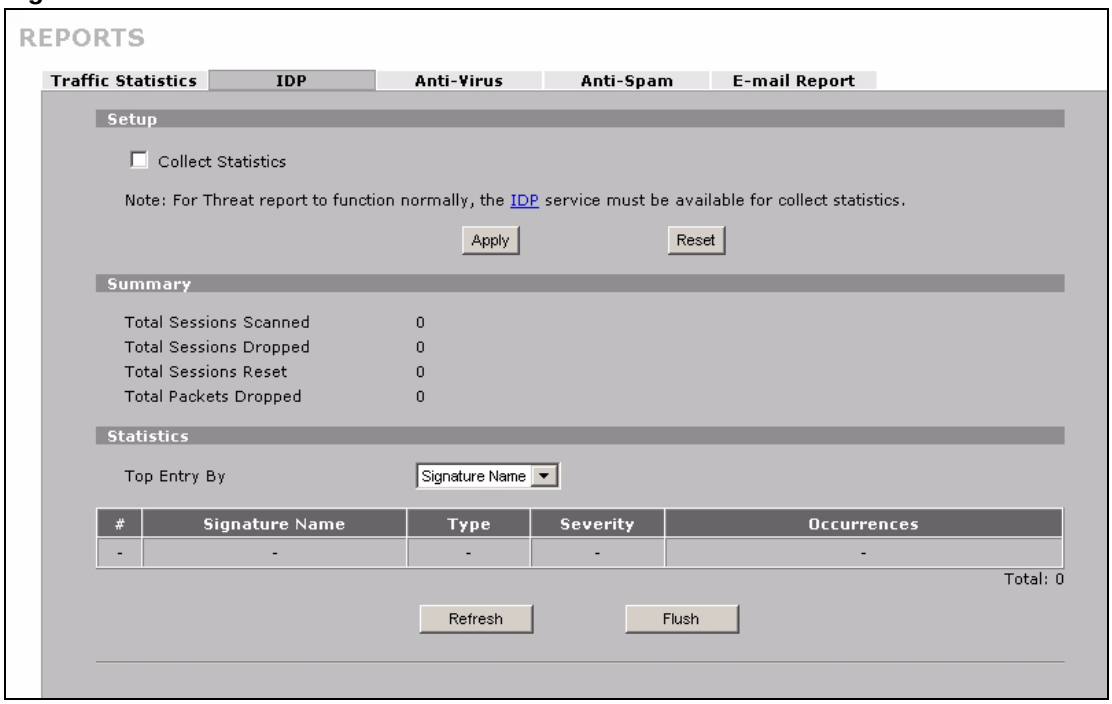
**Table 165** Report Specifications

| LABEL | DESCRIPTION |
|---|---|
| Number of web sites/protocols or ports/IP addresses listed: | 20 |
| Hit count limit: | Up to $2^{32}$ hits can be counted per web site. The count starts over at 0 if it passes four billion. |
| Bytes count limit: | Up to $2^{64}$ bytes can be counted per protocol/port or LAN IP address. The count starts over at 0 if it passes $2^{64}$ bytes. |

## 31.3 The IDP Screen

Click **REPORTS** > **IDP** to display the **IDP** screen. This screen displays IDP (Intrusion Detection and Prevention) statistics.

**Figure 326** REPORTS > IDP



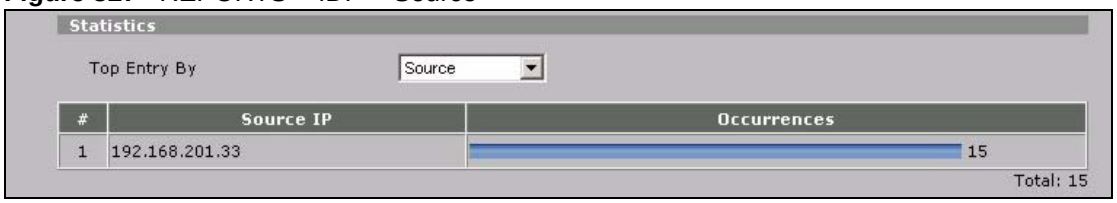
The following table describes the labels in this screen.

**Table 166** REPORTS > 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 the **Flush** button. Collecting starts over and a new collection start time displays. |
| Total Sessions Scanned | This field displays the number of sessions that the ZyWALL has checked for intrusion characteristics. |
| Total Sessions Dropped | The ZyWALL can detect and drop malicious sessions from network traffic. This field displays the number of sessions that the ZyWALL has dropped. |
| Total Sessions Reset | The ZyWALL can detect and reset suspicious network traffic sessions. This field displays the number of sessions that the ZyWALL has reset. |
| Total Packets Dropped | The ZyWALL can detect and drop malicious packets from network traffic. This field displays the number of packets that the ZyWALL has dropped. |
| 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>Select **Signature Name** to list the most common signatures that the ZyWALL has detected.<br>Select **Source** to list the source IP addresses from which the ZyWALL has detected the most intrusion attempts.<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 78 on page 281 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 79 on page 282 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. |
| Refresh | Click **Refresh** to update the report display with additional information that the ZyWALL may have collected while you had the screen open. The report also refreshes automatically when you close and reopen the screen. |
| Flush | Click **Flush** to discard the report data and restart collecting statistics. |

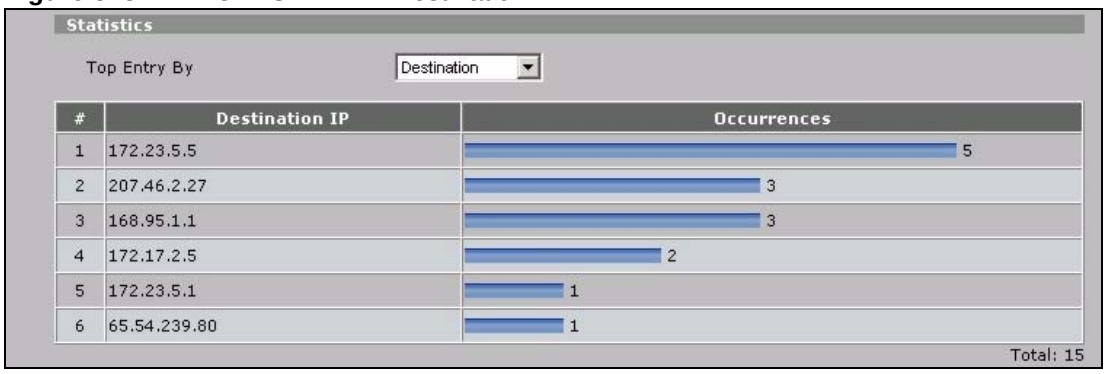
The statistics display as follows when you display the top entries by source.

**Figure 327** REPORTS > IDP > Source




The statistics display as follows when you display the top entries by destination.

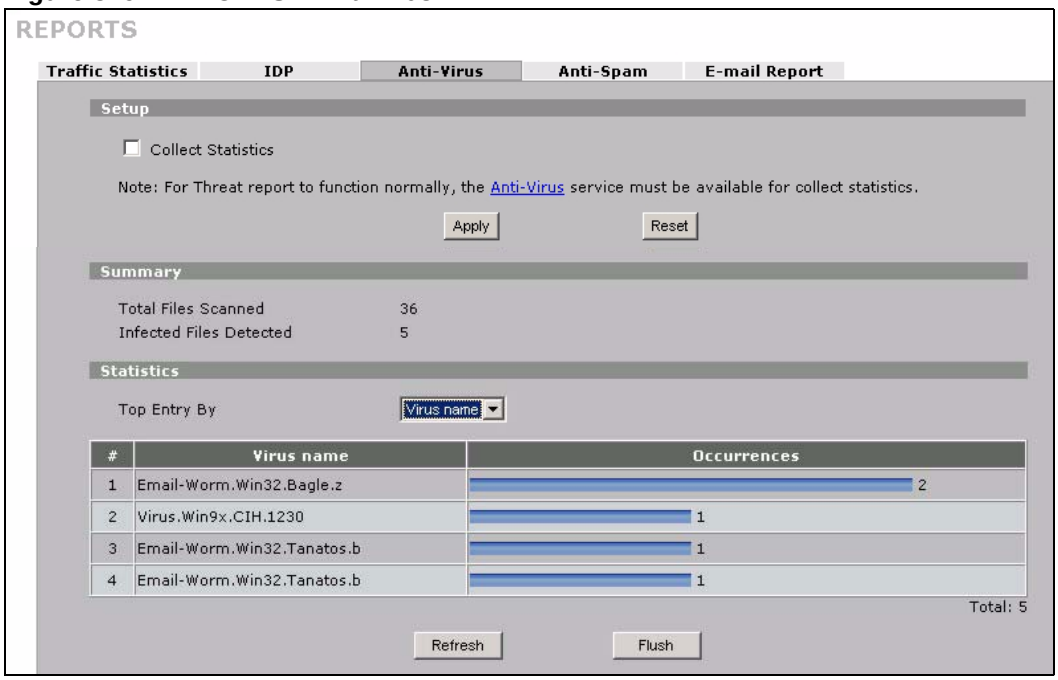
**Figure 328** REPORTS > IDP > Destination




# 31.4 The Anti-Virus Screen

Click **REPORTS** > **Anti-Virus** to display the **Anti-Virus** screen. This screen displays anti-virus statistics.

**Figure 329** REPORTS > Anti-Virus



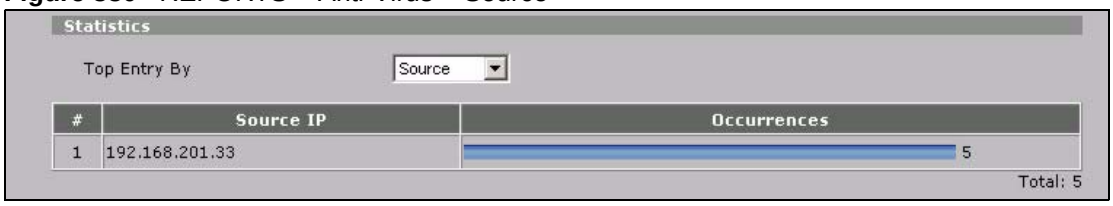
The following table describes the labels in this screen.

**Table 167** REPORTS > Anti-Virus

| LABEL | DESCRIPTION |
|---|---|
| Collect Statistics | Select this check box to have the ZyWALL collect anti-virus 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 the **Flush** button. Collecting starts over and a new collection start time displays. |
| Total Files Scanned | This field displays the number of files that the ZyWALL has scanned for viruses. |
| 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>Select **Virus Name** to list the most common viruses that the ZyWALL has detected.<br>Select **Source** to list the source IP addresses from which the ZyWALL has detected the most virus-infected files.<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. |
| 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. |
| Refresh | Click **Refresh** to update the report display with additional information that the ZyWALL may have collected while you had the screen open. The report also refreshes automatically when you close and reopen the screen. |
| Flush | Click **Flush** to discard the report data and restart collecting statistics. |

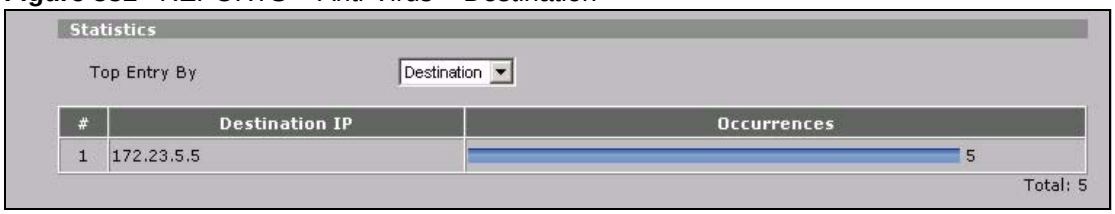
The statistics display as follows when you display the top entries by source.

**Figure 330** REPORTS > Anti-Virus > Source




The statistics display as follows when you display the top entries by destination.

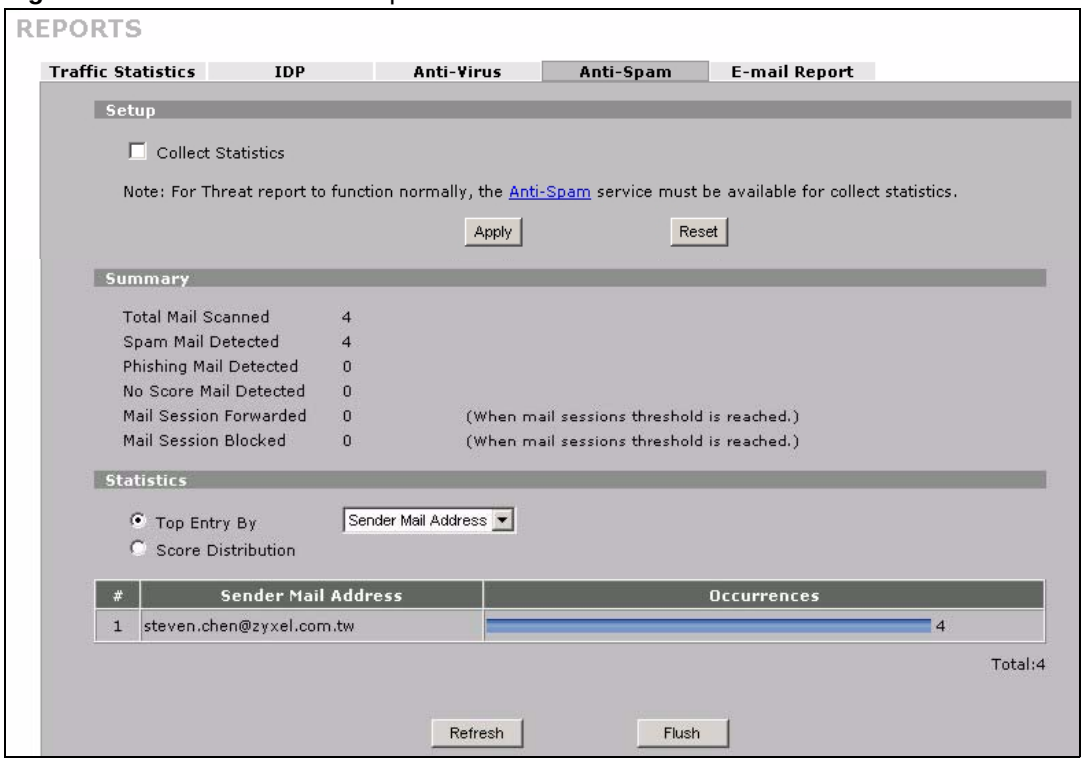
**Figure 331** REPORTS > Anti-Virus > Destination




## 31.5 The Anti-Spam Screen

Click **REPORTS** > **Anti-Spam** to display the **Anti-Spam** screen. This screen displays anti-spam statistics.

**Figure 332** REPORTS > Anti-Spam




The following table describes the labels in this screen.

**Table 168** REPORTS > Anti-Spam

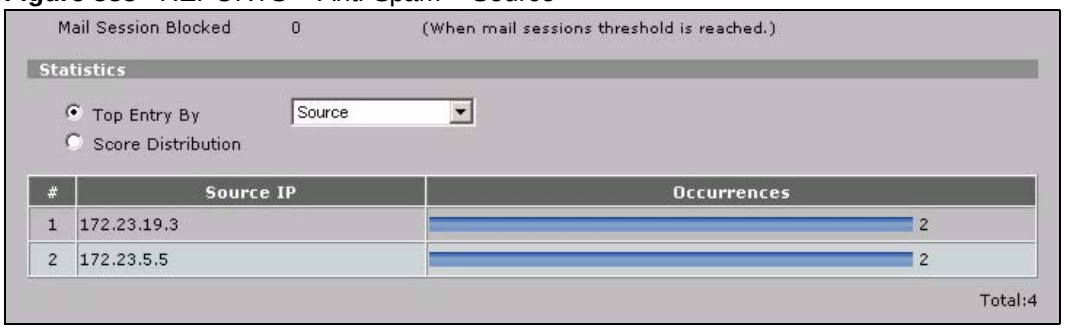
| LABEL | DESCRIPTION |
|---|---|
| Collect Statistics | Select this check box to have the ZyWALL collect anti-spam statistics.<br>The collection starting time displays after you click **Apply**. All of the statistics in this screen are for the time period starting at the time displayed here. The format is year, month, day and hour, minute, second. Collecting starts over (and a new collection start time displays) if you restart the ZyWALL or click the **Flush** button. |
| Total Mail Scanned | This field displays the number of e-mails that the ZyWALL has checked. |
| Spam Mail Detected | This field displays the number of e-mails that the ZyWALL has classified as spam. |

**Table 168** REPORTS > Anti-Spam (continued)

| LABEL | DESCRIPTION |
|---|---|
| Phishing Mail Detected | This field displays the number of e-mails that the ZyWALL has classified as phishing. |
| No Score Mail Detected | This field displays the number of e-mails for which the ZyWALL did not receive a spam score. |
| Mail Session Forwarded | You can set the action that the ZyWALL takes when an e-mail session goes over the threshold of concurrent sessions that the ZyWALL checks for spam.<br>This field displays the number of e-mail sessions that the ZyWALL allowed because they exceeded the mail sessions threshold. |
| Mail Session Blocked | You can set the action that the ZyWALL takes when an e-mail session goes over the threshold of concurrent sessions that the ZyWALL checks for spam.<br>This field displays the number of e-mail sessions that the ZyWALL stopped because they exceeded the mail sessions threshold. |
| Top Entry By | Select **Top Entry by** to list the top e-mail or IP addresses from which the ZyWALL has detected the most spam.<br>Select **Sender Mail Address** to list the top e-mail addresses from which the ZyWALL has detected the most spam.<br>Select **Source** to list the source IP addresses from which the ZyWALL has detected the most spam. |
| Score Distribution | Select **Score Distribution** to display the numbers of different spam scores of the e-mails that the ZyWALL has checked. |
| # | This field displays the entry's rank in the list of the top entries. |
| 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. |
| Source IP | This column displays when you display the entries by **Source.** It shows the source IP address of spam e-mails that the ZyWALL has detected. |
| Occurrences | This column displays when you display the entries by **Sender Mail Address** or **Source**. This field displays how many times the ZyWALL received spam from the entry's e-mail address. |
| Total | This field displays when you select **Sender Mail Address** or **Source**.<br>This field displays the sum of the occurrences of the events in the entries. |
| Spam Threshold | This field displays when you select **Score Distribution**.<br>This is the spam score for classifying e-mail as spam. Any e-mail with a spam score higher than this number is classified as spam. |
| Mail Count<br>Threshold<br>Score | When you select **Score Distribution**, this table displays the distribution of e-mail spam scores.<br>Each bar represents the number of e-mails that had a spam score close to the threshold score listed at the bottom. The numbers on the left are numbers of e-mails. |
| Refresh | Click **Refresh** to update the report display with additional information that the ZyWALL may have collected while you had the screen open. The report also refreshes automatically when you close and reopen the screen. |
| Flush | Click **Flush** to discard the report data and restart collecting statistics. |

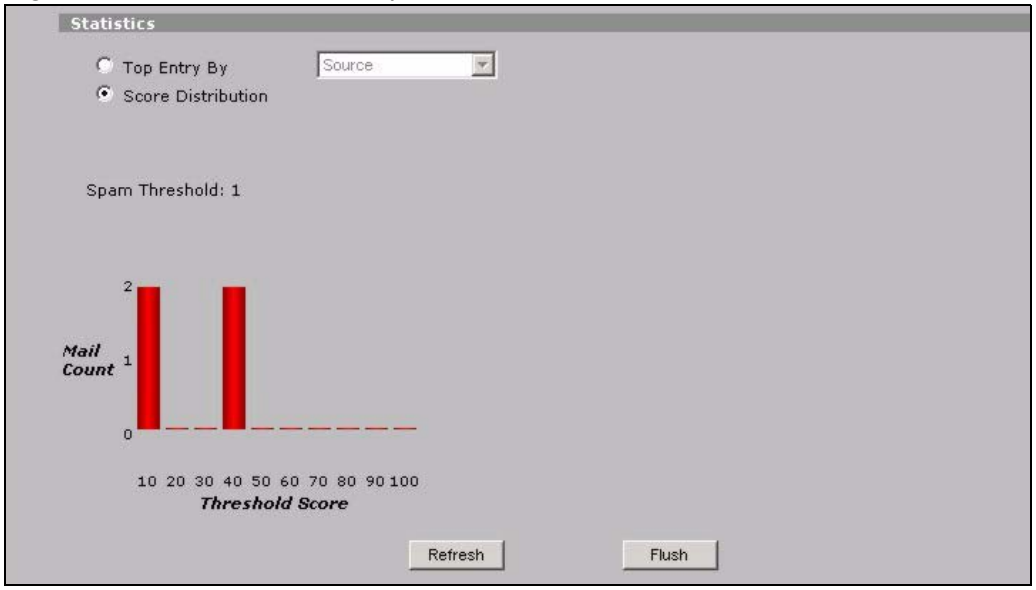
The statistics display as follows when you display the top entries by source.

**Figure 333** REPORTS > Anti-Spam > Source




The statistics display as follows when you display the score distribution.

**Figure 334** REPORTS > Anti-Spam > Score Distribution

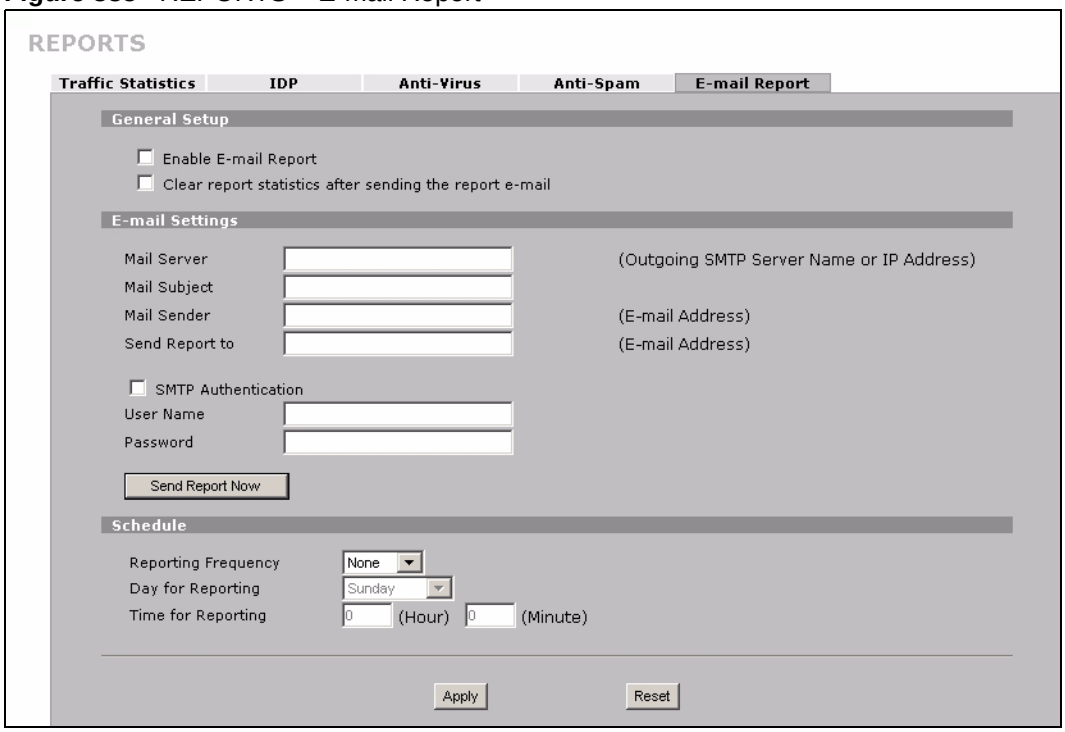



## 31.6 The E-mail Report Screen

You can configure the ZyWALL to email a report including the information on network traffic, IDP, anti-virus and anti-spam statistics provided in the report screens.

Click **REPORTS > E-mail Report** to display the following screen.

**Figure 335** REPORTS > E-mail Report




The following table describes the labels in this screen.

**Table 169** REPORTS > E-mail Report

| LABEL | DESCRIPTION |
|---|---|
| General Setup | |
| Enable E-mail Report | Select this to turn on the e-mail report feature. You must then specify a valid e-mail server in order to send reports. |
| Clear report statistics after sending the report e-mail | Select this to clear current records of IDP, anti-virus and anti-spam statistics (available in the **Reports** screens) once the report has been sent. |
| E-mail Settings | |
| Mail Server | Enter the server name or the IP address of the mail server for the e-mail address specified in the **Mail Sender** field. If this field is left blank, report files will not be sent via e-mail. |
| Mail Subject | Type a descriptive subject here to be included in the report e-mail subject header. |
| Mail Sender | Enter the e-mail address that you want to be in the from/sender line of the diagnostic e-mail message that the ZyWALL sends. If you activate SMTP authentication, the e-mail address must be able to be authenticated by the mail server as well. |
| Send Report to | Report files are sent to the e-mail address specified in this field. If this field is left blank, report files will not be sent via e-mail. |
| SMTP Authentication | SMTP (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. Select the check box to activate SMTP authentication. If mail server authentication is needed but this feature is disabled, you will not receive the report files. |
| User Name | Enter the user name (up to 63 characters) (usually the user name of a mail account you specified in the **Mail Sender** field). |
| Password | Enter the password associated with the user name above. |

**Table 169** REPORTS > E-mail Report (continued)

| LABEL | DESCRIPTION |
|---|---|
| Send Report Now | Click this to send the report e-mail immediately. |
| Schedule | |
| Reporting Frequency | Select the frequency of the report e-mail from the drop-down box. Options are **None**, **Hourly**, **Daily** and **Weekly**.<br>If you select **Daily** or **Weekly**, specify a time of day for the ZyWALL to generate and send diagnostic e-mails. If you select **Weekly**, then also specify which day of the week. Select **None** to have the ZyWALL not generate and send diagnostic e-mails based on a time period. |
| Day for Reporting | If **Weekly** is selected in the **Schedule** field, select the day for reporting from the drop-down box. |
| Time for Reporting | If **Daily** or **Weekly** is selected in the **Schedule** field, type the hour and minute in 24-hour format (for example, 23:00 equals 11:00 pm) to send the report email in these two boxes. |
| Apply | Click **Apply** to save your changes. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# 32

# Logs Screens

## 32.1 Overview

In the log screens you can configure general log settings and view the ZyWALL's logs. The logs cover categories such as system maintenance, system errors, access control, allowed or blocked web sites, blocked web features (such as ActiveX controls, java and cookies), attacks (such as DoS) and IPSec.

### 32.1.1 What You Can Do in the Log Screens

- Use the **View Log** screen (Section 32.2 on page 555) to see the logs for the categories that you selected in the **Log Settings** screen.
- Use the **Log Settings** screen (Section 32.3 on page 558) to configure to where the ZyWALL is to send logs; the schedule for when the ZyWALL is to send the logs and which logs and/or immediate alerts the ZyWALL is to send.

### 32.1.2 What You Need To Know About Logs

#### Alerts and Logs

An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites or web sites with restricted web features such as cookies, active X and so on. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts display in red and logs display in black.

#### Finding Out More

Refer to Section 32.4 on page 561 for log message explanations.

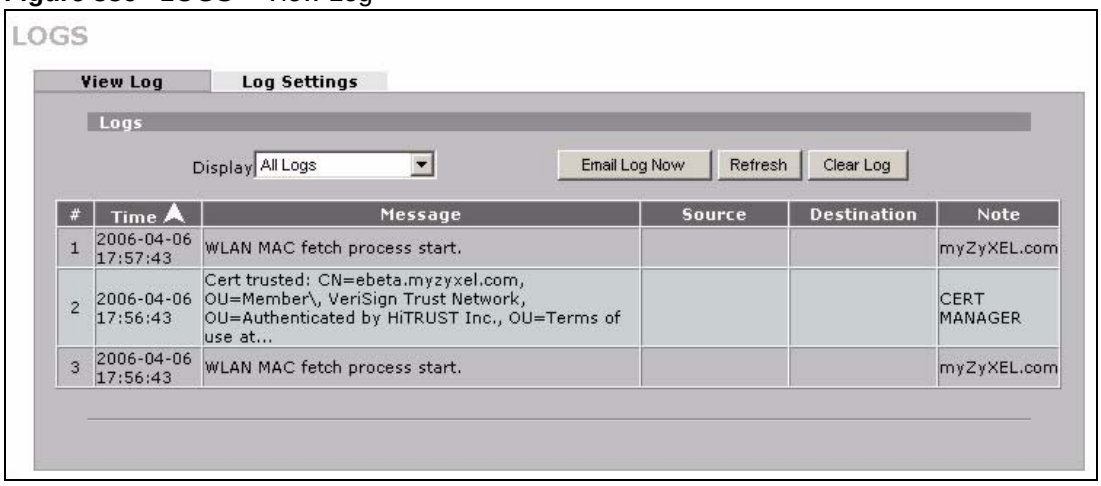
## 32.2 The View Log Screen

The web configurator allows you to look at all of the ZyWALL's logs in one location.

Click **LOGS** to open the **View Log** screen. Use the **View Log** screen to see the logs for the categories that you selected in the **Log Settings** screen (see Section 32.3 on page 558).

When the log is full it will begin to delete older entries as it adds new ones. You can configure the ZyWALL to email you the log when it is full in the **Log Settings** screen. Click a column heading to sort the entries by the relevant attribute. A triangle indicates ascending or descending sort order.

**Figure 336** LOGS > View Log




The following table describes the labels in this screen.

**Table 170** LOGS > View Log

| LABEL | DESCRIPTION |
|---|---|
| Display | The categories that you select in the **Log Settings** page (see Section 32.3 on page 558) display in the drop-down list box.<br>Select a category of logs to view; select **All Logs** to view logs from all of the log categories that you selected in the **Log Settings** page. |
| Email Log Now | Click **Email Log Now** to send the log screen to the e-mail address specified in the **Log Settings** page (make sure that you have first filled in the **E-mail Log Settings** fields in **Log Settings**, see Section 32.3 on page 558). |
| Refresh | Click **Refresh** to renew the log screen. |
| Clear Log | Click **Clear Log** to delete all the logs. |
| | The logs display in the table. Click a column's heading to sort the log entries by that criteria. |
| # | This field displays the log number. |
| Time | This field displays the time the log was recorded. See Section 33.4 on page 587 to configure the ZyWALL's time and date. |
| Message | This field states the reason for the log. |
| Source | This field lists the source IP address and the port number of the incoming packet. |
| Destination | This field lists the destination IP address and the port number of the incoming packet. |
| Note | This field displays additional information about the log entry. |

## 32.2.1 Log Description Example

The following is an example of how a log displays in the command line interpreter and a description of the sample log. Refer to Section  on page 561 for more log message descriptions and the CLI Reference Guide for details on using the command line interpreter to display logs.

```
#  .time                source                destination
notes
    message
```

```
  5|06/08/2004 05:58:20 |172.21.4.187:137      |172.21.255.255:137
|ACCESS BLOCK
    Firewall default policy: UDP (W to W/ZW)
```

**Table 171** Log Description Example

| LABEL | DESCRIPTION |
|---|---|
| # | This is log number five. |
| time | The log was generated on June 8, 2004 at 5:58 and 20 seconds AM. |
| source | The log was generated due to a NetBIOS packet sent from IP address 172.21.4.187 port 137. |
| destination | The NetBIOS packet was sent to the 172.21.255.255 subnet port 137. This was a NetBIOS UDP broadcast packet meant to discover devices on the network. |
| notes | The ZyWALL blocked the packet. |
| message | The ZyWALL blocked the packet in accordance with the firewall's default policy of blocking sessions that are initiated from the WAN. "UDP" means that this was a User Datagram Protocol packet. "W to W/ZW" indicates that the packet was traveling from the WAN to the WAN or the ZyWALL. |

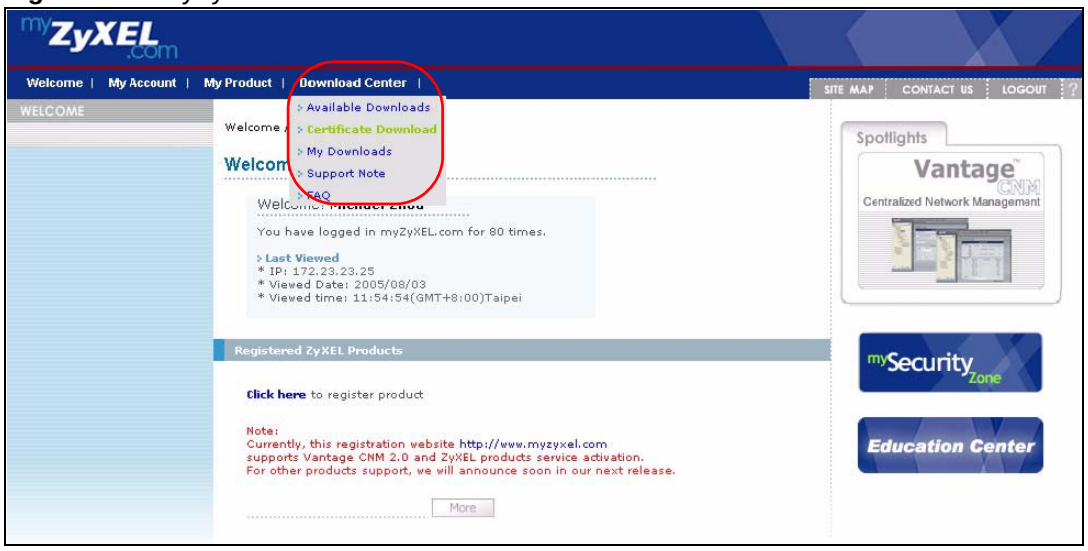
## 32.2.2 About the Certificate Not Trusted Log

myZyXEL.com and the update server use certificates signed by VeriSign to identify themselves. If the ZyWALL does not have a CA certificate signed by VeriSign as a trusted CA, the ZyWALL will not trust the certificate from myZyXEL.com and the update server. The ZyWALL will generate a log like "Due to error code(11), cert not trusted: SSL/TLS peer certif..." for every time it attempt to establish a (HTTPS) connection with myZyXEL.com and the update server. The V4.00 default configuration file includes a trusted CA certificate signed by VeriSign. If you upgraded to ZyNOS V4.00 firmware without uploading the V4.00 default configuration file, you can download a CA certificate signed by VeriSign from myZyXEL.com and import it into the ZyWALL as a trusted CA. This will stop the ZyWALL from generating this log every time it attempts to connect with myzyxel.com and the update server.

Follow the steps below to download the certificate from myZyXEL.com.

1. Go to http://www.myZyXEL.com and log in with your account.
2. Click **Download Center** and then **Certificate Download**.

**Figure 337** myZyXEL.com: Download Center




**3** Click the link in the **Certificate Download** screen.

**Figure 338** myZyXEL.com: Certificate Download

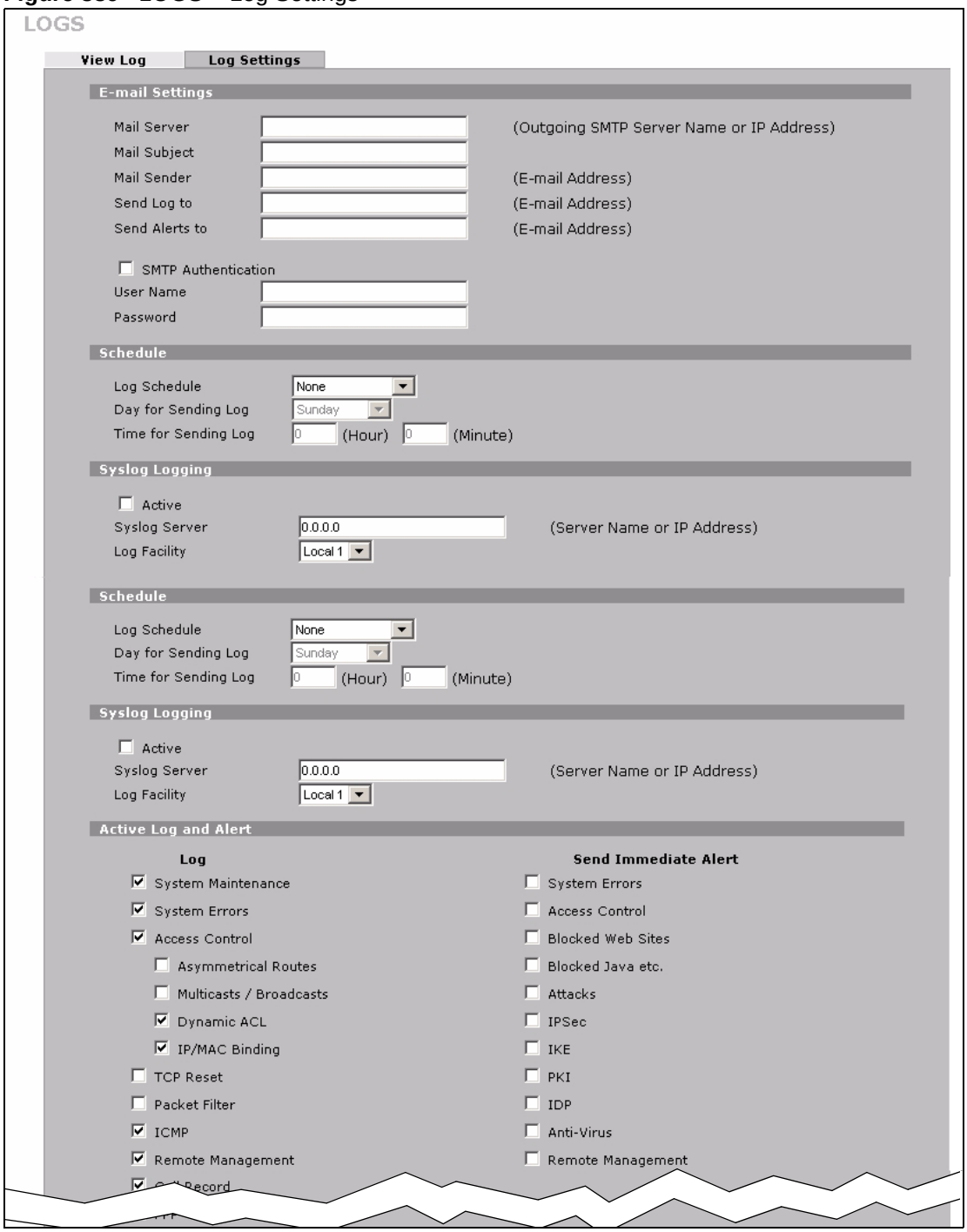

## 32.3 The Log Settings Screen

To change your ZyWALL's log settings, click **LOGS** > **Log Settings**. The screen appears as shown.

Use the **Log Settings** screen to configure to where the ZyWALL is to send logs; the schedule for when the ZyWALL is to send the logs and which logs and/or immediate alerts the ZyWALL is to send.

Alerts are e-mailed as soon as they happen. Logs may be e-mailed as soon as the log is full (see **Log Schedule**). Selecting many alert and/or log categories (especially **Access Control**) may result in many e-mails being sent.

**Figure 339** LOGS > Log Settings




The following table describes the labels in this screen.

**Table 172** LOGS > Log Settings

| LABEL | DESCRIPTION |
|---|---|
| E-mail Settings | |
| Mail Server | Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages will not be sent via e-mail. |

**Table 172** LOGS > Log Settings (continued)

| LABEL | DESCRIPTION |
|---|---|
| Mail Subject | Type a title that you want to be in the subject line of the log e-mail message that the ZyWALL sends. |
| Mail Sender | Enter the e-mail address that you want to be in the from/sender line of the log e-mail message that the ZyWALL sends. If you activate SMTP authentication, the e-mail address must be able to be authenticated by the mail server as well. |
| Send Log To | Logs are sent to the e-mail address specified in this field. If this field is left blank, logs will not be sent via e-mail. |
| Send Alerts To | Alerts are sent to the e-mail address specified in this field. If this field is left blank, alerts will not be sent via e-mail. |
| SMTP Authentication | SMTP (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.<br>Select the check box to activate SMTP authentication. If mail server authentication is needed but this feature is disabled, you will not receive the e-mail logs. |
| User Name | Enter the user name (up to 63 characters) (usually the user name of a mail account). |
| Password | Enter the password associated with the user name above. |
| Schedule | |
| Log Schedule | This drop-down menu is used to configure the frequency of log messages being sent as E-mail:<br>**When Log is Full**<br>**Hourly**<br>**Weekly**<br>**Daily**<br>**None**<br>If you select **Weekly** or **Daily**, specify a time of day when the E-mail should be sent. If you select **Weekly**, then also specify which day of the week the E-mail should be sent. If you select **When Log is Full**, an alert is sent when the log fills up. If you select **None**, no log messages are sent. |
| Day for Sending Log | Use the drop down list box to select which day of the week to send the logs. |
| Time for Sending Log | Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs. |
| Syslog Logging | Syslog allows you to send system logs to a server.<br>Syslog logging sends a log to an external syslog server. |
| Active | Click **Active** to enable syslog logging. |
| Syslog Server | Enter the server name or IP address of the syslog server that will log the selected categories of logs. |
| Log Facility | Select a location from the drop down list box. The log facility allows you to log the messages to different files in the syslog server. Refer to the documentation of your syslog program for more details. |
| Active Log and Alert | |
| Log | Select the categories of logs that you want to record. Logs include alerts. |
| Send Immediate Alert | Select the categories of alerts for which you want the ZyWALL to instantly e-mail alerts to the e-mail address specified in the **Send Alerts To** field. |
| Log Consolidation | |

**Table 172** LOGS > Log Settings (continued)

| LABEL | DESCRIPTION |
|---|---|
| Active | Some logs (such as the Attacks logs) may be so numerous that it becomes easy to ignore other important log messages. Select this check box to merge logs with identical messages into one log.<br>See the CLI Reference Guide for how to see what log messages will be consolidated. |
| Log Consolidation Period | Specify the time interval during which the ZyWALL merges logs with identical messages into one log. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 32.4 Technical Reference

# Log Descriptions

This section provides descriptions of example log messages.

The variables “%d”, “%x” and “%s” respectively refer to decimal numbers, hexadecimal numbers and strings (a list of upper/lower case letters or numbers).

**Table 173** System Maintenance Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| `Time set from NTP server: <server address>, offset: <time offset> sec` | The router has adjusted its time based on information from the time server. |
| `Failed to sync with <time server type> server: <time server address>` | The router failed to get information from the time server. |
| `WAN interface gets IP: %s` | A WAN interface got a new IP address from the DHCP, PPPoE, PPTP or dial-up server. |
| `DHCP client IP expired` | A DHCP client's IP address has expired. |
| `DHCP server assigns %s` | The DHCP server assigned an IP address to a client. |
| `Successful SMT login` | Someone has logged on to the router's SMT interface. |
| `SMT login failed` | Someone has failed to log on to the router's SMT interface. |
| `Successful WEB login` | Someone has logged on to the router's web configurator interface. |
| `WEB login failed` | Someone has failed to log on to the router's web configurator interface. |
| `Successful TELNET login` | Someone has logged on to the router via telnet. |
| `TELNET login failed` | Someone has failed to log on to the router via telnet. |
| `Successful FTP login` | Someone has logged on to the router via FTP. |
| `FTP login failed` | Someone has failed to log on to the router via FTP. |
| `NAT Session Table is Full!` | The maximum number of NAT session table entries has been exceeded and the table is full. |

**Table 173** System Maintenance Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Starting Connectivity Monitor | Starting Connectivity Monitor. |
| Time initialized by Daytime Server | The router got the time and date from the Daytime server. |
| Time initialized by Time server | The router got the time and date from the time server. |
| Time initialized by NTP server | The router got the time and date from the NTP server. |
| Connect to Daytime server fail | The router was not able to connect to the Daytime server. |
| Connect to Time server fail | The router was not able to connect to the Time server. |
| Connect to NTP server fail | The router was not able to connect to the NTP server. |
| Too large ICMP packet has been dropped | The router dropped an ICMP packet that was too large. |
| SMT Session Begin | An SMT management session has started. |
| SMT Session End | An SMT management session has ended. |
| Configuration Change: PC = 0x%x, Task ID = 0x%x | The router is saving configuration changes. |
| Successful SSH login | Someone has logged on to the router's SSH server. |
| SSH login failed | Someone has failed to log on to the router's SSH server. |
| Successful HTTPS login | Someone has logged on to the router's web configurator interface using HTTPS protocol. |
| HTTPS login failed | Someone has failed to log on to the router's web configurator interface using HTTPS protocol. |
| DNS server %s was not responding to last 32 consecutive queries… | The specified DNS server did not respond to the last 32 consecutive queries. |
| DDNS update IP:%s (host %d) successfully | The device updated the IP address of the specified DDNS host name. |
| SMTP successfully | The device sent an e-mail. |
| myZyXEL.com registration successful | Registration of the device with myZyXEL.com was successful. |
| Trial service registration successful | Registration for a trial service was successful. |
| Service upgrade successful | Registration for a service upgrade was successful. |
| Service refresh successful. | The device successfully refreshed service information from myZyXEL.com. |
| Content Filter trial service activation successfully | The content filtering trial service was successfully activated for this device. |
| Anti-Spam trial service activation successfully | The anti-spam trial service was successfully activated for this device. |
| IDP/Anti-Virus trial service activation successfully | The IDP and anti-virus trial service was successfully activated for this device. |

**Table 173** System Maintenance Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| %s | The myZyXEL.com service registration failed due to the error listed. If you are unable to register for services at myZYXEL.com, the error message displayed in this log may be useful when contacting customer support. |
| Remote node is connecting. | A remote user is connecting using PPP. Other PPP connection requests must wait until this process is complete. |
| Remote node is dropping | A remote user is releasing a PPP connection. Other PPP connection requests must wait until this process is complete. |

**Table 174** System Error Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| %s exceeds the max. number of session per host! | This attempt to create a NAT session exceeds the maximum number of NAT session table entries allowed to be created per host. |
| setNetBIOSFilter: calloc error | The router failed to allocate memory for the NetBIOS filter settings. |
| readNetBIOSFilter: calloc error | The router failed to allocate memory for the NetBIOS filter settings. |
| WAN%d connection is up | The specified WAN connection is up. |
| WAN connection is down. | A WAN connection is down. You cannot access the network through this interface. |
| Dial Backup starts | Dial backup started working. |
| Dial Backup ends | Dial backup stopped working. |
| DHCP Server cannot assign the static IP %S (out of range). | The LAN subnet, LAN alias 1, or LAN alias 2 was changed and the specified static DHCP IP addresses are no longer valid. |
| The DHCP static IP %s is conflict. | The static DHCP IP address conflicts with another host. |
| SMTP fail (%s) | The device failed to send an e-mail (error message included). |
| SMTP authentication fail (%s) | The device failed to authenticate with the SMTP server (error message included). |
| %s | The device will send a Gratuitous ARP to detect the IP collision. If the collision happens, there will be a log in centralized log |

**Table 175** Access Control Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Firewall default policy: [ TCP \| UDP \| IGMP \| ESP \| GRE \| OSPF ] <Packet Direction> | Attempted TCP/UDP/IGMP/ESP/GRE/OSPF access matched the default policy and was blocked or forwarded according to the default policy's setting. |
| Firewall rule [NOT] match:[ TCP \| UDP \| IGMP \| ESP \| GRE \| OSPF ] <Packet Direction>, <rule:%d> | Attempted TCP/UDP/IGMP/ESP/GRE/OSPF access matched (or did not match) a configured firewall rule (denoted by its number) and was blocked or forwarded according to the rule. |

**Table 175** Access Control Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Triangle route packet forwarded: [ TCP \| UDP \| IGMP \| ESP \| GRE \| OSPF ] | The firewall allowed a triangle route session to pass through. |
| Packet without a NAT table entry blocked: [ TCP \| UDP \| IGMP \| ESP \| GRE \| OSPF ] | The router blocked a packet that didn't have a corresponding NAT table entry. |
| Router sent blocked web site message: TCP | The router sent a message to notify a user that the router blocked access to a web site that the user requested. |
| Exceed maximum sessions per host (%d). | The device blocked a session because the host's connections exceeded the maximum sessions per host. |
| Firewall allowed a packet that matched a NAT session: [ TCP \| UDP ] | A packet from the WAN (TCP or UDP) matched a cone NAT session and the device forwarded it to the LAN. |
| Firewall matches a dynamic ACL rule of an ALG session | A packet matches a dynamic ACL rule created in an ALG session. |
| Maximum number of dynamic ACL rules exceeded. | The number of dynamic ACL rules exceeds the maximum allowed. |
| Dynamic ACL rule, listening port : %d, peer port : %d already exists. | The dynamic ACL rule already exists. |
| <srcMAC> was bind to [legalIP] but he uses [srcIP]. | The device's IP address is different from the IP address assigned to this device.<br>This log also records if the IP address assigned to this device is used by another device. |
| DHCP Server dynamic assigned [legalIP] to [srcMac] but he uses [srcIP]. | The dynamically assigned IP address differs from the IP address used by the device. |
| [srcMac] uses an untrusty IP address [srcIP]. | This device is using an IP address that does not fall within the specified range of trusted IP addresses. |

**Table 176** TCP Reset Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Under SYN flood attack, sent TCP RST | The router sent a TCP reset packet when a host was under a SYN flood attack (the TCP incomplete count is per destination host.) |
| Exceed TCP MAX incomplete, sent TCP RST | The router sent a TCP reset packet when the number of TCP incomplete connections exceeded the user configured threshold. (the TCP incomplete count is per destination host.) Note: Refer to **TCP Maximum Incomplete** in the **Firewall Attack Alerts** screen. |
| Peer TCP state out of order, sent TCP RST | The router sent a TCP reset packet when a TCP connection state was out of order.Note: The firewall refers to RFC793 Figure 6 to check the TCP state. |

**Table 176** TCP Reset Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| `Firewall session time out, sent TCP RST` | The router sent a TCP reset packet when a dynamic firewall session timed out.<br>The default timeout values are as follows:<br>ICMP idle timeout: 3 minutes<br>UDP idle timeout: 3 minutes<br>TCP connection (three way handshaking) timeout: 270 seconds<br>TCP FIN-wait timeout: 2 MSL (Maximum Segment Lifetime set in the TCP header).<br>TCP idle (established) timeout (s): 150 minutes<br>TCP reset timeout: 10 seconds |
| `Exceed MAX incomplete, sent TCP RST` | The router sent a TCP reset packet when the number of incomplete connections (TCP and UDP) exceeded the user-configured threshold. (Incomplete count is for all TCP and UDP connections through the firewall.)Note: When the number of incomplete connections (TCP + UDP) > “Maximum Incomplete High”, the router sends TCP RST packets for TCP connections and destroys TOS (firewall dynamic sessions) until incomplete connections < “Maximum Incomplete Low”. |
| `Access block, sent TCP RST` | The router sends a TCP RST packet and generates this log if you turn on the firewall TCP reset mechanism (via CI command: "`sys firewall tcprst`"). |

**Table 177** Packet Filter Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| `[ TCP \| UDP \| ICMP \| IGMP \| Generic ] packet filter matched (set: %d, rule: %d)` | Attempted access matched a configured filter rule (denoted by its set and rule number) and was blocked or forwarded according to the rule. |

For type and code details, see Table 192 on page 578.

**Table 178** ICMP Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| `Firewall default policy: ICMP <Packet Direction>, <type:%d>, <code:%d>` | ICMP access matched the default policy and was blocked or forwarded according to the user's setting. |
| `Firewall rule [NOT] match: ICMP <Packet Direction>, <rule:%d>, <type:%d>, <code:%d>` | ICMP access matched (or didn’t match) a firewall rule (denoted by its number) and was blocked or forwarded according to the rule. |
| `Triangle route packet forwarded: ICMP` | The firewall allowed a triangle route session to pass through. |
| `Packet without a NAT table entry blocked: ICMP` | The router blocked a packet that didn’t have a corresponding NAT table entry. |
| `Unsupported/out-of-order ICMP: ICMP` | The firewall does not support this kind of ICMP packets or the ICMP packets are out of order. |
| `Router reply ICMP packet: ICMP` | The router sent an ICMP reply packet to the sender. |

**Table 179** CDR Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| board %d line %d channel %d, call %d, %s C01 Outgoing Call dev=%x ch=%x %s | The router received the setup requirements for a call. “call” is the reference (count) number of the call. “dev” is the device type (3 is for dial-up, 6 is for PPPoE, 10 is for PPTP). "channel" or “ch” is the call channel ID. For example, "board 0 line 0 channel 0, call 3, C01 Outgoing Call dev=6 ch=0 "Means the router has dialed to the PPPoE server 3 times. |
| board %d line %d channel %d, call %d, %s C02 OutCall Connected %d %s | The PPPoE, PPTP or dial-up call is connected. |
| board %d line %d channel %d, call %d, %s C02 Call Terminated | The PPPoE, PPTP or dial-up call was disconnected. |

**Table 180** PPP Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| ppp:LCP Starting | The PPP connection’s Link Control Protocol stage has started. |
| ppp:LCP Opening | The PPP connection’s Link Control Protocol stage is opening. |
| ppp:CHAP Opening | The PPP connection’s Challenge Handshake Authentication Protocol stage is opening. |
| ppp:IPCP Starting | The PPP connection’s Internet Protocol Control Protocol stage is starting. |
| ppp:IPCP Opening | The PPP connection’s Internet Protocol Control Protocol stage is opening. |
| ppp:LCP Closing | The PPP connection’s Link Control Protocol stage is closing. |
| ppp:IPCP Closing | The PPP connection’s Internet Protocol Control Protocol stage is closing. |

**Table 181** 3G Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| SIM/3G card mismatch: %s. | The IMSI or ESN of the currently inserted card is different from the previous one configured for budget control. |
| Preconfigured SIM card/3G card mismatches with inserted card. Might need to reconfigure budget control settings. | The inserted 3G card is different from the previous one configured for budget control. You may need to reconfigure budget control settings specific to the current user account. |
| Budget counters are reset, budget control is resumed. | The ZyWALL restarted budget calculation from 0 after resetting the existing statistics. |
| Budget control is resumed. | The ZyWALL kept the existing budget control statistics and continue a counting. |
| Budget control is disabled. | Budget control is deactivated for the user account of the installed 3G card on the ZyWALL. |
| Skip 3G SIM authentication because 3G configuration is not set. | The ZyWALL skipped SIM card authentication because the PIN code is not specified or SIM card authentication is disabled. |

**Table 181** 3G Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| 3G SIM authentication failed because of no response from SIM card. | SIM card authentication failed because the ZyWALL received a SIM busy message three times when querying for the card status. |
| 3G card has no response, card is restarted. | The card was reset due to no response from the card for a period of time. |
| 3G SIM card PIN code is incorrect. | The specified PIN code does not match the inserted GSM 3G card. |
| The 3G card is not activated. | The user account of the 3G card is not activated. |
| 3G Modem is locked. | The internal modem on the inserted 3G card is blocked. |
| SIM card not inserted or damaged. | There is no SIM card in the inserted GSM 3G card or the SIM card is damaged. |
| 3G connection has been dropped - %s. | The 3G connection has been dropped due to the specific reason, such as idle timeout, manual disconnection, failure to get an IP address, switching to WAN 1, ping check failure, connection reset, and so on. |
| 3G signal strength is refreshed (%d dBm). | The ZyWALL updated the 3G network signal strength indication. |
| Warning: (%IMSI% or %ESN%) Over time budget! (budget = %CONFIGURED_BUDGET% hours, used = %USED_VOLUME%(2 decimals) hours). | This shows that the pre-configured time budget was exceeded. This also displays the IMSI of the SIM card in an inserted GSM 3G card or the ESN of the inserted CDMA 3G card and the 3G connection's usage time in hours. |
| Warning: (%IMSI% or %ESN%) Over %THRESHOLD%% of time budget (%REMAIN_BUDGET%(2 decimals) hours remain in %CONFIGURED_BUDGET% hours budget). | This shows that the specified percentage of the time budget was exceeded. This also displays the IMSI of the SIM card in an inserted GSM 3G card or the ESN of the inserted CDMA 3G card and the amount of time (in hours) the 3G connection can still be used. |
| Warning: (%ESN% or %IMSI%) Over data budget! (budget =%CONFIGURED_BUDGET%(2 decimals Mbytes, used = %USED_VOLUME%(2 decimals) Mbytes). | This shows that the pre-configured data limit was exceeded. The IMSI of the SIM card in an inserted GSM 3G card or the ESN of the inserted CDMA 3G card is displayed. The amount of data (in Mbytes) sent and/or received (depending on your configuration) through the 3G connection is also displayed. |
| Warning: (%ESN% or %IMSI%) Over %THRESHOLD%% of data budget (%REMAIN_BUDGET%(2 decimals) Mbytes remain in %CONFIGURED_BUDGET% Mbytes budget). | This shows that the specified percentage of data limit was exceeded. This also displays the IMSI of the SIM card in an inserted GSM 3G card or the ESN of the inserted CDMA 3G card and how much data (in Mbytes) can still be transmitted through the 3G connection. |

**Table 182** UPnP Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| UPnP pass through Firewall | UPnP packets can pass through the firewall. |

**Table 183** Content Filtering Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| %s: Keyword blocking | The content of a requested web page matched a user defined keyword. |
| %s: Not in trusted web list | The web site is not in a trusted domain, and the router blocks all traffic except trusted domain sites. |
| %s: Forbidden Web site | The web site is in the forbidden web site list. |
| %s: Contains ActiveX | The web site contains ActiveX. |
| %s: Contains Java applet | The web site contains a Java applet. |
| %s: Contains cookie | The web site contains a cookie. |
| %s: Proxy mode detected | The router detected proxy mode in the packet. |
| %s | The content filter server responded that the web site is in the blocked category list, but it did not return the category type. |
| %s: %s | The content filter server responded that the web site is in the blocked category list, and returned the category type. |
| %s(cache hit) | The system detected that the web site is in the blocked list from the local cache, but does not know the category type. |
| %s :%s(cache hit) | The system detected that the web site is in blocked list from the local cache, and knows the category type. |
| %s: Trusted Web site | The web site is in a trusted domain. |
| %s | When the content filter is not on according to the time schedule or you didn't select the "Block Matched Web Site" check box, the system forwards the web content. |
| Waiting content filter server timeout | The external content filtering server did not respond within the timeout period. |
| DNS resolving failed | The ZyWALL cannot get the IP address of the external content filtering via DNS query. |
| Creating socket failed | The ZyWALL cannot issue a query because TCP/IP socket creation failed, port: port number. |
| Connecting to content filter server fail | The connection to the external content filtering server failed. |
| License key is invalid | The external content filtering license key is invalid. |

For type and code details, see Table 192 on page 578.

**Table 184** Attack Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| attack [ TCP \| UDP \| IGMP \| ESP \| GRE \| OSPF ] | The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF attack. |
| attack ICMP (type:%d, code:%d) | The firewall detected an ICMP attack. |
| land [ TCP \| UDP \| IGMP \| ESP \| GRE \| OSPF ] | The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF land attack. |
| land ICMP (type:%d, code:%d) | The firewall detected an ICMP land attack. |

**Table 184** Attack Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| ip spoofing - WAN [ TCP \| UDP \| IGMP \| ESP \| GRE \| OSPF ] | The firewall detected an IP spoofing attack on the WAN port. |
| ip spoofing - WAN ICMP (type:%d, code:%d) | The firewall detected an ICMP IP spoofing attack on the WAN port. |
| icmp echo : ICMP (type:%d, code:%d) | The firewall detected an ICMP echo attack. |
| syn flood TCP | The firewall detected a TCP syn flood attack. |
| ports scan TCP | The firewall detected a TCP port scan attack. |
| teardrop TCP | The firewall detected a TCP teardrop attack. |
| teardrop UDP | The firewall detected an UDP teardrop attack. |
| teardrop ICMP (type:%d, code:%d) | The firewall detected an ICMP teardrop attack. |
| illegal command TCP | The firewall detected a TCP illegal command attack. |
| NetBIOS TCP | The firewall detected a TCP NetBIOS attack. |
| ip spoofing - no routing entry [ TCP \| UDP \| IGMP \| ESP \| GRE \| OSPF ] | The firewall classified a packet with no source routing entry as an IP spoofing attack. |
| ip spoofing - no routing entry ICMP (type:%d, code:%d) | The firewall classified an ICMP packet with no source routing entry as an IP spoofing attack. |
| vulnerability ICMP (type:%d, code:%d) | The firewall detected an ICMP vulnerability attack. |
| traceroute ICMP (type:%d, code:%d) | The firewall detected an ICMP traceroute attack. |
| ports scan UDP | The firewall detected a UDP port scan attack. |
| Firewall sent TCP packet in response to DoS attack TCP | The firewall sent TCP packet in response to a DoS attack |
| ICMP Source Quench ICMP | The firewall detected an ICMP Source Quench attack. |
| ICMP Time Exceed ICMP | The firewall detected an ICMP Time Exceed attack. |
| ICMP Destination Unreachable ICMP | The firewall detected an ICMP Destination Unreachable attack. |
| ping of death. ICMP | The firewall detected an ICMP ping of death attack. |
| smurf ICMP | The firewall detected an ICMP smurf attack. |
| IP address in FTP port command is different from the client IP address. It maybe a bounce attack. | The IP address in an FTP port command is different from the client IP address. It may be a bounce attack. |
| Fragment packet size is smaller than the MTU size of output interface. | The fragment packet size is smaller than the MTU size of output interface. |

**Table 185** Remote Management Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Remote Management: FTP denied | Attempted use of FTP service was blocked according to remote management settings. |
| Remote Management: TELNET denied | Attempted use of TELNET service was blocked according to remote management settings. |
| Remote Management: HTTP or UPnP denied | Attempted use of HTTP or UPnP service was blocked according to remote management settings. |
| Remote Management: WWW denied | Attempted use of WWW service was blocked according to remote management settings. |
| Remote Management: HTTPS denied | Attempted use of HTTPS service was blocked according to remote management settings. |
| Remote Management: SSH denied | Attempted use of SSH service was blocked according to remote management settings. |
| Remote Management: ICMP Ping response denied | Attempted use of ICMP service was blocked according to remote management settings. |
| Remote Management: SNMP denied | Attempted use of SNMP service was blocked according to remote management settings. |
| Remote Management: DNS denied | Attempted use of DNS service was blocked according to remote management settings. |

**Table 186** Wireless Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| WLAN MAC Filter Fail | The MAC filter blocked a wireless station from connecting to the device. |
| WLAN MAC Filter Success | The MAC filter allowed a wireless station to connect to the device. |
| WLAN STA Association | A wireless station associated with the device. |
| WLAN STA Association List Full | The maximum number of associated wireless clients has been reached. |
| WLAN STA Association Again | The SSID and time of association were updated for an wireless station that was already associated. |
| WLAN STA DisAssociation | Station dis-association ok |
| WDS link is up | The WDS link is up. |
| WDS link is down | The WDS link is down |
| User PMK cache hits. | The user's PMK is in the cache. |
| User Pre-authentication succeeds. | The user's pre-authentication is succeed. |
| Rogue AP Detection | A rogue AP is detected. |
| WPA-PSK user. | WPA-PSK user login. |
| WPA2-PSK user. | WPA2-PSK user login. |
| The wireless card does not work because RADIUS server is not active. | The ZyWALL is not using the installed wireless card because the RADIUS server is not active. |

**Table 187** IPSec Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Discard REPLAY packet | The router received and discarded a packet with an incorrect sequence number. |
| Inbound packet authentication failed | The router received a packet that has been altered. A third party may have altered or tampered with the packet. |
| Receive IPSec packet, but no corresponding tunnel exists | The router dropped an inbound packet for which SPI could not find a corresponding phase 2 SA. |
| Rule <%d> idle time out, disconnect | The router dropped a connection that had outbound traffic and no inbound traffic for a certain time period. You can use the "ipsec timer chk_conn" CI command to set the time period. The default value is 2 minutes. |
| WAN IP changed to <IP> | The router dropped all connections with the “MyIP” configured as “0.0.0.0” when the WAN IP address changed. |
| Inbound packet decryption failed | Please check the algorithm configuration. |
| Cannot find outbound SA for rule <%d> | A packet matches a rule, but there is no phase 2 SA for outbound traffic. |
| Rule [%s] sends an echo request to peer | The device sent a ping packet to check the specified VPN tunnel's connectivity. |
| Rule [%s] receives an echo reply from peer | The device received a ping response when checking the specified VPN tunnel's connectivity. |
| Delete all tunnels | All IPSec tunnels are disconnected. See the CLI Reference Guide for information on how to do this. |

**Table 188** IKE Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Active connection allowed exceeded | The IKE process for a new connection failed because the limit of simultaneous phase 2 SAs has been reached. |
| Start Phase 2: Quick Mode | Phase 2 Quick Mode has started. |
| Verifying Remote ID failed: | The connection failed during IKE phase 2 because the router and the peer’s Local/Remote Addresses don’t match. |
| Verifying Local ID failed: | The connection failed during IKE phase 2 because the router and the peer’s Local/Remote Addresses don’t match. |
| IKE Packet Retransmit | The router retransmitted the last packet sent because there was no response from the peer. |
| Failed to send IKE Packet | An Ethernet error stopped the router from sending IKE packets. |
| Too many errors! Deleting SA | An SA was deleted because there were too many errors. |
| Phase 1 IKE SA process done | The phase 1 IKE SA process has been completed. |
| Duplicate requests with the same cookie | The router received multiple requests from the same peer while still processing the first IKE packet from the peer. |
| IKE Negotiation is in process | The router has already started negotiating with the peer for the connection, but the IKE process has not finished yet. |

**Table 188** IKE Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| No proposal chosen | Phase 1 or phase 2 parameters don't match. Please check all protocols / settings. Ex. One device being configured for 3DES and the other being configured for DES causes the connection to fail. |
| Local / remote IPs of incoming request conflict with rule <%d> | The security gateway is set to "0.0.0.0" and the router used the peer's "Local Address" as the router's "Remote Address". This information conflicted with static rule #d; thus the connection is not allowed. |
| Cannot resolve Secure Gateway Addr for rule <%d> | The router couldn't resolve the IP address from the domain name that was used for the secure gateway address. |
| Peer ID: <peer id> <My remote type> -<My local type> | The displayed ID information did not match between the two ends of the connection. |
| vs. My Remote <My remote> - <My remote> | The displayed ID information did not match between the two ends of the connection. |
| vs. My Local <My local>-<My local> | The displayed ID information did not match between the two ends of the connection. |
| Send <packet> | A packet was sent. |
| Recv <packet> | IKE uses ISAKMP to transmit data. Each ISAKMP packet contains many different types of payloads. All of them show in the LOG. Refer to RFC2408 – ISAKMP for a list of all ISAKMP payload types. |
| Recv <Main or Aggressive> Mode request from <IP> | The router received an IKE negotiation request from the peer address specified. |
| Send <Main or Aggressive> Mode request to <IP> | The router started negotiation with the peer. |
| Invalid IP <Peer local> / <Peer local> | The peer's "Local IP Address" is invalid. |
| Remote IP <Remote IP> / <Remote IP> conflicts | The security gateway is set to "0.0.0.0" and the router used the peer's "Local Address" as the router's "Remote Address". This information conflicted with static rule #d; thus the connection is not allowed. |
| Phase 1 ID type mismatch | This router's "Peer ID Type" is different from the peer IPSec router's "Local ID Type". |
| Phase 1 ID content mismatch | This router's "Peer ID Content" is different from the peer IPSec router's "Local ID Content". |
| No known phase 1 ID type found | The router could not find a known phase 1 ID in the connection attempt. |
| ID type mismatch. Local / Peer: <Local ID type/Peer ID type> | The phase 1 ID types do not match. |
| ID content mismatch | The phase 1 ID contents do not match. |
| Configured Peer ID Content: <Configured Peer ID Content> | The phase 1 ID contents do not match and the configured "Peer ID Content" is displayed. |
| Incoming ID Content: <Incoming Peer ID Content> | The phase 1 ID contents do not match and the incoming packet's ID content is displayed. |
| Unsupported local ID Type: <%d> | The phase 1 ID type is not supported by the router. |

**Table 188** IKE Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| ERROR !!! build_id(): Unable to obtain my DSS keys | RCA encryption in phase 1 failed because the ZyWALL did not receive the DSS (Digital Signature Standard) keys. |
| Build Phase 1 ID | The router has started to build the phase 1 ID. |
| Adjust TCP MSS to %d | The router automatically changed the TCP Maximum Segment Size value after establishing a tunnel. |
| Rule <%d> input idle time out, disconnect | The tunnel for the listed rule was dropped because there was no inbound traffic within the idle timeout period. |
| XAUTH succeed! Remote user: <Username> | The ZyWALL, acting as authentication server, was able to authenticate the username given in this log. |
| XAUTH fail! Remote user: <Username> | The ZyWALL, acting as authentication server, was not able to authenticate the username given in this log. |
| XAUTH succeed! My name: <Username> | The ZyWALL, acting as an authentication client, provided the listed username to the authentication server and it was authenticated. |
| XAUTH fail! My name: <Username> | The ZyWALL, acting as an authentication client, provided the listed username to the authentication server and it was not authenticated. |
| Rule[%d] Phase 1 negotiation mode mismatch | The listed rule's IKE phase 1 negotiation mode did not match between the router and the peer. |
| Rule [%d] Phase 1 encryption algorithm mismatch | The listed rule's IKE phase 1 encryption algorithm did not match between the router and the peer. |
| Rule [%d] Phase 1 authentication algorithm mismatch | The listed rule's IKE phase 1 authentication algorithm did not match between the router and the peer. |
| Rule [%d] Phase 1 authentication method mismatch | The listed rule's IKE phase 1 authentication method did not match between the router and the peer. |
| Rule [%d] Phase 1 key group mismatch | The listed rule's IKE phase 1 key group did not match between the router and the peer. |
| Rule [%d] Phase 2 protocol mismatch | The listed rule's IKE phase 2 protocol did not match between the router and the peer. |
| Rule [%d] Phase 2 encryption algorithm mismatch | The listed rule's IKE phase 2 encryption algorithm did not match between the router and the peer. |
| Rule [%d] Phase 2 authentication algorithm mismatch | The listed rule's IKE phase 2 authentication algorithm did not match between the router and the peer. |
| Rule [%d] Phase 2 encapsulation mismatch | The listed rule's IKE phase 2 encapsulation did not match between the router and the peer. |
| Rule [%d]> Phase 2 pfs mismatch | The listed rule's IKE phase 2 perfect forward secret (PFS) setting did not match between the router and the peer. |
| Rule [%d] Phase 1 ID mismatch | The listed rule's IKE phase 1 ID did not match between the router and the peer. |
| Rule [%d] Phase 1 hash mismatch | The listed rule's IKE phase 1 hash did not match between the router and the peer. |
| Rule [%d] Phase 1 preshared key mismatch | The listed rule's IKE phase 1 pre-shared key did not match between the router and the peer. |

**Table 188** IKE Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Rule [%d] Tunnel built successfully | The listed rule's IPSec tunnel has been built successfully. |
| Rule [%d] Peer's public key not found | The listed rule's IKE phase 1 peer's public key was not found. |
| Rule [%d] Verify peer's signature failed | The listed rule's IKE phase 1verification of the peer's signature failed. |
| Rule [%d] Sending IKE request | IKE sent an IKE request for the listed rule. |
| Rule [%d] Receiving IKE request | IKE received an IKE request for the listed rule. |
| Swap rule to rule [%d] | The router changed to using the listed rule. |
| Rule [%d] Phase 1 key length mismatch | The listed rule's IKE phase 1 key length (with the AES encryption algorithm) did not match between the router and the peer. |
| Rule [%d] phase 1 mismatch | The listed rule's IKE phase 1 did not match between the router and the peer. |
| Rule [%d] phase 2 mismatch | The listed rule's IKE phase 2 did not match between the router and the peer. |
| Rule [%d] Phase 2 key length mismatch | The listed rule's IKE phase 2 key lengths (with the AES encryption algorithm) did not match between the router and the peer. |
| Remote Gateway Addr in rule [%s] is changed to %s" | The IP address for the domain name of the peer gateway in the listed rule changed to the listed IP address. |
| New My ZyWALL Addr in rule [%s] is changed to %s | The IP address for the domain name of the ZyWALL in the listed rule changed to the listed IP address. |
| Remote Gateway Addr has changed, tunnel [%s] will be deleted | The listed tunnel will be deleted because the remote gateway's IP address changed. |
| My ZyWALL Addr has changed, tunnel [%s] will be deleted | The listed tunnel will be deleted because the ZyWALL's IP address changed. |
| Rule [%s] delete successfully | The ZyWALL successfully deleted a phase 2 tunnel. |
| Cannot get My IP Addr from DDNS for rule [%s] | The ZyWALL was unable to resolve the domain name used as the My IP Address for the listed phase 1 rule. |

**Table 189** PKI Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Enrollment successful | The SCEP online certificate enrollment was successful. The Destination field records the certification authority server IP address and port. |
| Enrollment failed | The SCEP online certificate enrollment failed. The Destination field records the certification authority server's IP address and port. |
| Failed to resolve <SCEP CA server url> | The SCEP online certificate enrollment failed because the certification authority server's address cannot be resolved. |
| Enrollment successful | The CMP online certificate enrollment was successful. The Destination field records the certification authority server's IP address and port. |

**Table 189** PKI Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| `Enrollment failed` | The CMP online certificate enrollment failed. The Destination field records the certification authority server's IP address and port. |
| `Failed to resolve <CMP CA server url>` | The CMP online certificate enrollment failed because the certification authority server's IP address cannot be resolved. |
| `Rcvd ca cert: <subject name>` | The router received a certification authority certificate, with subject name as recorded, from the LDAP server whose IP address and port are recorded in the Source field. |
| `Rcvd user cert: <subject name>` | The router received a user certificate, with subject name as recorded, from the LDAP server whose IP address and port are recorded in the Source field. |
| `Rcvd CRL <size>: <issuer name>` | The router received a CRL (Certificate Revocation List), with size and issuer name as recorded, from the LDAP server whose IP address and port are recorded in the Source field. |
| `Rcvd ARL <size>: <issuer name>` | The router received an ARL (Authority Revocation List), with size and issuer name as recorded, from the LDAP server whose address and port are recorded in the Source field. |
| `Failed to decode the received ca cert` | The router received a corrupted certification authority certificate from the LDAP server whose address and port are recorded in the Source field. |
| `Failed to decode the received user cert` | The router received a corrupted user certificate from the LDAP server whose address and port are recorded in the Source field. |
| `Failed to decode the received CRL` | The router received a corrupted CRL (Certificate Revocation List) from the LDAP server whose address and port are recorded in the Source field. |
| `Failed to decode the received ARL` | The router received a corrupted ARL (Authority Revocation List) from the LDAP server whose address and port are recorded in the Source field. |
| `Rcvd data <size> too large! Max size allowed: <max size>` | The router received directory data that was too large (the size is listed) from the LDAP server whose address and port are recorded in the Source field. The maximum size of directory data that the router allows is also recorded. |
| `Cert trusted: <subject name>` | The router has verified the path of the certificate with the listed subject name. |
| `Due to <reason codes>, cert not trusted: <subject name>` | Due to the reasons listed, the certificate with the listed subject name has not passed the path verification. The recorded reason codes are only approximate reasons for not trusting the certificate. Please see Table 197 on page 575 for the corresponding descriptions of the codes. |

| 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. |

| CODE | DESCRIPTION |
|---|---|
| 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. |
| 25 | Database method failed due to timeout. |
| 26 | Database method failed. |
| 27 | Path was not verified. |
| 28 | Maximum path length reached. |

**Table 190** 802.1X Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Local User Database accepts user. | A user was authenticated by the local user database. |
| Local User Database reports user credential error. | A user was not authenticated by the local user database because of an incorrect user password. |
| Local User Database does not find user`s credential. | A user was not authenticated by the local user database because the user is not listed in the local user database. |
| RADIUS accepts user. | A user was authenticated by the RADIUS Server. |
| RADIUS rejects user. Pls check RADIUS Server. | A user was not authenticated by the RADIUS Server. Please check the RADIUS Server. |
| Local User Database does not support authentication method. | The local user database only supports the EAP-MD5 method. A user tried to use another authentication method and was not authenticated. |
| User logout because of session timeout expired. | The router logged out a user whose session expired. |
| User logout because of user deassociation. | The router logged out a user who ended the session. |

**Table 190** 802.1X Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| User logout because of no authentication response from user. | The router logged out a user from which there was no authentication response. |
| User logout because of idle timeout expired. | The router logged out a user whose idle timeout period expired. |
| User logout because of user request. | A user logged out. |
| Local User Database does not support authentication mothed. | A user tried to use an authentication method that the local user database does not support (it only supports EAP-MD5). |
| No response from RADIUS. Pls check RADIUS Server. | There is no response message from the RADIUS server, please check the RADIUS server. |
| Use Local User Database to authenticate user. | The local user database is operating as the authentication server. |
| Use RADIUS to authenticate user. | The RADIUS server is operating as the authentication server. |
| No Server to authenticate user. | There is no authentication server to authenticate a user. |
| Local User Database does not find user`s credential. | A user was not authenticated by the local user database because the user is not listed in the local user database. |
| Invalid RADIUS Authentication Server Port number | The RADIUS authentication server port number is invalid. |
| Invalid RADIUS Accounting Server Port number | The RADIUS accounting server port number is invalid. |

**Table 191** ACL Setting Notes

| PACKET DIRECTION | DIRECTION | DESCRIPTION |
|---|---|---|
| (L to W) | LAN to WAN | ACL set for packets traveling from the LAN to the WAN. |
| (W to L) | WAN to LAN | ACL set for packets traveling from the WAN to the LAN. |
| (D to L) | DMZ to LAN | ACL set for packets traveling from the DMZ to the LAN. |
| (D to W) | DMZ to WAN | ACL set for packets traveling from the DMZ to the WAN. |
| (W to D) | WAN to DMZ | ACL set for packets traveling from the WAN to the DMZ. |
| (L to D) | LAN to DMZ | ACL set for packets traveling from the LAN to the DMZ. |
| (L to L/ZW) | LAN to LAN/ ZyWALL | ACL set for packets traveling from the LAN to the LAN or the ZyWALL. |
| (W to W/ZW) | WAN to WAN/ ZyWALL | ACL set for packets traveling from the WAN to the WAN or the ZyWALL. |
| (D to D/ZW) | DMZ to DMZ/ ZyWALL | ACL set for packets traveling from the DMZ to the DM or the ZyWALL. |
| (L to WL) | LAN to WLAN | ACL set for packets traveling from the LAN to the WLAN. |
| (WL to L) | WLAN to LAN | ACL set for packets traveling from the WLAN to the LAN. |
| (W to WL) | WAN to WLAN | ACL set for packets traveling from the WAN to the WLAN. |
| (WL to W) | WLAN to WAN | ACL set for packets traveling from the WLAN to the WAN. |

**Table 191** ACL Setting Notes (continued)

| PACKET DIRECTION | DIRECTION | DESCRIPTION |
|---|---|---|
| (D to WL) | DMZ to WLAN | ACL set for packets traveling from the DMZ to the WLAN. |
| (WL to D) | WLAN to DMZ | ACL set for packets traveling from the WLAN to the DMZ. |
| (WL to WL) | WLAN to WLAN/ ZyWALL | ACL set for packets traveling from the WLAN to the WLAN or the ZyWALL. |

**Table 192** ICMP Notes

| TYPE | CODE | DESCRIPTION |
|---|---|---|
| 0 | | Echo Reply |
| | 0 | Echo reply message |
| 3 | | Destination Unreachable |
| | 0 | Net unreachable |
| | 1 | Host unreachable |
| | 2 | Protocol unreachable |
| | 3 | Port unreachable |
| | 4 | A packet that needed fragmentation was dropped because it was set to Don't Fragment (DF) |
| | 5 | Source route failed |
| 4 | | Source Quench |
| | 0 | A gateway may discard internet datagrams if it does not have the buffer space needed to queue the datagrams for output to the next network on the route to the destination network. |
| 5 | | Redirect |
| | 0 | Redirect datagrams for the Network |
| | 1 | Redirect datagrams for the Host |
| | 2 | Redirect datagrams for the Type of Service and Network |
| | 3 | Redirect datagrams for the Type of Service and Host |
| 8 | | Echo |
| | 0 | Echo message |
| 11 | | Time Exceeded |
| | 0 | Time to live exceeded in transit |
| | 1 | Fragment reassembly time exceeded |
| 12 | | Parameter Problem |
| | 0 | Pointer indicates the error |
| 13 | | Timestamp |
| | 0 | Timestamp request message |
| 14 | | Timestamp Reply |
| | 0 | Timestamp reply message |
| 15 | | Information Request |
| | 0 | Information request message |

**Table 192** ICMP Notes (continued)

| TYPE | CODE | DESCRIPTION |
|---|---|---|
| 16 | | Information Reply |
| | 0 | Information reply message |

**Table 193** IDP Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| The buffer size is too small! | The buffer for holding IDP information such as the signature file version was too small to hold any more information. |
| The format of the user config file is incorrect! | There was a format error in the configuration backup file that someone attempted to load into the system. |
| The system is doing signature update now , please wait! | The device is updating the signature file. |
| No data! | The system could not find any IDP signatures that matched a search. |
| IDP %s! | The device detected an intrusion event in a connection. The format of %s is “ID” followed by the IDP ID signature number and the IDP signature name. For example, ID:10001,Window Ping. |
| Can not find the signature , please update the signature! | The device does not have a signature file loaded. |
| Failed in signature update - %s! | The device failed to update the signature file through the Internet. %s describes the reason for the error. You may need to provide the error message when contacting customer support if you are repeatedly unable to download the signature file from the update server. |
| Check signature version - %s. | The device attempted to check for the latest available signature version. %s gives details. Either the check was unsuccessful due to the server being busy or the device is already using the latest available firmware. |
| Signature update OK - New signature version: <Signature version> Release Date: <Release date>! | The device updated the signature file successfully. The signature file’s version and release date are included. |
| The turbo card is not ready , please insert the card and reboot! | The turbo card is not installed. |

**Table 194** AV Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| HTTP Virus infected - %s! | The device detected a virus in an HTTP connection. The format of %s is “ID” Virus ID number, virus name, filename. For example, ID:30001,CIH.Win95,/game.exe. |
| FTPDATA Virus infected - %s! | The device detected a virus in a FTPDATA connection. The format of %s is “ID” Virus ID number, virus name, filename. For example, ID:30001,CIH.Win95,/game.exe. |

**Table 194** AV Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| SMTP Virus infected - %s! | The device detected a virus in a SMTP connection. The format of %s is "ID" Virus ID number, virus name, filename. For example, ID:30001,CIH.Win95,/game.exe. |
| POP3 Virus infected - %s! | The device detected a virus in a POP3 connection. The format of %s is "ID" Virus ID number, virus name, filename. For example, ID:30001,CIH.Win95,/game.exe. |
| HTTP Bypass - %s! | The device bypassed the scanning of files in HTTP connections. %s is the filename. For example, game.zip. |
| FTPDATA Bypass - %s! | The device bypassed the scanning of files in FTP data connections. %s is the filename. For example, game.zip. |
| SMTP Bypass - %s! | The device bypassed the scanning of files in SMTP connections. %s is the filename. For example, game.zip. |
| POP3 Bypass - %s! | The device bypassed the scanning of files in POP3 connections. %s is the filename. For example, game.zip. |
| Can not find the signature , please update the signature! | The device does not have a signature file loaded. |
| Failed in signature update - %s! | The device failed to update the signature file through the Internet. %s describes the reason for the error. You may need to provide the error message when contacting customer support if you are repeatedly unable to download the signature file from the update server. |
| Check signature version - %s. | The device attempted to check for the latest available signature version. %s gives details. Either the check was unsuccessful due to the server being busy or the device is already using the latest available firmware. |
| Update the signature file successfully. | The device updated the signature file successfully. |
| The turbo card is not ready , please insert the card and reboot! | The turbo card is not installed. |
| The system is doing signature update now , please wait! | The device is updating signature files. |
| The signature search engine is not ready! | The signature search engine is not ready. Check that you have properly inserted the Turbocard. |
| HTTP Block. The session is over maximun ZIP sessions - %s! %PACKET_DIRECTION% | The number of zip files in HTTP connections has exceeded the maximum number that can be concurrently scanned.<br>"%s" is the name of the zip file which has exceeded the limit. |
| FTPDATA Block. The session is over maximun ZIP sessions - %s! %PACKET_DIRECTION% | The number of zip files in FTP data connections has exceeded the maximum number that can be concurrently scanned.<br>"%s" is the name of the zip file which has exceeded the limit. |

**Table 194** AV Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| SMTP Block. The session is over maximun ZIP sessions - %s! %PACKET_DIRECTION% | The number of zip files in SMTP connections has exceeded the maximum number that can be concurrently scanned.<br>"%s" is the name of the zip file which has exceeded the limit. |
| POP3 Block. The session is over maximun ZIP sessions - %s! %PACKET_DIRECTION% | The number of zip files in POP3 connections has exceeded the maximum number that can be concurrently scanned.<br>"%s" is the name of the zip file which has exceeded the limit. |
| Zip file unsupported - %s! %PACKET_DIRECTION% | The zip file compression method is unsupported. The ZyWALL supports common zip file compression methods such as stored, deflated or deflated64.<br>"%s" is the name of the zip file. |

**Table 195** AS Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Mail is in the Black List - Mail From:%EMAIL_ADDRESS% Subject:%MAIL_SUBJECT%! | An e-mail with the listed source and subject matched an anti-spam blacklist entry. |
| Mail score is higher or equal than threshold - Spam Score:%d Mail From:%EMAIL_ADDRESS% Subject:%MAIL_SUBJECT%! | The spam score (listed) for the e-mail with the listed source and subject was higher than or equal to the spam score threshold. |
| Query external database timeout - [%Rating Server IP Address%] | The anti-spam external database query timed out. The following log identifies the e-mail that was being checked. |
| Mail From:Email address Subject:Mail Subject! | This is the source and subject of an e-mail for which the anti-spam external database query failed. |
| External database query failed - [%Rating Server IP Address%] %s! | An anti-spam external database query failed due to an error, such as Http Error 404, Http connection can't be built. Please refer to "reason" field. The following log identifies the e-mail that was being checked. |
| Mail From:Email address Subject:Mail Subject! | This is the source and subject of an e-mail for which the anti-spam external database query failed. |
| Exceed maximum mail sessions (%d). | The number of concurrent mail sessions went over the limit (%d). |
| Error code from anti-spam server - [%Rating Server IP Address%] %s! | The device received an error code from the anti-spam external database server. Please refer to "reason" field. The following log identifies the e-mail that was being checked. |
| Mail From:Email address Subject:Mail Subject! | This is the source and subject of an e-mail for which the anti-spam external database query failed. |
| Unknown anti-spam query response - [%Rating Server IP Address%]! | The device received a response with an unknown format from the anti-spam external database server. The following log identifies the e-mail that was being checked. |

**Table 195** AS Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Mail From:Email address Subject:Mail Subject! | This is the source and subject of an e-mail for which the anti-spam external database query failed. |
| Remove rating server [%Rating Server IP Address%] from server list! | The listed server IP address has been removed from the list of anti-spam external database servers. |
| "This is a phishing mail - Spam Score:%d Mail From:%EMAIL_ADDRESS% Subject:%MAIL_SUBJECT%! " | The spam score (listed) for the e-mail with the listed source and subject was higher than the spam score threshold. The anti-spam external database identified the e-mail as a phishing mail. |
| Invalid parameter for AsEngine! | There was an internal AS system error. This type of error causes the device to restart. |
| Mail Parser buffer is overflow! | There were too many characters in a single line of an e-mail header that the device was attempting to parse. |
| There is no available HTTP session for external database! | There was not an HTTP session available to query the external database. |
| Mail From:Email address Subject:Mail Subject! | This is the source and subject of an e-mail for which there was not an HTTP session available for queuing the external database. |
| Mail Digest creating failed! | The device was not able to create a digest of an e-mail. |
| Mail From:Email address Subject:Mail Subject! | This is the source and subject of an e-mail for which the device was not able to create a digest. |
| There is no available timer for external database! | There was not an internal timer mechanism free for the anti-spam feature to use when sending a query to the external database. |
| Mail From:Email address Subject:Mail Subject! | This is the source and subject of an e-mail for which there was not an internal timer mechanism available for queuing the external database. |
| There is no available HTTP session and timer for external database! | There was not an HTTP session available to query the external database. There also was not an internal timer mechanism free for the anti-spam feature to use when sending a query to the external database. |
| Mail From:Email address Subject:Mail Subject! | This is the source and subject of an e-mail for which there was no HTTP session and no internal timer mechanism available for queuing the external database. |

## Syslog Logs

There are two types of syslog: event logs and traffic logs. The device generates an event log when a system event occurs, for example, when a user logs in or the device is under attack. The device generates a traffic log when a "session" is terminated. A traffic log summarizes the session's type, when it started and stopped the amount of traffic that was sent and received and so on. An external log analyzer can reconstruct and analyze the traffic flowing through the device after collecting the traffic logs.

**Table 196** Syslog Logs

| LOG MESSAGE | DESCRIPTION |
|---|---|
| `Event Log: <Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="<msg>" note="<note>" devID="<mac address>" cat="<category>"` | This message is sent by the system ("RAS" displays as the system name if you haven't configured one) when the router generates a syslog. The facility is defined in the web **MAIN MENU**, **LOGS**, **Log Settings** page. The severity is the log's syslog class. The definition of messages and notes are defined in the other log tables. The "devID" is the MAC address of the router's LAN port. The "cat" is the same as the category in the router's logs. |
| `Traffic Log: <Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="Traffic Log" note="Traffic Log" devID="<mac address>" cat="Traffic Log" duration=seconds sent=sentBytes rcvd=receiveBytes dir="<from:to>" protoID=IPProtocolID proto="serviceName" trans="IPSec/Normal"` | This message is sent by the device when the connection (session) is closed. The facility is defined in the Log Settings screen. The severity is the traffic log type. The message and note always display "Traffic Log". The "proto" field lists the service name. The "dir" field lists the incoming and outgoing interfaces ("LAN:LAN", "LAN:WAN", "LAN:DMZ", "LAN:DEV" for example). |
| `Event Log: <Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" ob="<0\|1>" ob_mac="<mac address>" msg="<msg>" note="<note>" devID="<mac address>" cat="<category>"` | This message is sent by the device ("RAS" displays as the system name if you haven't configured one) at the time when this syslog is generated. The facility is defined in the web **MAIN MENU**, **LOGS**, **Log Settings** page. The severity is the log's syslog class. The definition of messages and notes are defined in the other log tables. OB is the Out Break flag and the mac address of the Out Break PC. |
| `Event Log: <Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" ob="0\|1" ob_mac="<mac address>" msg="<msg>" note="<note>" devID="<mac address>" cat="Anti Virus" encode="< uu \| b64 >"` | This message is sent by the device ("RAS" displays as the system name if you haven't configured one) at the time when this syslog is generated. The facility is defined in the web **MAIN MENU**, **LOGS**, **Log Settings** page. The severity is the log's syslog class. The "encode" message indicates the mail attachments encoding method. The definition of messages and notes are defined in the Anti-Virus log descriptions. |

**Table 196** Syslog Logs (continued)

| LOG MESSAGE | DESCRIPTION |
|---|---|
| Event Log: <Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" ob="<0\|1>" ob_mac="<mac address>" msg="<msg>" note="<note>" devID="<mac address>" cat="IDP" class="<idp class>" sid="<idp sid> act="<idp action>" count="1" | This message is sent by the device ("RAS" displays as the system name if you haven't configured one) at the time when this syslog is generated. The facility is defined in the web **MAIN MENU**, **LOGS**, **Log Settings** page. The severity is the log's syslog class. The definition of messages and notes are defined in the IDP log descriptions. |
| Event Log: <Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" ob="<0\|1>" ob_mac="<mac address>" msg="<msg>" note="<note>" devID="<mac address>" cat="Anti Spam" 1stReIP="<IP>" | This message is sent by the device ("RAS" displays as the system name if you haven't configured one) at the time when this syslog is generated. The facility is defined in the web **MAIN MENU**, **LOGS**, **Log Settings** page. The severity is the log's syslog class. 1stReIP is the IP address of the first mail relay server. The definition of messages and notes are defined in the Anti-Spam log descriptions. |

The following table shows RFC-2408 ISAKMP payload types that the log displays. Please refer to the RFC for detailed information on each type.

**Table 197** RFC-2408 ISAKMP Payload Types

| LOG DISPLAY | PAYLOAD TYPE |
|---|---|
| SA | Security Association |
| PROP | Proposal |
| TRANS | Transform |
| KE | Key Exchange |
| ID | Identification |
| CER | Certificate |
| CER_REQ | Certificate Request |
| HASH | Hash |
| SIG | Signature |
| NONCE | Nonce |
| NOTFY | Notification |
| DEL | Delete |
| VID | Vendor ID |

# 33

# Maintenance Screens

## 33.1 Overview

This chapter displays information on the maintenance screens. The maintenance screens can help you view system information, upload new firmware, manage configuration and restart your ZyWALL.

### 33.1.1 What You Can Do in the Maintenance Screens

- Use the **General Setup** screen (Section 33.2 on page 585) to configure administrative and system-related information.
- Use the **Password** screen (Section 33.3 on page 586) to change the ZyWALL's management password.
- Use the **Time and Date** screen (Section 33.4 on page 587) to configure the ZyWALL's time based on your local time zone.
- Use the **Device Mode** screen (Section 33.5 on page 591) to configure the ZyWALL as a router or a bridge.
- Use the **F/W Upload** screen (Section 33.8 on page 595) to upgrade the ZyWALL's firmware.
- Use the **Backup and Restore** screen (Section 33.9 on page 597) to backup and restore the ZyWALL configuration file and to reset the device to factory settings.
- Use the **Restart** screen (Section 33.10 on page 599) to reboot the ZyWALL device.
- Use the **Diagnostics** screen (Section 33.11 on page 599) to have the ZyWALL generate and send diagnostic files by e-mail and/or the console port.

## 33.2 The General Setup Screen

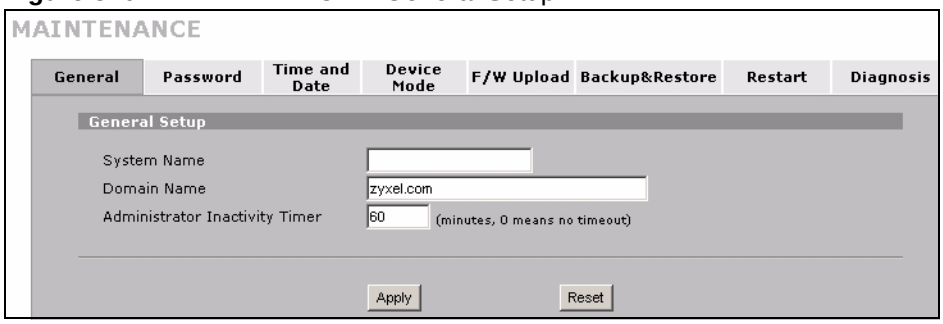
**General Setup** contains administrative and system-related information. **System Name** is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name".

- In Windows 95/98 click **Start**, **Settings**, **Control Panel**, **Network**. Click the Identification tab, note the entry for the **Computer Name** field and enter it as the **System Name**.
- In Windows 2000, click **Start**, **Settings**, **Control Panel** and then double-click **System**. Click the **Network Identification** tab and then the **Properties** button. Note the entry for the **Computer name** field and enter it as the **System Name**.

- In Windows XP, click **Start**, **My Computer**, **View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the ZyWALL **System Name**.

Click **MAINTENANCE** to open the **General** screen. Use this screen to configure administrative and system-related information.

**Figure 340** MAINTENANCE > General Setup




The following table describes the labels in this screen.

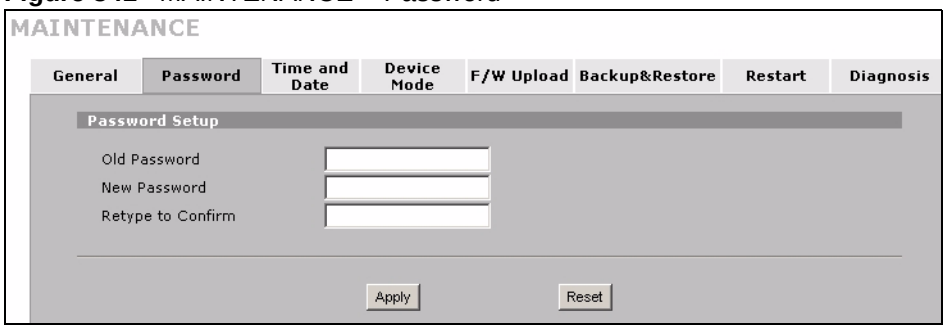
**Table 198** MAINTENANCE > General Setup

| LABEL | DESCRIPTION |
|---|---|
| General Setup | |
| System Name | Choose a descriptive name for identification purposes. It is recommended you enter your computer's "Computer name" in this field. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted. |
| Domain Name | The **Domain Name** entry is what is propagated to the DHCP clients on the LAN. If you leave this blank, the domain name obtained by DHCP from the ISP is used. While you must enter the host name (System Name), the domain name can be assigned from the ZyWALL via DHCP.<br>Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP.<br>The domain name entered by you is given priority over the ISP assigned domain name. |
| Administrator Inactivity Timer | Type how many minutes a management session (either via the web configurator or SMT) can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended). |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 33.3 The Password Screen

Click **MAINTENANCE** > **Password** to open the following screen. Use this screen to change the ZyWALL's management password.

**Figure 341** MAINTENANCE > Password




The following table describes the labels in this screen.

**Table 199** MAINTENANCE > Password

| LABEL | DESCRIPTION |
|---|---|
| Old Password | Type the default password or the existing password you use to access the system in this field. If you forget the password, you may have to use the hardware **RESET** button. This restores the default password of 1234. |
| New Password | Type your new system password (up to 30 characters). Note that as you type a password, the screen displays a (*) for each character you type. |
| Retype to Confirm | Type the new password again for confirmation. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 33.4 The Time and Date Screen

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 when you turn on your ZyWALL.

### Pre-defined NTP Time Server Pools

When you turn on the ZyWALL for the first time, the date and time start at 2000-01-01 00:00:00. The ZyWALL then attempts to synchronize with an NTP time server from one of the 0.pool.ntp.org, 1.pool.ntp.org or 2.pool.ntp.org NTP time server pools. These are virtual clusters of time servers that use a round robin method to provide different NTP servers to clients.

The ZyWALL continues to use the NTP time server pools if you do not specify a time server or it cannot synchronize with the time server you specified.

The ZyWALL can use the NTP time server pools regardless of the time protocol you select.

When the ZyWALL uses the NTP time server pools, it randomly selects one pool and tries to synchronize with a server in 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 server pools have been tried.

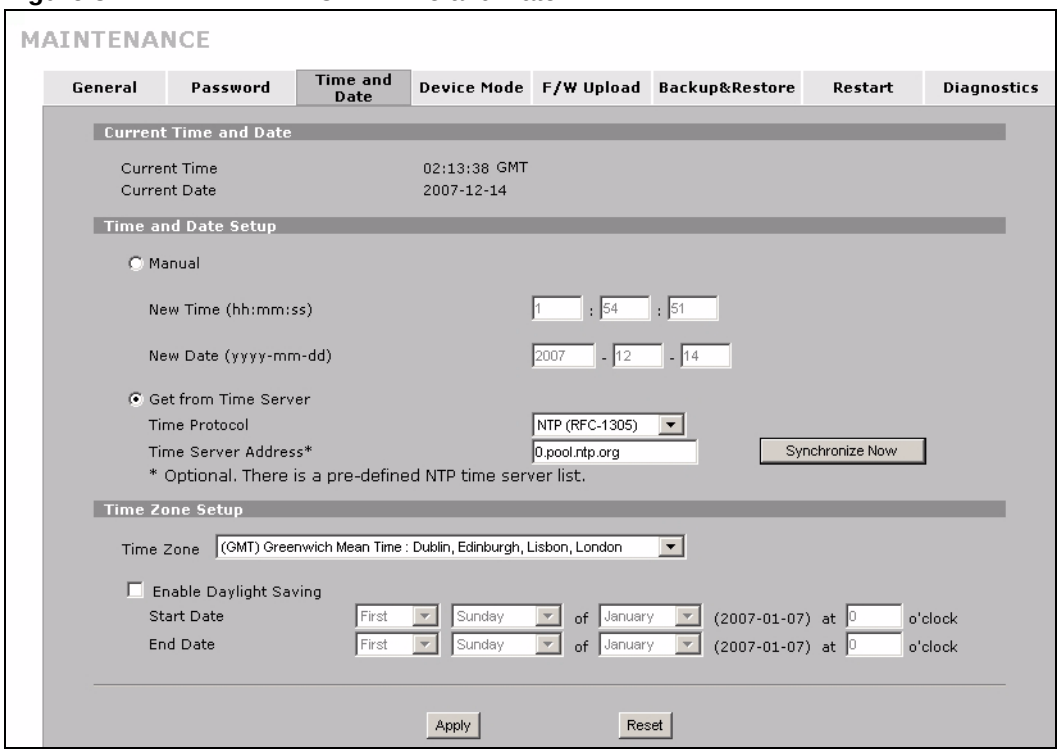
### Resetting the Time

The ZyWALL resets the time in the following instances:

- When you click **Synchronize Now**.
- On saving your changes.
- When the ZyWALL starts up.
- 24-hour intervals after starting.

To change your ZyWALL's time and date, click **MAINTENANCE** > **Time and Date**. The screen appears as shown. Use this screen to configure the ZyWALL's time based on your local time zone.

**Figure 342** MAINTENANCE > Time and Date




The following table describes the labels in this screen.

**Table 200** MAINTENANCE > Time and Date

| LABEL | DESCRIPTION |
|---|---|
| Current Time and Date | |
| Current Time | This field displays the ZyWALL's present time. |
| Current Date | This field displays the ZyWALL's present date. |
| Time and Date Setup | |

**Table 200** MAINTENANCE > Time and Date (continued)

| LABEL | DESCRIPTION |
|---|---|
| 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 new time and date you entered has priority and the Time Zone and Daylight Saving settings do not affect it. |
| 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**. |
| 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 specified below. |
| Time Protocol | Select the time service protocol that your time server uses. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works.<br>The main difference between them is the format.<br>**Daytime (RFC 867)** format is day/month/year/time zone of the server.<br>**Time (RFC 868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0.<br>The default, **NTP (RFC 1305)**, is similar to **Time (RFC 868)**. |
| 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 (including the time server address). |
| 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 **o'clock** 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 **2:00**.<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 **o'clock** 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 200** MAINTENANCE > Time and Date (continued)

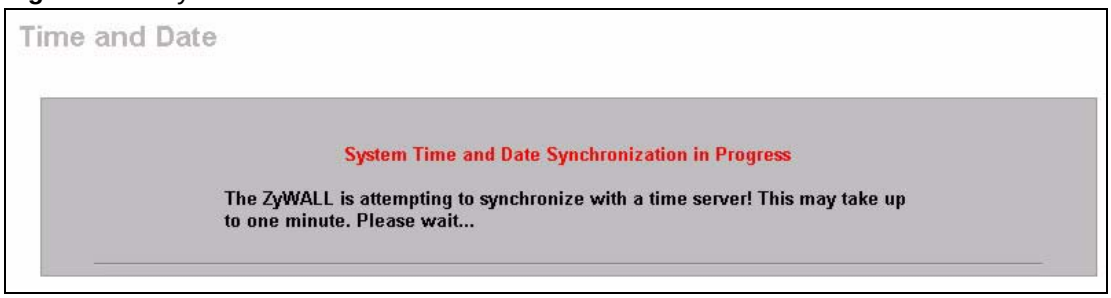
| LABEL | DESCRIPTION |
|---|---|
| End Date | Configure the day and time when Daylight Saving Time ends if you selected **Enable Daylight Saving**. The **o'clock** field uses the 24 hour format. Here are a couple of examples:<br>Daylight Saving Time ends in the United States on the first Sunday of November. 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 **2:00**.<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 **o'clock** 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). |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 33.4.1 Time Server Synchronization Example

Click the **Synchronize Now** button to get the time and date from the predefined time server or the time server you specified in the **Time Server Address** field.

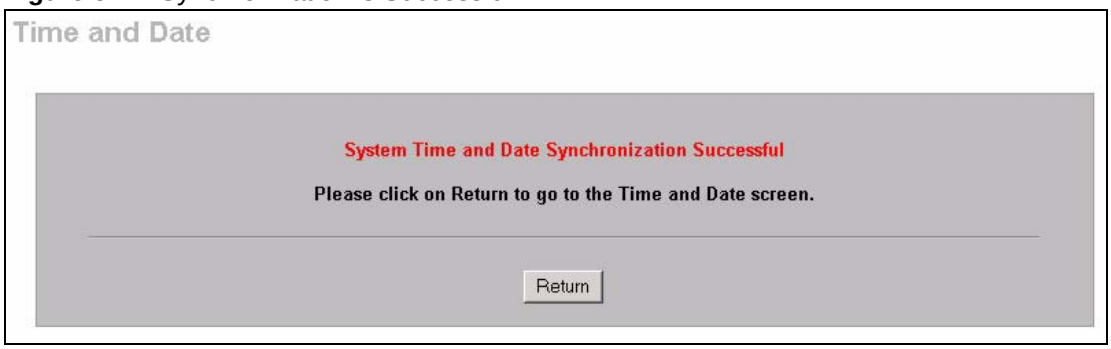
When the **System Time and Date Synchronization in Process** screen appears, wait up to one minute.

**Figure 343** Synchronization in Process



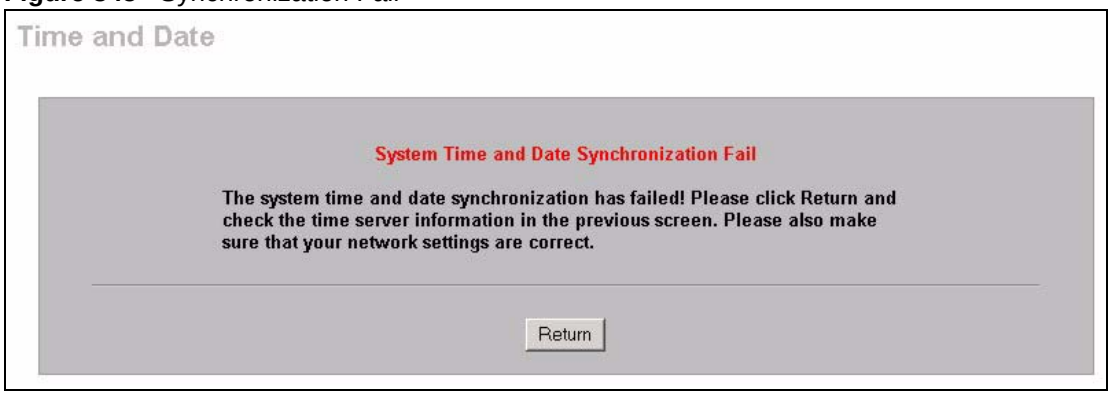

Click the **Return** button to go back to the **Time and Date** screen after the time and date is updated successfully.

**Figure 344** Synchronization is Successful




If the update was not successful, the following screen appears. Click **Return** to go back to the **Time and Date** screen.

**Figure 345** Synchronization Fail




## 33.5 The Device Mode Screen

Use this screen to configure your ZyWALL as a router or a bridge. In router mode, the ZyWALL functions as a router. In bridge mode, the ZyWALL functions as a transparent firewall (also known as a bridge firewall).

### Introduction To Transparent Bridging

A transparent bridge is invisible to the operation of a network in that it does not modify the frames it forwards. The bridge checks the source address of incoming frames on the port and learns MAC addresses to associate with that port. All future communications to that MAC address will only be sent on that port.

The bridge gradually builds a host MAC-address-to-port mapping table such as in the following example, during the learning process.

**Table 201** MAC-address-to-port Mapping Table

| HOST MAC ADDRESS | PORT |
|---|---|
| 00a0c5123456 | 3 |
| 00a0c5123478 (host A) | 1 |
| 00a0c512349a | 3 |
| 00a0c51234bc | 2 |
| 00a0c51234de | 4 |

For example, if a bridge receives a frame via port 1 from host A (MAC address 00a0c5123478), the bridge associates host A with port 1. When the bridge receives another frame on one of its ports with destination address 00a0c5123478, it forwards the frame directly through port 1 after checking the internal table.

The bridge takes one of these actions after it checks the destination address of an incoming frame with its internal table:

- If the table contains an association between the destination address and any of the bridge's ports aside from the one on which the frame was received, the frame is forwarded out the associated port.

- If no association is found, the frame is flooded to all ports except the inbound port. Broadcasts and multicasts also are flooded in this way.
- If the associated port is the same as the incoming port, then the frame is dropped (filtered).

### Transparent Firewalls

A transparent firewall (also known as a transparent, in-line, shadow, stealth or bridging firewall) has the following advantages over “router firewalls”:

1. The use of a bridging firewall reduces configuration and deployment time because no networking configuration changes to your existing network (hosts, neighboring routers and the firewall itself) are needed. Just put it in-line with the network it is protecting. As it only moves frames between ports (after inspecting them), it is completely transparent.
2. Performance is improved as there's less processing overhead.
3. As a transparent bridge does not modify the frames it forwards, it is effectively “stealth” as it is invisible to attackers.

Bridging devices are most useful in complex environments that require a rapid or new firewall deployment. A transparent, bridging firewall can also be good for companies with several branch offices since the setups at these offices are often the same and it's likely that one design can be used for many of the networks. A bridging firewall could be configured at HQ, sent to the branches and then installed directly without additional configuration.

## 33.6 Configuring the Device Mode Screen (Router)

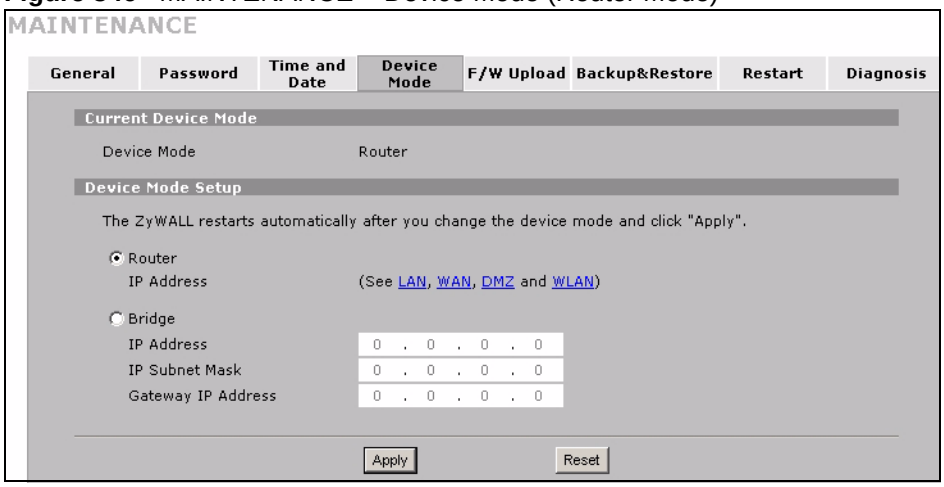
Click **MAINTENANCE** > **Device Mode** to open the following screen.

In router mode, the ZyWALL functions as a router. The ZyWALL routes traffic traveling between the ZyWALL's interfaces and filters and inspects packets.

In router mode, the ZyWALL can provide multiple WAN with load balancing (including 3G on the ZyWALL 5). It can also get an IP address from a DHCP server. It can also serve as a DHCP server to assign IP addresses to your local computers. The LAN, WAN, DMZ and WLAN interfaces all have different IP addresses. The ZyWALL also provides NAT, port forwarding, policy routing, and DNS in router mode. These features allow you to set up private network. See Table 6 on page 74 for a detailed list of other features available in router mode.

The following screen displays when the ZyWALL is in router mode.

**Figure 346** MAINTENANCE > Device Mode (Router Mode)




The following table describes the labels in this screen.

**Table 202** MAINTENANCE > Device Mode (Router Mode)

| LABEL | DESCRIPTION |
|---|---|
| Current Device Mode | |
| Device Mode | This displays whether the ZyWALL is functioning as a router or a bridge. |
| Device Mode Setup | |
| Router | When the ZyWALL is in router mode, there is no need to select or clear this radio button. |
| IP Address | Click **LAN**, **WAN**, **DMZ** or **WLAN** to go to the **LAN**, **WAN**, **DMZ** or **WLAN** screen where you can view and/or change the corresponding settings. |
| Bridge | Select this radio button and configure the following fields, then click **Apply** to set the ZyWALL to bridge mode. |
| IP Address | Enter the IP address of your ZyWALL in dotted decimal notation. |
| IP Subnet Mask | Enter the IP subnet mask of the ZyWALL. |
| Gateway IP Address | Enter the gateway IP address. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. After you click **Apply**, please wait for one minute and use the IP address you configured in the **IP Address** field to access the ZyWALL again. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

## 33.7 Configuring the Device Mode Screen (Bridge)

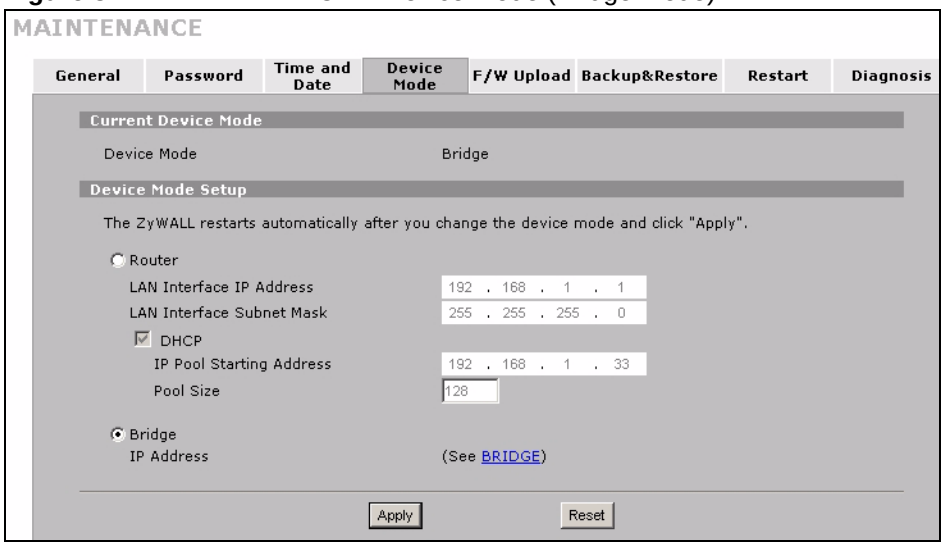
Click **MAINTENANCE** > **Device Mode** to open the following screen. Use this screen to configure your ZyWALL as a router or a bridge.

In bridge mode, the ZyWALL functions as a transparent firewall (also known as a bridge firewall). The ZyWALL bridges traffic traveling between the ZyWALL's interfaces and still filters and inspects packets. You do not need to change the configuration of your existing network.

In bridge mode, the ZyWALL cannot get an IP address from a DHCP server. The LAN, WAN, DMZ and WLAN interfaces all have the same (static) IP address and subnet mask. You can configure the ZyWALL's IP address in order to access the ZyWALL for management. If you connect your computer directly to the ZyWALL, you also need to assign your computer a static IP address in the same subnet as the ZyWALL's IP address in order to access the ZyWALL.

You can use the firewall and VPN in bridge mode. See Table 6 on page 74the user's guide for a detailed list of other features available in bridge mode.

**Figure 347** MAINTENANCE > Device Mode (Bridge Mode)




The following table describes the labels in this screen.

**Table 203** MAINTENANCE > Device Mode (Bridge Mode)

| LABEL | DESCRIPTION |
|---|---|
| Current Device Mode | |
| Device Mode | This displays whether the ZyWALL is functioning as a router or a bridge. |
| Device Mode Setup | |
| Router | Select this radio button and click **Apply** to set the ZyWALL to router mode. |
| LAN Interface IP Address | Enter the IP address of your ZyWALL' s LAN port in dotted decimal notation. 192.168.1.1 is the factory default. |
| LAN Interface Subnet Mask | Enter the IP subnet mask of the ZyWALL's LAN port. |
| DHCP | DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (computers) to obtain TCP/IP configuration at startup from a server. Unless you are instructed by your ISP, leave the **DHCP** check box selected. Clear it to stop the ZyWALL from acting as a DHCP server. When configured as a server, the ZyWALL provides TCP/IP configuration for the clients. If not, DHCP service is disabled and you must have another DHCP server on your LAN, or else the computers must be manually configured. When set as a server, fill in the rest of the DHCP setup fields. |
| IP Pool Starting Address | This field specifies the first of the contiguous addresses in the IP address pool. |
| Pool Size | This field specifies the size, or count of the IP address pool. |

**Table 203** MAINTENANCE > Device Mode (Bridge Mode) (continued)

| LABEL | DESCRIPTION |
|---|---|
| Bridge | When the ZyWALL is in bridge mode, there is no need to select or clear this radio button. |
| IP Address | Click **Bridge** to go to the **Bridge** screen where you can view and/or change the bridge settings. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. After you click **Apply**, please wait for one minute and use the IP address you configured in the **LAN Interface IP Address** field to access the ZyWALL again. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

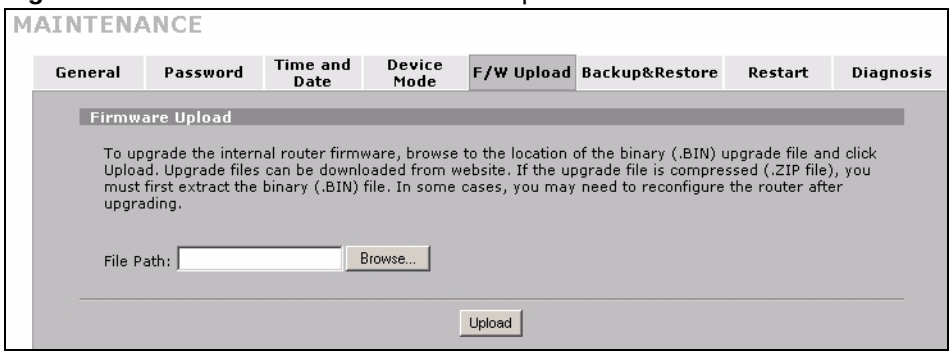
## 33.8 The F/W Upload Screen

Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a .bin extension, for example, “zywall.bin”. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot. See Section 49.5 on page 733 for upgrading firmware using FTP/TFTP commands.

Click **MAINTENANCE** > **F/W UPLOAD**. Follow the instructions in this screen to upload firmware to your ZyWALL.

Only upload firmware for your specific model!

**Figure 348** MAINTENANCE > Firmware Upload




The following table describes the labels in this screen.

**Table 204** MAINTENANCE > Firmware Upload

| LABEL | DESCRIPTION |
|---|---|
| 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. |

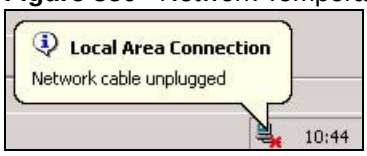
Do not turn off the ZyWALL while firmware upload is in progress!

After you see the **Firmware Upload in Process** screen, wait two minutes before logging into the ZyWALL again.

**Figure 349** Firmware Upload In Process


The ZyWALL automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

**Figure 350** Network Temporarily Disconnected




After two minutes, log in again and check your new firmware version in the **HOME** screen.

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **F/W Upload** screen.

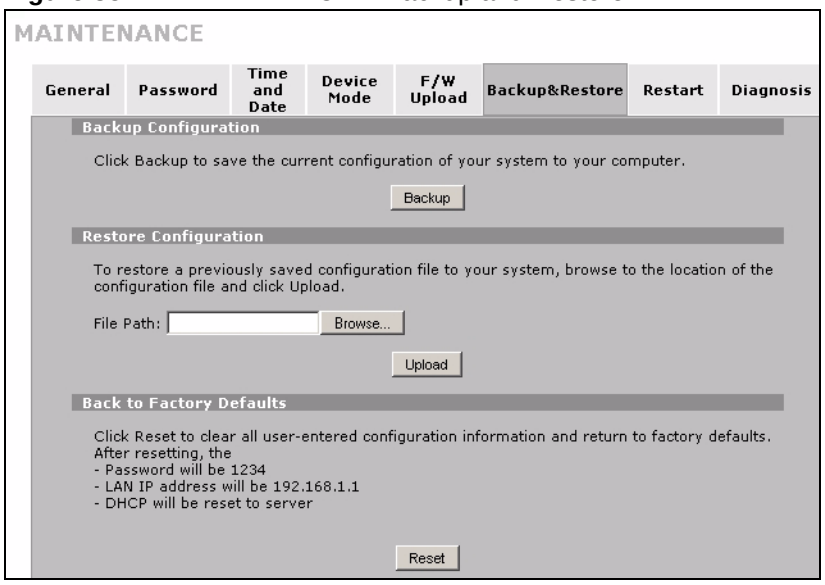
**Figure 351** Firmware Upload Error

# 33.9 The Backup and Restore Screen

See Section 49.5 on page 733 for transferring configuration files using FTP/TFTP commands.

Click **MAINTENANCE** > **Backup & Restore**. Information related to factory defaults, backup configuration, and restoring configuration appears as shown next.

**Figure 352** MAINTENANCE > Backup and Restore




## Backup Configuration

Backup configuration allows you to back up (save) the ZyWALL's current configuration to a file on your computer. Once your ZyWALL is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the ZyWALL's current configuration to your computer.

## Restore Configuration

Load a configuration file from your computer to your ZyWALL.

**Table 205** Restore Configuration

| LABEL | DESCRIPTION |
|---|---|
| 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 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. |

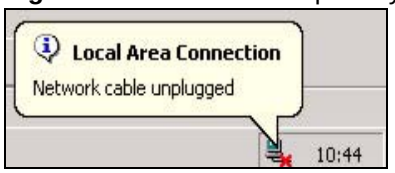
Do not turn off the ZyWALL while configuration file upload is in progress.

After you see a “restore configuration successful” screen, you must then wait one minute before logging into the ZyWALL again.

**Figure 353** Configuration Upload Successful


The ZyWALL automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

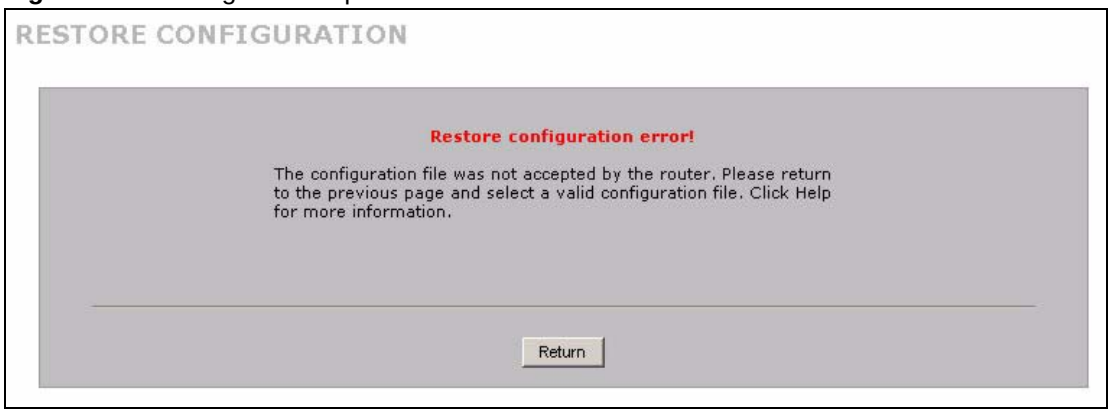
**Figure 354** Network Temporarily Disconnected




If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.1). See your Quick Start Guide for details on how to set up your computer’s IP address.

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **Configuration** screen.

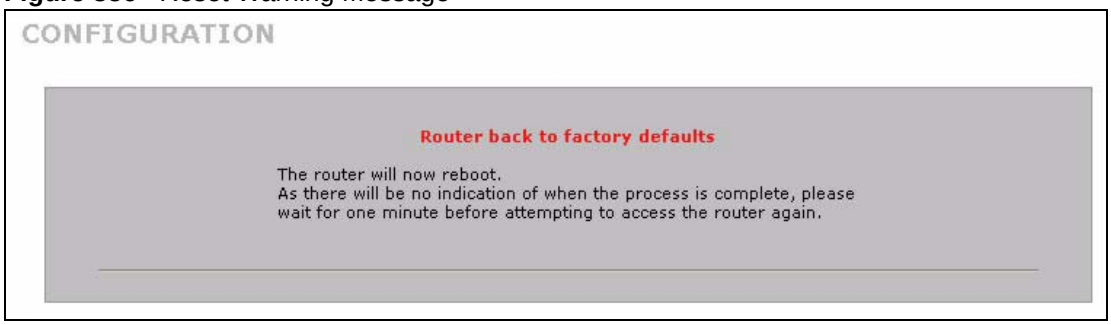
**Figure 355** Configuration Upload Error




### Back to Factory Defaults

Click the **Reset** button to clear all user-entered configuration information and return the ZyWALL to its factory defaults as shown on the screen. The following warning screen appears.

**Figure 356** Reset Warning Message



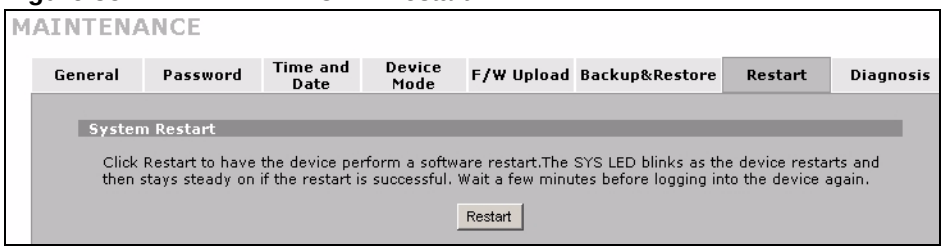

You can also press the hardware **RESET** button to reset the factory defaults of your ZyWALL. Refer to Section 3.3 on page 63 for more information on the **RESET** button.

## 33.10 The Restart Screen

System restart allows you to reboot the ZyWALL without turning the power off.

Click **MAINTENANCE** > **Restart**. Click **Restart** to have the ZyWALL reboot. Restart is different to reset; (see Section  on page 598) reset returns the device to its default configuration.

**Figure 357** MAINTENANCE > Restart



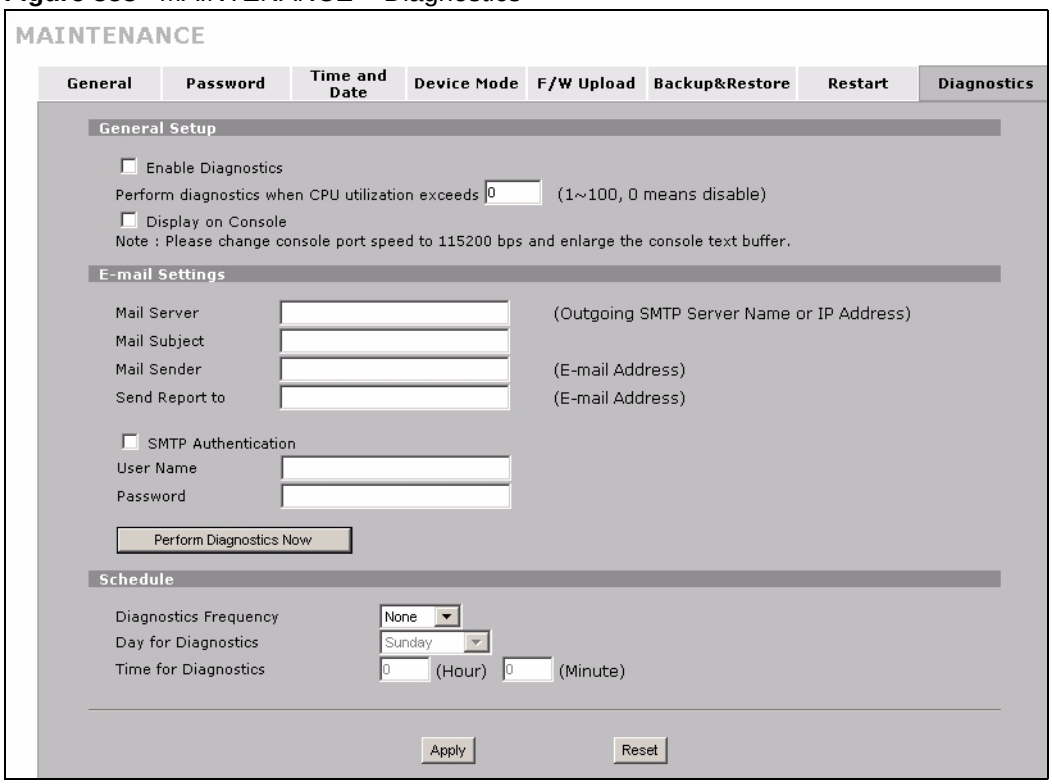

## 33.11 The Diagnostics Screen

Use the **Diagnostics** screen to have the ZyWALL generate and send diagnostic files by e-mail and/or the console port. The diagnostics files contain 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 following screen.

The ZyWALL sends only one diagnostic e-mail within five minutes (unless you click **Perform Diagnostics Now**).

**Figure 358** MAINTENANCE > Diagnostics




The following table describes the labels in this screen.

**Table 206** MAINTENANCE > Diagnostics

| LABEL | DESCRIPTION |
|---|---|
| General Setup | |
| Enable Diagnostics | Select this option to turn on the diagnostics feature. |
| Perform Diagnostics when CPU utilization exceeds | Set the ZyWALL to generate and send a diagnostic e-mail every time the CPU usage goes over the specified percent for more than 60 seconds. Enter 0 to have the ZyWALL not generate and send diagnostic files based on CPU usage going over a specific level. |
| Display on Console | Select this option to have the ZyWALL send diagnostic information through the console port. To receive the information through the console port, you still need to configure the mail settings and open a terminal emulation program on the computer connected to the console port.<br>To handle the size of the diagnostic file, change your console port speed to 115200 bps (on both the ZyWALL and your terminal emulation program) and enlarge the console text buffer. |
| E-mail Settings | |
| Mail Server | Enter the server name or the IP address of the mail server for the e-mail address specified in the **Mail Sender** field. If this field is left blank, diagnostic files will not be sent via e-mail. |
| Mail Subject | Type a title that you want to be in the subject line of the diagnostic e-mail message that the ZyWALL sends. |
| Mail Sender | Enter the e-mail address that you want to be in the from/sender line of the diagnostic e-mail message that the ZyWALL sends. If you activate SMTP authentication, the e-mail address must be able to be authenticated by the mail server as well. |

**Table 206** MAINTENANCE > Diagnostics (continued)

| LABEL | DESCRIPTION |
|---|---|
| Send Report to | Diagnostic files are sent to the e-mail address specified in this field. If this field is left blank, diagnostic files will not be sent via e-mail. |
| SMTP Authentication | SMTP (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.<br>Select the check box to activate SMTP authentication. If mail server authentication is needed but this feature is disabled, you will not receive the diagnostic files. |
| User Name | Enter the user name (up to 63 characters) (usually the user name of a mail account you specified in the **Mail Sender** field). |
| Password | Enter the password associated with the user name above. |
| Perform Diagnostics Now | Click this button to generate and send a diagnostic e-mail immediately, instead of based on a time period or CPU usage level. |
| Schedule | |
| Periodic Diagnostics | Use these fields to set the ZyWALL to generate and send diagnostic e-mails at regular intervals.<br>Even if you enable both CPU utilization-based and periodic diagnostics, the ZyWALL only sends one diagnostic e-mail within five minutes (unless you click **Perform Diagnostics Now**). |
| Diagnostics Frequency | Set how often the ZyWALL generates and sends diagnostic files.<br>**Hourly**<br>**Daily**<br>**Weekly**<br>**None**.<br>If you select **Daily** or **Weekly**, specify a time of day for the ZyWALL to generate and send diagnostic e-mails. If you select **Weekly**, then also specify which day of the week. Select **None** to have the ZyWALL not generate and send diagnostic e-mails based on a time period. |
| Day for Diagnostics | Use the drop down list box to select which day of the week to generate and send diagnostic files. |
| Time for Diagnostics | Enter the time of day in 24-hour format (for example 23:00 equals 11:00 pm) to generate and send diagnostic files. |
| Apply | Click **Apply** to save your changes back to the ZyWALL. |
| Reset | Click **Reset** to begin configuring this screen afresh. |

# PART VI
# SMT

# 34

# Introducing the SMT

This chapter explains how to access the System Management Terminal and gives an overview of its menus.

## 34.1 Introduction to the SMT

The ZyWALL's SMT (System Management Terminal) is a menu-driven interface that you can access from a terminal emulator through the console port or over a telnet connection. This chapter shows you how to access the SMT (System Management Terminal) menus via console port, how to navigate the SMT and how to configure SMT menus.

## 34.2 Accessing the SMT via the Console Port

Make sure you have the physical connection properly set up as described in the Quick Start Guide.

When configuring using the console port, you need a computer equipped with communications software configured to the following parameters:

- VT100 terminal emulation.
- 9600 Baud.
- No parity, 8 data bits, 1 stop bit, flow control set to none.

### 34.2.1 Initial Screen

When you turn on your ZyWALL, it performs several internal tests as well as line initialization.

After the tests, the ZyWALL asks you to press [ENTER] to continue, as shown next.

**Figure 359** Initial Screen

```
Copyright (c) 1994 - 2007 ZyXEL Communications Corp.

initialize ch =0, ethernet address: 00:A0:C5:01:23:45
initialize ch =1, ethernet address: 00:A0:C5:01:23:46
initialize ch =2, ethernet address: 00:A0:C5:01:23:47
initialize ch =3, ethernet address: 00:A0:C5:01:23:48
initialize ch =4, ethernet address: 00:00:00:00:00:00
AUX port init . done
Modem init . inactive

Press ENTER to continue...
```

### 34.2.2 Entering the Password

The login screen appears after you press [ENTER], prompting you to enter the password, as shown below.

For your first login, enter the default password "1234". As you type the password, the screen displays an "X" for each character you type.

Please note that if there is no activity for longer than five minutes after you log in, your ZyWALL will automatically log you out and display a blank screen. If you see a blank screen, press [ENTER] to bring up the login screen again.

**Figure 360** Password Screen

```
Enter Password : XXXX
```

## 34.3 Navigating the SMT Interface

The SMT is an interface that you use to configure your ZyWALL.

Several operations that you should be familiar with before you attempt to modify the configuration are listed in the table below.

**Table 207** Main Menu Commands

| OPERATION | KEYSTROKES | DESCRIPTION |
|---|---|---|
| Move down to another menu | [ENTER] | To move forward to a submenu, type in the number of the desired submenu and press [ENTER]. |
| Move up to a previous menu | [ESC] | Press the [ESC] key to move back to the previous menu. |
| Move to a "hidden" menu | Press [SPACE BAR] to change No to Yes then press [ENTER]. | Fields beginning with "Edit" lead to hidden menus and have a default setting of No. Press [SPACE BAR] to change No to Yes, and then press [ENTER] to go to a "hidden" menu. |

**Table 207** Main Menu Commands

| OPERATION | KEYSTROKES | DESCRIPTION |
|---|---|---|
| Move the cursor | [ENTER] or [UP]/ [DOWN] arrow keys | Within a menu, press [ENTER] to move to the next field. You can also use the [UP]/[DOWN] arrow keys to move to the previous and the next field, respectively.<br>When you are at the top of a menu, press the [UP] arrow key to move to the bottom of a menu. |
| Entering information | Fill in, or press [SPACE BAR], then press [ENTER] to select from choices. | You need to fill in two types of fields. The first requires you to type in the appropriate information. The second allows you to cycle through the available choices by pressing [SPACE BAR]. |
| Required fields | <? > | All fields with the symbol <?> must be filled in order be able to save the new configuration. |
| N/A fields | <N/A> | Some of the fields in the SMT will show a <N/A>. This symbol refers to an option that is Not Applicable. |
| Save your configuration | [ENTER] | Save your configuration by pressing [ENTER] at the message “Press ENTER to confirm or ESC to cancel”. Saving the data on the screen will take you, in most cases to the previous menu.<br>Make sure you save your settings in each screen that you configure. |
| Exit the SMT | Type 99, then press [ENTER]. | Type 99 at the main menu prompt and press [ENTER] to exit the SMT interface. |

## 34.3.1 Main Menu

After you enter the password, the SMT displays the **ZyWALL Main Menu**, as shown next. This guide uses the ZyWALL 70 menus as an example. The menus may vary slightly for different ZyWALL models. Not all fields or menus are available on all models.

**Figure 361** Main Menu (Router Mode)

```
            Copyright (c) 1994 - 2007 ZyXEL Communications Corp.

                        ZyWALL 70 Main Menu

            Getting Started                 Advanced Management
              1. General Setup               21. Filter and Firewall Setup
              2. WAN Setup                     22. SNMP Configuration
              3. LAN Setup                     23. System Password
              4. Internet Access Setup         24. System Maintenance
              5. DMZ Setup                     25. IP Routing Policy Setup
              6. Route Setup                   26. Schedule Setup
              7. Wireless Setup
            Advanced Applications
              11. Remote Node Setup
              12. Static Routing Setup
              15. NAT Setup

                                                          99. Exit


                        Enter Menu Selection Number:
```

**Figure 362** Main Menu (Bridge Mode)

```
            Copyright (c) 1994 - 2007 ZyXEL Communications Corp.

                              ZyWALL 70 Main Menu

            Getting Started                Advanced Management
              1. General Setup               21. Filter and Firewall Setup
                                             22. SNMP Configuration
                                             23. System Password
                                             24. System Maintenance

              7. Wireless Setup

                                             99. Exit


                           Enter Menu Selection Number:
```

The following table describes the fields in this menu.

**Table 208** Main Menu Summary

| NO. | MENU TITLE | FUNCTION |
|---|---|---|
| 1 | General Setup | Use this menu to set up device mode, dynamic DNS and administrative information. |
| 2 | WAN Setup | Use this menu to clone a MAC address from a computer on your LAN and configure the backup WAN dial-up connection. |
| 3 | LAN Setup | Use this menu to apply LAN filters, configure LAN DHCP and TCP/IP settings. |
| 4 | Internet Access Setup | Configure your Internet access setup (Internet address, gateway, login, etc.) with this menu. |
| 5 | DMZ Setup | Use this menu to apply DMZ filters, and configure DHCP and TCP/IP settings for the DMZ port. |
| 6 | Route Setup | Use this menu to configure your WAN route assessment, traffic redirect properties and failover parameters. |
| 7 | Wireless Setup | Use this menu to configure wireless security, WLAN DHCP and TCP/IP settings for the wireless LAN interface. |
| 11 | Remote Node Setup | Use this menu to configure detailed remote node settings (your ISP is also a remote node) as well as apply WAN filters. |
| 12 | Static Routing Setup | Configure IP static routes in this menu. |
| 15 | NAT Setup | Use this menu to configure Network Address Translation. |
| 21 | Filter and Firewall Setup | Configure filters and activate/deactivate the firewall. |
| 22 | SNMP Configuration | Use this menu to configure SNMP-related parameters. |
| 23 | System Password | Change your password in this menu (recommended). |
| 24 | System Maintenance | From displaying system status to uploading firmware, this menu provides comprehensive system maintenance. |
| 25 | IP Routing Policy Setup | Configure and display policies for use in IP policy routing. |

**Table 208** Main Menu Summary

| NO. | MENU TITLE | FUNCTION |
|---|---|---|
| 26 | Schedule Setup | Use this menu to schedule outgoing calls. |
| 99 | Exit | Use this menu to exit (necessary for remote configuration). |

## 34.3.2 SMT Menus Overview

The following table gives you an overview of your ZyWALL's various SMT menus.

**Table 209** SMT Menus Overview

| MENUS | SUB MENUS | | |
|---|---|---|---|
| 1 General Setup | 1.1 Configure Dynamic DNS | 1.1.1 DDNS Host Summary | 1.1.1 DDNS Edit Host |
| 2 WAN Setup | 2.1 Advanced WAN Setup | | |
| 3 LAN Setup | 3.1 LAN Port Filter Setup | | |
| | 3.2 TCP/IP and DHCP Ethernet Setup | 3.2.1 IP Alias Setup | |
| 4 Internet Access Setup | | | |
| 5 DMZ Setup | 5.1 DMZ Port Filter Setup | | |
| | 5.2 TCP/IP and DHCP Ethernet Setup | 5.2.1 IP Alias Setup | |
| 6 Route Setup | 6.1 Route Assessment | | |
| | 6.2 Traffic Redirect | | |
| | 6.3 Route Failover | | |
| 7 Wireless Setup | 7.1 Wireless Setup | 7.1.1 WLAN MAC Address Filter | |
| | 7.2 TCP/IP and DHCP Ethernet Setup | 7.2.1 IP Alias Setup | |
| 11 Remote Node Setup | 11.1 Remote Node Profile | 11.1.2 Remote Node Network Layer Options | |
| | | 11.1.4 Remote Node Filter | |
| | 11.2 Remote Node Profile | 11.2.2 Remote Node Network Layer Options | |
| | | 11.2.3 Remote Node Script | |
| | | 11.2.4 Remote Node Filter | |
| | 11.3 Remote Node Profile (Backup ISP) | 11.3.2 Remote Node Network Layer Options | |
| | | 11.3.3 Remote Node Script | |
| | | 11.3.4 Remote Node Filter | |
| 12 Static Routing Setup | 12.1 Edit Static Route Setup | | |
| 15 NAT Setup | 15.1 Address Mapping Sets | 15.1.x Address Mapping Rules | 15.1.x.x Address Mapping Rule |
| | 15.2 NAT Server Sets | 15.2.x NAT Server Setup | 15.2.x.x - NAT Server Configuration |
| | 15.3 Trigger Ports | 15.3.x Trigger Port Setup | |

**Table 209** SMT Menus Overview (continued)

| MENUS | SUB MENUS | | |
|---|---|---|---|
| 21 Filter and Firewall Setup | 21.1 Filter Set Configuration | 21.1.x Filter Rules Summary | 21.1.x.x Generic Filter Rule |
| | | | 21.1.x.x TCP/IP Filter Rule |
| | 21.2 Firewall Setup | | |
| 22 SNMP Configuration | | | |
| 23 System Password | | | |
| 24 System Maintenance | 24.1 System Status | | |
| | 24.2 System Information and Console Port Speed | 24.2.1 System Information | |
| | | 24.2.2 Console Port Speed | |
| | 24.3 Log and Trace | 24.3.1 View Error Log | |
| | | 24.3.2 Syslog Logging | |
| | | 24.3.4 Call-Triggering Packet | |
| | 24.4 Diagnostic | | |
| | 24.5 Backup Configuration | | |
| | 24.6 Restore Configuration | | |
| | 24.7 Upload Firmware | 24.7.1 Upload System Firmware | |
| | | 24.7.2 Upload System Configuration File | |
| | 24.8 Command Interpreter Mode | | |
| | 24.9 Call Control | 24.9.1 Budget Management | |
| | | 24.9.2 Call History | |
| | 24.10 Time and Date Setting | | |
| | 24.11 Remote Management Setup | | |
| 25 IP Routing Policy Summary | 25.1 IP Routing Policy Setup | 25.1.1 IP Routing Policy Setup | |
| 26 Schedule Setup | 26.1 Schedule Set Setup | | |

## 34.4 Changing the System Password

Change the system password by following the steps shown next.

1 Enter 23 in the main menu to open **Menu 23 - System Password** as shown next.

**Figure 363** Menu 23: System Password

```
                    Menu 23 - System Password

            Old Password= ?
            New Password= ?
            Retype to confirm= ?



             Enter here to CONFIRM or ESC to CANCEL:
```

2. Type your existing password and press [ENTER].
3. Type your new system password and press [ENTER].
4. Re-type your new system password for confirmation and press [ENTER].

Note that as you type a password, the screen displays an “x” for each character you type.

## 34.5 Resetting the ZyWALL

See Section 3.3 on page 63 for directions on resetting the ZyWALL.

# 35

# SMT Menu 1 - General Setup

**Menu 1 - General Setup** contains administrative and system-related information.

## 35.1 Introduction to General Setup

**Menu 1 - General Setup** contains administrative and system-related information.

## 35.2 Configuring General Setup

1. Enter 1 in the main menu to open **Menu 1 - General Setup**.
2. The **Menu 1 - General Setup** screen appears, as shown next. Fill in the required fields.

**Figure 364** Menu 1: General Setup (Router Mode)

```
                Menu 1 - General Setup

          System Name=
          Domain Name=

          Device Mode= Router Mode


          Edit Dynamic DNS= No

          Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

**Table 210** Menu 1: General Setup (Router Mode)

| FIELD | DESCRIPTION |
|---|---|
| System Name | Choose a descriptive name for identification purposes. It is recommended you enter your computer's "Computer name" in this field. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted. |
| Domain Name | Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. You can go to menu 24.8 and type "sys domain name" to see the current domain name used by your router.<br>The domain name entered by you is given priority over the ISP assigned domain name. If you want to clear this field just press [SPACE BAR] and then [ENTER]. |

**Table 210** Menu 1: General Setup (Router Mode) (continued)

| FIELD | DESCRIPTION |
|---|---|
| Device Mode | Press [SPACE BAR] and then [ENTER] to select **Router Mode**. |
| Edit Dynamic DNS | Press [SPACE BAR] and then [ENTER] to select **Yes** or **No** (default). Select **Yes** to configure **Menu 1.1: Configure Dynamic DNS** discussed next. |
| When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel. | |

**Figure 365** Menu 1: General Setup (Bridge Mode)

```
                        Menu 1 - General Setup

            System Name=
            Domain Name=

            Device Mode= Bridge Mode

            IP Address= 192.168.1.1
            Network Mask= 255.255.255.0
            Gateway= 0.0.0.0
            First System DNS Server
              IP Address= 0.0.0.0
            Second System DNS Server
              IP Address= 0.0.0.0
            Third System DNS Server
              IP Address= 0.0.0.0

                       Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields not previously discussed (see Table 210 on page 613).

**Table 211** Menu 1: General Setup (Bridge Mode)

| FIELD | DESCRIPTION |
|---|---|
| Device Mode | Press [SPACE BAR] and then [ENTER] to select **Bridge Mode**. |
| IP Address | Enter the IP address of your ZyWALL in dotted decimal notation. |
| Network Mask | Enter the subnet mask of your ZyWALL. |
| Gateway | Enter the gateway IP address. |
| First System DNS Server<br>Second System DNS Server<br>Third System DNS Server | Enter the DNS server's IP address(es) in the **IP Address** field(s) if you have the IP address(es) of the DNS server(s). |

## 35.2.1 Configuring Dynamic DNS

To configure Dynamic DNS, set the ZyWALL to router mode in menu 1 or in the **MAINTENANCE Device Mode** screen and go to **Menu 1 - General Setup** and press [SPACE BAR] to select **Yes** in the **Edit Dynamic DNS** field. Press [ENTER] to display **Menu 1.1 - Configure Dynamic DNS** (shown next).

**Figure 366** Menu 1.1: Configure Dynamic DNS

```
            Menu 1.1 - Configure Dynamic DNS

                Service Provider= WWW.DynDNS.COM
                Active= No
                Username=
                Password= ********
                Edit Host= No


              Press ENTER to Confirm or ESC to Cancel:
```

Follow the instructions in the next table to configure Dynamic DNS parameters.

**Table 212** Menu 1.1: Configure Dynamic DNS

| FIELD | DESCRIPTION |
|---|---|
| Service Provider | This is the name of your Dynamic DNS service provider. |
| Active | Press [SPACE BAR] to select **Yes** and then press [ENTER] to make dynamic DNS active. |
| Username | Enter your user name. |
| Password | Enter the password assigned to you. |
| Edit Host | Press [SPACE BAR] and then [ENTER] to select **Yes** if you want to configure a DDNS host. |
| When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel. | |

### 35.2.1.1 Editing DDNS Host

To configure a DDNS host, follow the procedure below.

1. Configure your ZyWALL as a router in menu 1 or the **MAINTENANCE Device Mode** screen.
2. Enter 1 in the main menu to open **Menu 1 - General Setup**.
3. Press [SPACE BAR] to select **Yes** in the **Edit Dynamic DNS** field. Press [ENTER] to display **Menu 1.1 - Configure Dynamic DNS**.
4. Press [SPACE BAR] and then [ENTER] to select **Yes** in the **Edit Host** field. Press [ENTER] to display **Menu 1.1.1 - DDNS Host Summary**.

**Figure 367** Menu 1.1.1: DDNS Host Summary

```
                Menu 1.1.1 DDNS Host Summary

#                          Summary
--- - ------------------------------------------------------
01    Hostname=ZyWALL,
        Type=Dynamic,WC=Yes,Offline=No,Policy=DDNS Server
      Detect, WAN1, HA=Yes
02    ____________________________________________________
      ____________________________________________________
03    ____________________________________________________
      ____________________________________________________
04    ____________________________________________________
      ____________________________________________________
05    ____________________________________________________
      ____________________________________________________


              Select Command= None          Select Rule= N/A
                    Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this screen.

**Table 213** Menu 1.1.1: DDNS Host Summary

| FIELD | DESCRIPTION |
|---|---|
| # | This is the DDNS host index number. |
| Summary | This displays the details about the DDNS host. |
| Select Command | Press [SPACE BAR] to choose from **None**, **Edit**, **Delete**, **Next Page** or **Previous Page** and then press [ENTER]. You must select a DDNS host in the next field when you choose the **Edit** or **Delete** commands.<br>Select **None** and then press [ENTER] to go to the "Press ENTER to Confirm…" prompt.<br>Use **Edit** to create or edit a rule. Use **Delete** to remove a rule. To edit or delete a DDNS host, first make sure you are on the correct page. When a rule is deleted, subsequent rules do not move up in the page list.<br>Select **Next Page** or **Previous Page** to view the next or previous page of DDNS hosts (respectively). |
| Select Rule | Type the DDNS host index number you wish to edit or delete and then press [ENTER]. |
| When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel. | |

5 Select **Edit** in the **Select Command** field; type the index number of the DDNS host you want to configure in the **Select Rule** field and press [ENTER] to open **Menu 1.1.1 - DDNS Edit Host** (see the next figure).

**Figure 368** Menu 1.1.1: DDNS Edit Host

```
                    Menu 1.1.1 - DDNS Edit Host

          Hostname= ZyWALL
          DDNS Type= DynamicDNS
          Enable Wildcard Option= Yes
          Enable Off Line Option= N/A
          Bind WAN= 1
          HA= Yes
          IP Address Update Policy:
            Let DDNS Server Auto Detect= Yes
            Use User-Defined= N/A
            Use WAN IP Address= N/A


                        Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this screen.

**Table 214** Menu 1.1.1: DDNS Edit Host

| FIELD | DESCRIPTION |
|---|---|
| Host Name | Enter your host name in this field. |
| DDNS Type | Press [SPACE BAR] and then [ENTER] to select **DynamicDNS** if you have the Dynamic DNS service.<br>Select **StaticDNS** if you have the Static DNS service.<br>Select **CustomDNS** if you have the Custom DNS service. |
| Enable Wildcard Option | Your ZyWALL supports DYNDNS Wildcard. Press [SPACE BAR] and then [ENTER] to select **Yes** or **No**. This field is **N/A** when you choose DDNS client as your service provider. |
| Enable Off Line Option | This field is only available when **CustomDNS** is selected in the **DDNS Type** field. Press [SPACE BAR] and then [ENTER] to select **Yes**. When **Yes** is selected, http://www.dyndns.com/ traffic is redirected to a URL that you have previously specified (see www.dyndns.com for details). |
| Bind WAN | Enter the WAN to use for updating the IP address of the domain name. |
| HA | Press [SPACE BAR] and then [ENTER] to select **Yes** to enable the high availability (HA) feature.<br>If the WAN specified in the **Bind WAN** field does not have a connection, the ZyWALL will attempt to use the IP address of another WAN to update the domain name.<br>When the WAN s are in the active/passive operating mode, the ZyWALL will update the domain name with the IP address of whichever WAN has a connection, regardless of the setting in the **Bind WAN** field.<br>Clear this check box and the ZyWALL will not update the domain name with an IP address if the WAN specified in the **Bind WAN** field does not have a connection.<br><br>Note: If you enable high availability, DDNS can also function when the ZyWALL uses the dial backup port. DDNS does not function when the ZyWALL uses traffic redirect.<br><br>Refer to Section  on page 489 for detailed information. |

**Table 214** Menu 1.1.1: DDNS Edit Host (continued)

| FIELD | DESCRIPTION |
|---|---|
| IP Address Update Policy: | You can select **Yes** in either the **Let DDNS Server Auto Detect** field (recommended) or the **Use User-Defined** field, but not both.<br>With the **Let DDNS Server Auto Detect** and **Use User-Defined** fields both set to **No**, the DDNS server automatically updates the IP address of the host name(s) with the ZyWALL's WAN IP address.<br>DDNS does not work with a private IP address. When both fields are set to **No**, the ZyWALL must have a public WAN IP address in order for DDNS to work. |
| Let DDNS Server Auto Detect | Only select this option when there are one or more **NAT** routers between the ZyWALL and the DDNS server. Press [SPACE BAR] to select **Yes** and then press [ENTER] to have the DDNS server automatically detect and use the IP address of the NAT router that has a public IP address.<br>Note: The DDNS server may not be able to detect the proper IP address if there is an HTTP proxy server between the ZyWALL and the DDNS server. |
| Use User-Defined | Press [SPACE BAR] to select **Yes** and then press [ENTER] to update the IP address of the host name(s) to the IP address specified below.<br>Only select **Yes** if the ZyWALL uses or is behind a static public IP address. |
| Use WAN IP Address | Enter the static public IP address if you select **Yes** in the **Use User-Defined** field. |
| When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel. | |

The IP address updates when you reconfigure menu 1 or perform DHCP client renewal.

# 36

# WAN and Dial Backup Setup

This chapter describes how to configure the WAN using menu 2 and dial-backup using menus 2.1 and 11.1.

## 36.1 Introduction to WAN and Dial Backup Setup

This chapter explains how to configure settings for your, a dial backup connection using the SMT menus.

## 36.2 WAN Setup

From the main menu, enter 2 to open menu 2.

**Figure 369** MAC Address Cloning in WAN Setup

```
                Menu 2 - WAN Setup

      WAN 1 MAC Address:
        Assigned By= Factory default
        IP Address= N/A
      WAN 2 MAC Address:
        Assigned By= Factory default
        IP Address= N/A

      Dial-Backup:
        Active= No
        Port Speed= 115200
        AT Command String:
          Init= at&fs0=0
        Edit Advanced Setup= No


    Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this screen.

**Table 215** MAC Address Cloning in WAN Setup

| FIELD | DESCRIPTION |
|---|---|
| (WAN 1/2) MAC Address | |
| Assigned By | Press [SPACE BAR] and then [ENTER] to choose one of two methods to assign a MAC Address. Choose **Factory Default** to select the factory assigned default MAC Address. Choose **IP address attached on LAN** to use the MAC Address of that computer whose IP you give in the following field. |
| IP Address | This field is applicable only if you choose the **IP address attached on LAN** method in the **Assigned By** field. Enter the IP address of the computer on the LAN whose MAC you are cloning. |
| When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel. | |

## 36.3 Dial Backup

The Dial Backup port can be used in reserve, as a traditional dial-up connection should the broadband connection to the WAN port fail. To set up the auxiliary port (Dial Backup) for use in the event that the regular WAN connection is dropped, first make sure you have set up the switch and port connection (see the Quick Start Guide), then configure

1. Menu 2 - WAN Setup,
2. Menu 2.1 - Advanced WAN Setup and

Refer also to the section about traffic redirect for information on an alternate backup WAN connection.

### 36.3.1 Configuring Dial Backup in Menu 2

From the main menu, enter 2 to open menu 2.

**Figure 370** Menu 2: Dial Backup Setup

```
                Menu 2 - WAN Setup

            WAN 1 MAC Address:
              Assigned By= Factory default
              IP Address= N/A
            WAN 2 MAC Address:
              Assigned By= Factory default
              IP Address= N/A

            Dial-Backup:
              Active= No
              Port Speed= 115200
              AT Command String:
                Init= at&fs0=0
              Edit Advanced Setup= Yes


           Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

**Table 216** Menu 2: Dial Backup Setup

| FIELD | DESCRIPTION |
|---|---|
| Dial-Backup: | |
| Active | Use this field to turn the dial-backup feature on (**Yes**) or off (**No**). |
| Port Speed | Press [SPACE BAR] and then press [ENTER] to select the speed of the connection between the Dial Backup port and the external device.<br>Available speeds are:<br>**9600**, **19200**, **38400**, **57600**, **115200** or **230400** bps. |
| AT Command String: | |
| Init | Enter the AT command string to initialize the WAN device. Consult the manual of your WAN device connected to your Dial Backup port for specific AT commands. |
| Edit Advanced Setup | To edit the advanced setup for the Dial Backup port, move the cursor to this field; press the [SPACE BAR] to select **Yes** and then press [ENTER] to go to **Menu 2.1 - Advanced Setup**. |
| When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel. | |

## 36.3.2 Advanced WAN Setup

Consult the manual of your WAN device connected to your Dial Backup port for specific AT commands.

To edit the advanced setup for the Dial Backup port, move the cursor to the **Edit Advanced Setup** field in **Menu 2 - WAN Setup**, press the [SPACE BAR] to select **Yes** and then press [ENTER].

**Figure 371** Menu 2.1: Advanced WAN Setup

```
                        Menu 2.1 - Advanced WAN Setup

          AT Command Strings:                  Call Control:
            Dial= atdt                           Dial Timeout(sec)= 60
            Drop= ~~+++~~ath                     Retry Count= 0
            Answer= ata                          Retry Interval(sec)= N/A
                                                 Drop Timeout(sec)= 20
          Drop DTR When Hang Up= Yes             Call Back Delay(sec)= 15

          AT Response Strings:
            CLID= NMBR =
            Called Id=
            Speed= CONNECT


             Press ENTER to Confirm or ESC to Cancel:
```

The following table describes fields in this menu.

**Table 217** Advanced WAN Port Setup: AT Commands Fields

| FIELD | DESCRIPTION |
|---|---|
| AT Command Strings: | |
| Dial | Enter the AT Command string to make a call. |
| Drop | Enter the AT Command string to drop a call. “~” represents a one second wait, e.g., “~~~+++~~ath” can be used if your modem has a slow response time. |
| Answer | Enter the AT Command string to answer a call. |
| Drop DTR When Hang Up | Press the [SPACE BAR] to choose either **Yes** or **No**. When **Yes** is selected (the default), the DTR (Data Terminal Ready) signal is dropped after the “AT Command String: Drop” is sent out. |
| AT Response Strings: | |
| CLID (Calling Line Identification) | Enter the keyword that precedes the CLID (Calling Line Identification) in the AT response string. This lets the ZyWALL capture the CLID in the AT response string that comes from the WAN device. CLID is required for CLID authentication. |
| Called Id | Enter the keyword preceding the dialed number. |
| Speed | Enter the keyword preceding the connection speed. |

**Table 218** Advanced WAN Port Setup: Call Control Parameters

| FIELD | DESCRIPTION |
|---|---|
| Call Control | |
| Dial Timeout (sec) | Enter a number of seconds for the ZyWALL to keep trying to set up an outgoing call before timing out (stopping). The ZyWALL times out and stops if it cannot set up an outgoing call within the timeout value. |
| Retry Count | Enter a number of times for the ZyWALL to retry a busy or no-answer phone number before blacklisting the number. |
| Retry Interval (sec) | Enter a number of seconds for the ZyWALL to wait before trying another call after a call has failed. This applies before a phone number is blacklisted. |
| Drop Timeout (sec) | Enter a number of seconds for the ZyWALL to wait before dropping the DTR signal if it does not receive a positive disconnect confirmation. |
| Call Back Delay (sec) | Enter a number of seconds for the ZyWALL to wait between dropping a callback request call and dialing the co-responding callback call. |
| When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel. | |

## 36.3.3 Remote Node Profile (Backup ISP)

Enter **3** in **Menu 11 - Remote Node Setup** to open **Menu 11.3 - Remote Node Profile (Backup ISP)** (shown below) and configure the setup for your Dial Backup port connection. Not all fields are available on all models.

**Figure 372** Menu 11.3: Remote Node Profile (Backup ISP)

```
              Menu 11.3 - Remote Node Profile (Backup ISP)

Rem Node Name= Dial
Active= No
                                      Edit IP= No
Outgoing:                             Edit Script Options= No
  My Login= ChangeMe
  My Password= ********               Telco Option:
  Retype to Confirm= ********           Allocated Budget(min)= 0
  Authen= CHAP/PAP                        Period(hr)= 0
  Pri Phone #= 0                        Schedules=
  Sec Phone #=                          Always On= No

                                      Session Options:
                                        Edit Filter Sets= No
                                        Idle Timeout(sec)= 100



                 Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

**Table 219** Menu 11.3: Remote Node Profile (Backup ISP)

| FIELD | DESCRIPTION |
|---|---|
| Rem Node Name | Enter a descriptive name for the remote node. This field can be up to eight characters. |
| Active | Press [SPACE BAR] and then [ENTER] to select **Yes** to enable the remote node or **No** to disable the remote node. |
| Outgoing | |
| My Login | Enter the login name assigned by your ISP for this remote node. |
| My Password | Enter the password assigned by your ISP for this remote node. |
| Retype to Confirm | Enter your password again to make sure that you have entered is correctly. |
| Authen | This field sets the authentication protocol used for outgoing calls.<br>Options for this field are:<br>**CHAP/PAP** - Your ZyWALL will accept either **CHAP** or **PAP** when requested by this remote node.<br>**CHAP** - accept CHAP only.<br>**PAP** - accept PAP only. |
| Pri Phone #<br>Sec Phone # | Enter the first (primary) phone number from the ISP for this remote node. If the Primary Phone number is busy or does not answer, your ZyWALL dials the Secondary Phone number if available. Some areas require dialing the pound sign # before the phone number for local calls. Include a # symbol at the beginning of the phone numbers as required. |
| Edit IP | This field leads to a “hidden” menu. Press [SPACE BAR] to select **Yes** and press [ENTER] to go to **Menu 11.3.2 - Remote Node Network Layer Options**. See Section 36.3.4 on page 625 for more information. |
| Edit Script Options | Press [SPACE BAR] to select **Yes** and press [ENTER] to edit the AT script for the dial backup remote node (**Menu 11.3.3 - Remote Node Script**). See Section 36.3.5 on page 626 for more information. |
| Telco Option | |
| Allocated Budget | Enter the maximum number of minutes that this remote node may be called within the time period configured in the **Period** field. The default for this field is 0 meaning there is no budget control and no time limit for accessing this remote node. |
| Period(hr) | Enter the time period (in hours) for how often the budget should be reset. For example, to allow calls to this remote node for a maximum of 10 minutes every hour, set the **Allocated Budget** to 10 (minutes) and the **Period** to 1 (hour). |
| Schedules | You can apply up to four schedule sets here. For more details please refer to Chapter 53 on page 757. |
| Always On | Press [SPACE BAR] to select **Yes** to set this connection to be on all the time, regardless of whether or not there is any traffic. Select **No** to have this connection act as a dial-up connection. |
| Session Options | |
| Edit Filter sets | This field leads to another “hidden” menu. Use [SPACE BAR] to select **Yes** and press [ENTER] to open menu 11.3.4 to edit the filter sets. See Section 36.3.6 on page 628 for more details. |
| Idle Timeout | Enter the number of seconds of idle time (when there is no traffic from the ZyWALL to the remote node) that can elapse before the ZyWALL automatically disconnects the PPP connection. This option only applies when the ZyWALL initiates the call. |
| Once you have configured this menu, press [ENTER] at the message “Press ENTER to Confirm...” to save your configuration, or press [ESC] at any time to cancel. | |

## 36.3.4 Editing TCP/IP Options

Move the cursor to the **Edit IP** field in menu 11.3, then press [SPACE BAR] to select **Yes**. Press [ENTER] to open **Menu 11.3.2 - Remote Node Network Layer Options**. Not all fields are available on all models.

**Figure 373** Menu 11.3.2: Remote Node Network Layer Options

```
            Menu 11.3.2 - Remote Node Network Layer Options

              IP Address Assignment= Static
              Rem IP Addr= 0.0.0.0
              Rem Subnet Mask= 0.0.0.0
              My WAN Addr= 0.0.0.0

              Network Address Translation= SUA Only
              NAT Lookup Set= 255
              Metric= 15
              Private= No
              RIP Direction= None
                Version= N/A
              Multicast= None

               Enter here to CONFIRM or ESC to CANCEL:
```

The following table describes the fields in this menu.

**Table 220** Menu 11.3.2: Remote Node Network Layer Options

| FIELD | DESCRIPTION |
|---|---|
| IP Address Assignment | If your ISP did not assign you a fixed IP address, press [SPACE BAR] and then [ENTER] to select **Dynamic**, otherwise select **Static** and enter the IP address and subnet mask in the following fields. |
| Rem IP Address | Enter the (fixed) IP address assigned to you by your ISP (static IP address assignment is selected in the previous field). |
| Rem Subnet Mask | Enter the subnet mask associated with your static IP. |
| My WAN Addr | Leave the field set to 0.0.0.0 to have the ISP or other remote router dynamically (automatically) assign your WAN IP address if you do not know it. Enter your WAN IP address here if you know it (static).<br>This is the address assigned to your local ZyWALL, not the remote router. |

**Table 220** Menu 11.3.2: Remote Node Network Layer Options

| FIELD | DESCRIPTION |
|---|---|
| Network Address Translation | Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet).<br>Press [SPACE BAR] and then [ENTER] to select either **Full Feature**, **None** or **SUA Only**.<br>Choose **None** to disable NAT.<br>Choose **SUA Only** if you have a single public IP address. SUA (Single User Account) is a subset of NAT that supports two types of mapping: **Many-to-One** and **Server**.<br>Choose **Full Feature** if you have multiple public IP addresses. **Full Feature** mapping types include: **One-to-One**, **Many-to-One** (SUA/PAT), **Many-to-Many Overload**, **Many- One-to-One** and **Server**. When you select **Full Feature** you must configure at least one address mapping set.<br>See Chapter 22 on page 435 for a full discussion on this feature. |
| NAT Lookup Set | If you select **SUA Only** in the **Network Address Translation** field, it displays **255** and indicates the SMT will use the pre-configured **Set 255** (read only) in menu 15.1.<br>If you select **Full Feature** or **None** in the **Network Address Translation** field, it displays **1**, **2** or **3** and indicates the SMT will use the pre-configured **Set 1** in menu 15.1 for the first WAN port, **Set 2** in menu 15.1 for the second WAN port and **Set 3** for the Backup port.<br>Refer to Section 44.2 on page 675 for more information. |
| Metric | Enter a number from 1 to 15 to set this route's priority among the ZyWALL's routes. The smaller the number, the higher priority the route has. |
| Private | This parameter determines if the ZyWALL will include the route to this remote node in its RIP broadcasts. If set to **Yes**, this route is kept private and not included in RIP broadcasts. If **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts. |
| RIP Direction | Press [SPACE BAR] and then [ENTER] to select the **RIP Direction** from **Both**, **None**, **In Only**, **Out Only** and **None**. |
| Version | Press [SPACE BAR] and then [ENTER] to select the RIP version from **RIP-1**, **RIP-2B** and **RIP-2M**. |
| Multicast | IGMP (Internet Group Management Protocol) is a session-layer protocol used to establish membership in a Multicast group. The ZyWALL supports both IGMP version 1 (**IGMP-v1**) and version 2 (**IGMP-v2**). Press the [SPACE BAR] to enable IP Multicasting or select **None** to disable it. See Section on page 152 for more information on this feature. |
| Once you have completed filling in **Menu 11.3.2 Remote Node Network Layer Options**, press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration and return to menu 11.3, or press [ESC] at any time to cancel. | |

## 36.3.5 Editing Login Script

For some remote gateways, text login is required before PPP negotiation is started. The ZyWALL provides a script facility for this purpose. The script has six programmable sets; each set is composed of an 'Expect' string and a 'Send' string. After matching a message from the server to the 'Expect' field, the ZyWALL returns the set's 'Send' string to the server.

For instance, a typical login sequence starts with the server printing a banner, a login prompt for you to enter the user name and a password prompt to enter the password:

```
Welcome to Acme, Inc.
Login: myLogin
Password:
```

To handle the first prompt, you specify "`ogin: `" as the 'Expect' string and "`myLogin`" as the 'Send' string in set 1. The reason for leaving out the leading "`L`" is to avoid having to know exactly whether it is upper or lower case. Similarly, you specify "`word: `" as the 'Expect' string and your password as the 'Send' string for the second prompt in set 2.

You can use two variables, `$USERNAME` and `$PASSWORD` (all UPPER case), to represent the actual user name and password in the script, so they will not show in the clear. They are replaced with the outgoing login name and password in the remote node when the ZyWALL sees them in a 'Send' string. Please note that both variables must been entered exactly as shown. No other characters may appear before or after, either, i.e., they must be used alone in response to login and password prompts.

Please note that the ordering of the sets is significant, i.e., starting from set 1, the ZyWALL will wait until the 'Expect' string is matched before it proceeds to set 2, and so on for the rest of the script. When both the 'Expect' and the 'Send' fields of the current set are empty, the ZyWALL will terminate the script processing and start PPP negotiation. This implies two things: first, the sets must be contiguous; the sets after an empty one are ignored. Second, the last set should match the final message sent by the server. For instance, if the server prints:

```
login successful.
Starting PPP...
```

after you enter the password, then you should create a third set to match the final "`PPP...`" but without a "Send" string. Otherwise, the ZyWALL will start PPP prematurely right after sending your password to the server.

If there are errors in the script and it gets stuck at a set for longer than the "Dial Timeout" in menu 2 (default 60 seconds), the ZyWALL will timeout and drop the line. To debug a script, go to Menu 24.4 to initiate a manual call and watch the trace display to see if the sequence of messages and prompts from the server differs from what you expect.

**Figure 374** Menu 11.3.3: Remote Node Script

```
                 Menu 11.3.3 - Remote Node Script

                Active= No

                Set 1:                                  Set 5:
                  Expect=                                 Expect=
                  Send=                                   Send=
                Set 2:                                  Set 6:
                  Expect=                                 Expect=
                  Send=                                   Send=
                Set 3:
                  Expect=
                  Send=
                Set 4:
                  Expect=
                  Send=

          Enter here to CONFIRM or ESC to CANCEL:
```

The following table describes the fields in this menu.

**Table 221** Menu 11.3.3: Remote Node Script

| FIELD | DESCRIPTION |
|---|---|
| Active | Press [SPACE BAR] and then [ENTER] to select either **Yes** to enable the AT strings or **No** to disable them. |
| Set 1-6: Expect | Enter an Expect string to match. After matching the Expect string, the ZyWALL returns the string in the **Send** field. |
| Set 1-6: Send | Enter a string to send out after the Expect string is matched. |

## 36.3.6 Remote Node Filter

Move the cursor to the field **Edit Filter Sets** in menu 11.3, and then press [SPACE BAR] to set the value to **Yes**. Press [ENTER] to open **Menu 11.3.4 - Remote Node Filter**.

Use menu 11.3.4 to specify the filter set(s) to apply to the incoming and outgoing traffic between this remote node and the ZyWALL to prevent certain packets from triggering calls. You can specify up to four filter sets separated by commas, for example, 1, 5, 9, 12, in each filter field. Note that spaces are accepted in this field. Please refer to Chapter 46 on page 695 for more information on defining the filters.

**Figure 375** Menu 11.3.4: Remote Node Filter

```
            Menu 11.3.4 - Remote Node Filter

            Input Filter Sets:
              protocol filters=
                device filters=
            Output Filter Sets:
              protocol filters=
                device filters=
            Call Filter Sets:
              protocol filters=
                device filters=


                 Enter here to CONFIRM or ESC to CANCEL:
```

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. See Section 9.4 on page 192 for more information.

To set up a 3G connection, you need to configure

1. Menu 2 - WAN Setup,
2. Menu 11.2 - Remote Node Profile (3G WAN)

### 36.3.7 3G Modem Setup

From the main menu, enter 2 to open menu 2 on the ZyWALL that supports a 3G card.

It is not necessary to configure menu 2 with a Sierra Wireless AC595 3G card.

**Figure 376** 3G Modem Setup in WAN Setup (ZyWALL 5)

```
                          Menu 2 - WAN Setup

                      WAN 1 MAC Address:
                        Assigned By= Factory default
                        IP Address= N/A

                      Dial-Backup:
                        Active= No
                        Port Speed= 115200
                        AT Command String:
                          Init= at&fs0=0
                        Edit Advanced Setup= No

                      3G Modem Setup:
                        Init= Configure APN
                        APN =internet
                        PIN code= 0000

                Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this screen.

**Table 222** 3G Modem Setup in WAN Setup (ZyWALL 5)

| FIELD | DESCRIPTION |
|---|---|
| 3G Modem Setup | |
| Init | Press [SPACE BAR] and then [ENTER] to select **Configure directly** if your ISP provides the initial string or you know how to configure it. Only use this option with a GSM 3G card.<br>Select **Configure APN** if your ISP gave you an APN (Access Point Name) to use. |
| Init | This field displays when you select **Configure directly** in the previous field. Enter the string. It can be up to 72 ASCII printable characters. |
| APN | This field displays when you select **Configure APN** in the **Init** field. Enter the APN (Access Point Name) provided by 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>You can enter up to 31 ASCII printable characters. Spaces are allowed. |

**Table 222** 3G Modem Setup in WAN Setup (ZyWALL 5) (continued)

| FIELD | DESCRIPTION |
|---|---|
| PIN Code | A PIN (Personal Identification Number) code is a key to a 3G card. Without the PIN code, you cannot use the 3G card.<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>If your ISP disabled PIN code authentication, enter an arbitrary number. |
| When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel. | |

## 36.3.8 Remote Node Profile (3G WAN)

enter **2** in **Menu 11 - Remote Node Setup** to open **Menu 11.2 - Remote Node Profile (3G WAN)** (shown below) and configure the setup for your 3G connection.

**Figure 377** Menu 11.2: Remote Node Profile (3G WAN)

```
                Menu 11.2 - Remote Node Profile (3G WAN)

Rem Node Name= WAN 2
Active= Yes
                                        Edit IP= No
Outgoing:                               Edit Script Options= No
  My Login= test
  My Password= ********
  Retype to Confirm= ********
  Authen= CHAP/PAP
  Pri Phone #= *99#
                                          Always On= No

                                        Session Options:
                                          Edit Filter Sets= No
                                          Idle Timeout(sec)= 100



                Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

**Table 223** Menu 11.2: Remote Node Profile (3G WAN)

| FIELD | DESCRIPTION |
|---|---|
| Rem Node Name | Enter a descriptive name for the remote node. This field can be up to eight characters. |
| Active | Press [SPACE BAR] and then [ENTER] to select **Yes** to enable the remote node or **No** to disable the remote node. |
| Outgoing | |
| My Login | Enter the login name assigned by your ISP for this remote node. |
| My Password | Enter the password assigned by your ISP for this remote node. |

**Table 223** Menu 11.2: Remote Node Profile (3G WAN) (continued)

| FIELD | DESCRIPTION |
|---|---|
| Retype to Confirm | Enter your password again to make sure that you have entered is correctly. |
| Authen | This field sets the authentication protocol used for outgoing calls.<br>Options for this field are:<br>**CHAP/PAP** - Your ZyWALL will accept either **CHAP** or **PAP** when requested by this remote node.<br>**CHAP** - accept CHAP only.<br>**PAP** - accept PAP only. |
| Pri Phone # | Enter the phone number (dial string) used to dial up a connection to your service provider's base station. Your ISP should provide the phone number.<br>For example, *99# is the dial string to establish a GPRS or 3G connection in Taiwan. |
| Edit IP | This field leads to a "hidden" menu. Press [SPACE BAR] to select **Yes** and press [ENTER] to go to **Menu 11.3.2 - Remote Node Network Layer Options**. See Section 36.3.4 on page 625 for more information. |
| Edit Script Options | Press [SPACE BAR] to select **Yes** and press [ENTER] to edit the AT script for the dial backup remote node (**Menu 11.3.3 - Remote Node Script**). See Section 36.3.5 on page 626 for more information. |
| Always On | Press [SPACE BAR] to select **Yes** to set this connection to be on all the time, regardless of whether or not there is any traffic. Select **No** to have this connection act as a dial-up connection. |
| Session Options | |
| Edit Filter sets | This field leads to another "hidden" menu. Use [SPACE BAR] to select **Yes** and press [ENTER] to open menu 11.3.4 to edit the filter sets. See Section 36.3.6 on page 628 for more details. |
| Idle Timeout | Enter the number of seconds of idle time (when there is no traffic from the ZyWALL to the remote node) that can elapse before the ZyWALL automatically disconnects the 3G connection. |
| Once you have configured this menu, press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel. | |

# 37

# LAN Setup

This chapter describes how to configure the LAN using **Menu 3 - LAN Setup**.

## 37.1 Introduction to LAN Setup

This chapter describes how to configure the ZyWALL for LAN and wireless LAN connections.

## 37.2 Accessing the LAN Menus

From the main menu, enter 3 to open **Menu 3 - LAN Setup**.

**Figure 378** Menu 3: LAN Setup

```
                        Menu 3 - LAN Setup

                1. LAN Port Filter Setup
                2. TCP/IP and DHCP Setup




                     Enter Menu Selection Number:
```

## 37.3 LAN Port Filter Setup

This menu allows you to specify the filter sets that you wish to apply to the LAN traffic. You seldom need to filter the LAN traffic, however, the filter sets may be useful to block certain packets, reduce traffic and prevent security breaches.

**Figure 379** Menu 3.1: LAN Port Filter Setup

```
            Menu 3.1 - LAN Port Filter Setup

            Input Filter Sets:
              protocol filters=
                device filters=
            Output Filter Sets:
              protocol filters=
                device filters=

            Press ENTER to Confirm or ESC to Cancel:
```

## 37.4 TCP/IP and DHCP Ethernet Setup Menu

From the main menu, enter 3 to open **Menu 3 - LAN Setup** to configure TCP/IP (RFC 1155) and DHCP Ethernet setup.

**Figure 380** Menu 3: TCP/IP and DHCP Setup

```
                Menu 3 - LAN Setup

            1. LAN Port Filter Setup
            2. TCP/IP and DHCP Setup



                     Enter Menu Selection Number:
```

From menu 3, select the submenu option **TCP/IP and DHCP Setup** and press [ENTER]. The screen now displays **Menu 3.2 - TCP/IP and DHCP Ethernet Setup**, as shown next. Not all fields are available on all models.

**Figure 381** Menu 3.2: TCP/IP and DHCP Ethernet Setup

```
          Menu 3.2 - TCP/IP and DHCP Ethernet Setup


     DHCP= Server                       TCP/IP Setup:
     Client IP Pool:
       Starting Address= 192.168.1.33   IP Address= 192.168.1.1
       Size of Client IP Pool= 128      IP Subnet Mask= 255.255.255.0
                                        RIP Direction= Both
                                          Version= RIP-1
                                        Multicast= None
                                        Edit IP Alias= No


     DHCP Server Address= N/A


                       Press ENTER to Confirm or ESC to Cancel:
```

Follow the instructions in the next table on how to configure the DHCP fields.

**Table 224** Menu 3.2: DHCP Ethernet Setup Fields

| FIELD | DESCRIPTION |
|---|---|
| DHCP | This field enables/disables the DHCP server.<br>If set to **Server**, your ZyWALL will act as a DHCP server.<br>If set to **None**, the DHCP server will be disabled.<br>If set to **Relay**, the ZyWALL acts as a surrogate DHCP server and relays requests and responses between the remote server and the clients.<br>When set to **Server**, the following items need to be set: |
| Client IP Pool: | |
| Starting Address | This field specifies the first of the contiguous addresses in the IP address pool. |
| Size of Client IP Pool | This field specifies the size, or count of the IP address pool. |
| DHCP Server Address | If **Relay** is selected in the **DHCP** field above, then type the IP address of the actual, remote DHCP server here. |

Use the instructions in the following table to configure TCP/IP parameters for the LAN port.

LAN and DMZ IP addresses must be on separate subnets.

**Table 225** Menu 3.2: LAN TCP/IP Setup Fields

| FIELD | DESCRIPTION |
|---|---|
| TCP/IP Setup: | |
| IP Address | Enter the IP address of your ZyWALL in dotted decimal notation |

**Table 225** Menu 3.2: LAN TCP/IP Setup Fields (continued)

| FIELD | DESCRIPTION |
|---|---|
| IP Subnet Mask | Your ZyWALL will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyWALL. |
| RIP Direction | Press [SPACE BAR] and then [ENTER] to select the RIP direction. Options are: **Both**, **In Only**, **Out Only** or **None**. |
| Version | Press [SPACE BAR] and then [ENTER] to select the RIP version. Options are: **RIP-1**, **RIP-2B** or **RIP-2M**. |
| Multicast | IGMP (Internet Group Management Protocol) is a session-layer protocol used to establish membership in a Multicast group. The ZyWALL supports both IGMP version 1 (**IGMP-v1**) and version 2 (**IGMP-v2**). Press [SPACE BAR] and then [ENTER] to enable IP Multicasting or select **None** (default) to disable it. |
| Edit IP Alias | The ZyWALL supports three logical LAN interfaces via its single physical Ethernet interface with the ZyWALL itself as the gateway for each LAN network. Press [SPACE BAR] to select **Yes** and then press [ENTER] to display menu 3.2.1 |
| When you have completed this menu, press [ENTER] at the prompt [Press ENTER to Confirm…] to save your configuration, or press [ESC] at any time to cancel. | |

## 37.4.1 IP Alias Setup

IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The ZyWALL supports three logical LAN interfaces via its single physical Ethernet interface with the ZyWALL itself as the gateway for each LAN network.

Use menu 3.2 to configure the first network. Move the cursor to the **Edit IP Alias** field, press [SPACE BAR] to choose **Yes** and press [ENTER] to open **Menu 3.2.1 - IP Alias Setup**, as shown next. Use this menu to configure the second and third networks.

**Figure 382** Menu 3.2.1: IP Alias Setup

```
                Menu 3.2.1 - IP Alias Setup

          IP Alias 1= Yes
            IP Address= 192.168.2.1
            IP Subnet Mask= 255.255.255.0
            RIP Direction= None
              Version= RIP-1
            Incoming protocol filters=
            Outgoing protocol filters=
          IP Alias 2= No
            IP Address= N/A
            IP Subnet Mask= N/A
            RIP Direction= N/A
              Version= N/A
            Incoming protocol filters= N/A
            Outgoing protocol filters= N/A


                     Enter here to CONFIRM or ESC to CANCEL:
```

Use the instructions in the following table to configure IP alias parameters.

**Table 226** Menu 3.2.1: IP Alias Setup

| FIELD | DESCRIPTION |
|---|---|
| IP Alias 1, 2 | Choose **Yes** to configure the LAN network for the ZyWALL. |
| IP Address | Enter the IP address of your ZyWALL in dotted decimal notation. |
| IP Subnet Mask | Your ZyWALL will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyWALL. |
| RIP Direction | Press [SPACE BAR] and then [ENTER] to select the RIP direction. Options are **Both**, **In Only**, **Out Only** or **None**. |
| Version | Press [SPACE BAR] and then [ENTER] to select the RIP version. Options are **RIP-1**, **RIP-2B** or **RIP-2M**. |
| Incoming Protocol Filters | Enter the filter set(s) you wish to apply to the incoming traffic between this node and the ZyWALL. |
| Outgoing Protocol Filters | Enter the filter set(s) you wish to apply to the outgoing traffic between this node and the ZyWALL. |
| When you have completed this menu, press [ENTER] at the prompt [Press ENTER to Confirm…] to save your configuration, or press [ESC] at any time to cancel. | |

# 38

# Internet Access

This chapter shows you how to configure your ZyWALL for Internet access.

## 38.1 Introduction to Internet Access Setup

Use information from your ISP along with the instructions in this chapter to set up your ZyWALL to access the Internet. There are three different menu 4 screens depending on whether you chose **Ethernet**, **PPTP** or **PPPoE** Encapsulation. Contact your ISP to determine what encapsulation type you should use.

This menu configures **WAN 1** on a ZyWALL with multiple WAN ports. Configure the WAN 2 port in **Menu 11.2 - Remote Node Profile** or in the **WAN > WAN 2** screen via the web configurator.

## 38.2 Ethernet Encapsulation

If you choose **Ethernet** in menu 4 you will see the next menu.

**Figure 383** Menu 4: Internet Access Setup (Ethernet)

```
                    Menu 4 - Internet Access Setup

                ISP's Name= WAN_1
                Encapsulation= Ethernet
                  Service Type= Standard
                  My Login= N/A
                  My Password= N/A
                  Retype to Confirm= N/A
                  Login Server= N/A
                  Relogin Every (min)=  N/A
                IP Address Assignment= Dynamic
                  IP Address= N/A
                  IP Subnet Mask= N/A
                  Gateway IP Address= N/A
                Network Address Translation= SUA Only

                Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

**Table 227** Menu 4: Internet Access Setup (Ethernet)

| FIELD | DESCRIPTION |
|---|---|
| ISP's Name | This is the descriptive name of your ISP for identification purposes. |
| Encapsulation | Press [SPACE BAR] and then press [ENTER] to choose **Ethernet**. The encapsulation method influences your choices for the **IP Address** field. |
| Service Type | Press [SPACE BAR] and then [ENTER] to select **Standard**, **RR-Toshiba** (RoadRunner Toshiba authentication method), **RR-Manager** (RoadRunner Manager authentication method), **RR-Telstra** or **Telia Login**. Choose a RoadRunner flavor if your ISP is Time Warner's RoadRunner; otherwise choose **Standard**. |
| Note: DSL users must choose the **Standard** option only. The **My Login**, **My Password** and **Login Server** fields are not applicable in this case. | |
| My Login | Enter the login name given to you by your ISP. |
| My Password | Type your password again for confirmation. |
| Retype to Confirm | Enter your password again to make sure that you have entered is correctly. |
| Login Server | The ZyWALL will find the RoadRunner Server IP if this field is left blank. If it does not, then you must enter the authentication server IP address. |
| Relogin Every (min) | This field is available when you select **Telia Login** in the **Service Type** field.<br>The Telia server logs the ZyWALL out if the ZyWALL does not log in periodically. Type the number of minutes from 1 to 59 (30 recommended) for the ZyWALL to wait between logins. |
| IP Address Assignment | If your ISP did not assign you a fixed IP address, press [SPACE BAR] and then [ENTER] to select **Dynamic**, otherwise select **Static** and enter the IP address and subnet mask in the following fields. |
| IP Address | Enter the (fixed) IP address assigned to you by your ISP (static IP address assignment is selected in the previous field). |
| IP Subnet Mask | Enter the subnet mask associated with your static IP. |

**Table 227** Menu 4: Internet Access Setup (Ethernet) (continued)

| FIELD | DESCRIPTION |
|---|---|
| Gateway IP Address | Enter the gateway IP address associated with your static IP. |
| Network Address Translation | Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet).<br>Choose **None** to disable NAT.<br>Choose **SUA Only** if you have a single public IP address. SUA (Single User Account) is a subset of NAT that supports two types of mapping: **Many-to-One** and **Server**.<br>Choose **Full Feature** if you have multiple public IP addresses. **Full Feature** mapping types include: **One-to-One**, **Many-to-One** (SUA/PAT), **Many-to-Many Overload**, **Many- One-to-One** and **Server**. When you select **Full Feature** you must configure at least one address mapping set!<br>Please see Chapter 22 on page 435 for a more detailed discussion on the Network Address Translation feature. |
| When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel. | |

## 38.3 Configuring the PPTP Client

The ZyWALL supports only one PPTP server connection at any given time.

To configure a PPTP client, you must configure the **My Login** and **Password** fields for a PPP connection and the PPTP parameters for a PPTP connection.

After configuring **My Login** and **Password** for PPP connection, press [SPACE BAR] and then [ENTER] in the **Encapsulation** field in **Menu 4 -Internet Access Setup** to choose **PPTP** as your encapsulation option. This brings up the following screen.

**Figure 384** Internet Access Setup (PPTP)

```
                    Menu 4 - Internet Access Setup

                ISP's Name= WAN_1
                Encapsulation= PPTP
                  Service Type= N/A
                  My Login=
                  My Password= ********
                  Retype to Confirm= ********
                  Idle Timeout= 100

                IP Address Assignment= Dynamic
                  IP Address= N/A
                  IP Subnet Mask= N/A
                  Gateway IP Address= N/A
                Network Address Translation= SUA Only

                Press ENTER to Confirm or ESC to Cancel:
```

The following table contains instructions about the new fields when you choose **PPTP** in the **Encapsulation** field in menu 4.

**Table 228** New Fields in Menu 4 (PPTP) Screen

| FIELD | DESCRIPTION |
|---|---|
| Encapsulation | Press [SPACE BAR] and then press [ENTER] to choose **PPTP**. The encapsulation method influences your choices for the **IP Address** field. |
| Idle Timeout | This value specifies the time, in seconds, that elapses before the ZyWALL automatically disconnects from the PPTP server. |

## 38.4 Configuring the PPPoE Client

If you enable PPPoE in menu 4, you will see the next screen.

**Figure 385** Internet Access Setup (PPPoE)

```
                    Menu 4 - Internet Access Setup

               ISP's Name= WAN_1
               Encapsulation= PPPoE
                 Service Type= N/A
                 My Login=
                 My Password= ********
                 Retype to Confirm= ********
                 Idle Timeout= 100

               IP Address Assignment= Dynamic
                 IP Address= N/A
                 IP Subnet Mask= N/A
                 Gateway IP Address= N/A
               Network Address Translation= SUA Only

               Press ENTER to Confirm or ESC to Cancel:
```

The following table contains instructions about the new fields when you choose **PPPoE** in the **Encapsulation** field in menu 4.

**Table 229** New Fields in Menu 4 (PPPoE) screen

| FIELD | DESCRIPTION |
|---|---|
| Encapsulation | Press [SPACE BAR] and then press [ENTER] to choose **PPPoE**. The encapsulation method influences your choices in the **IP Address** field. |
| Idle Timeout | This value specifies the time in seconds that elapses before the ZyWALL automatically disconnects from the PPPoE server. |

If you need a PPPoE service name to identify and reach the PPPoE server, please go to menu 11 and enter the PPPoE service name provided to you in the **Service Name** field.

## 38.5 Basic Setup Complete

Well done! You have successfully connected, installed and set up your ZyWALL to operate on your network as well as access the Internet.

When the firewall is activated, the default policy allows all communications to the Internet that originate from the LAN, and blocks all traffic to the LAN that originates from the Internet.

You may deactivate the firewall in menu 21.2 or via the ZyWALL embedded web configurator. You may also define additional firewall rules or modify existing ones but please exercise extreme caution in doing so. See the chapters on firewall for more information on the firewall.

# 39

# DMZ Setup

This chapter describes how to configure the ZyWALL's DMZ using **Menu 5 - DMZ Setup**.

## 39.1 Configuring DMZ Setup

From the main menu, enter 5 to open **Menu 5 – DMZ Setup**.

**Figure 386** Menu 5: DMZ Setup

```
Menu 5 - DMZ Setup

1. DMZ Port Filter Setup
2. TCP/IP and DHCP Setup

Enter Menu Selection Number:
```

## 39.2 DMZ Port Filter Setup

This menu allows you to specify the filter sets that you wish to apply to your public server(s) traffic.

**Figure 387** Menu 5.1: DMZ Port Filter Setup

```
Menu 5.1 - DMZ Port Filter Setup

Input Filter Sets:
  protocol filters=
    device filters=
Output Filter Sets:
  protocol filters=
    device filters=

Press ENTER to Confirm or ESC to Cancel:
```

## 39.3 TCP/IP Setup

For more detailed information about RIP setup, IP Multicast and IP alias, please refer to Chapter 7 on page 149.

### 39.3.1 IP Address

From the main menu, enter 5 to open **Menu 5 - DMZ Setup** to configure TCP/IP (RFC 1155).

**Figure 388** Menu 5: DMZ Setup

```
            Menu 5 - DMZ Setup

            1. DMZ Port Filter Setup
            2. TCP/IP and DHCP Setup

                    Enter Menu Selection Number:
```

From menu 5, select the submenu option **2. TCP/IP and DHCP Setup** and press [ENTER]. The screen now displays **Menu 5.2 - TCP/IP and DHCP Ethernet Setup**, as shown next.

**Figure 389** Menu 5.2: TCP/IP and DHCP Ethernet Setup

```
                    Menu 5.2 - TCP/IP and DHCP Ethernet Setup


      DHCP= None                                TCP/IP Setup:
      Client IP Pool:
        Starting Address= N/A                   IP Address= 10.10.2.1
        Size of Client IP Pool= N/A            IP Subnet Mask= 255.255.255.0
                                                RIP Direction= None
                                                  Version= N/A
                                                Multicast= IGMP-v2
                                                Edit IP Alias= No


      DHCP Server Address= N/A


                    Press ENTER to Confirm or ESC to Cancel:
```

The DHCP and TCP/IP setup fields are the same as the ones in **Menu 3.2 - TCP/IP and DHCP Ethernet Setup**. Each public server will need a unique IP address. Refer to Section 37.4 on page 634 for information on how to configure these fields.

DMZ, WLAN and LAN IP addresses must be on separate subnets. You must also configure NAT for the DMZ port (see Chapter 44 on page 673) in menus 15.1 and 15.2.

## 39.3.2 IP Alias Setup

Use menu 5.2 to configure the first network. Move the cursor to the **Edit IP Alias** field, press [SPACE BAR] to choose **Yes** and press [ENTER] to open **Menu 5.2.1 - IP Alias Setup**, as shown next. Use this menu to configure the second and third networks.

**Figure 390** Menu 5.2.1: IP Alias Setup

```
            Menu 5.2.1 - IP Alias Setup

            IP Alias 1= No
              IP Address= N/A
              IP Subnet Mask= N/A
              RIP Direction= N/A
                Version= N/A
              Incoming protocol filters= N/A
              Outgoing protocol filters= N/A
            IP Alias 2= No
              IP Address= N/A
              IP Subnet Mask= N/A
              RIP Direction= N/A
                Version= N/A
              Incoming protocol filters= N/A
              Outgoing protocol filters= N/A

            Enter here to CONFIRM or ESC to CANCEL:
```

Refer to Table 226 on page 637 for instructions on configuring IP alias parameters.

# 40

# Route Setup

This chapter describes how to configure the ZyWALL's traffic redirect.

## 40.1 Configuring Route Setup

From the main menu, enter 6 to open **Menu 6 - Route Setup**.

**Figure 391** Menu 6: Route Setup

```
Menu 6 - Route Setup

1. Route Assessment
2. Traffic Redirect
3. Route Failover


        Enter Menu Selection Number:
```

## 40.2 Route Assessment

This menu allows you to configure traffic redirect properties.

**Figure 392** Menu 6.1: Route Assessment

```
Menu 6.1 - Route Assessment


Probing WAN 1 Check Point= Yes
  Use Default Gateway as Check Point= Yes
  Check Point= N/A
Probing WAN 2 Check Point= Yes
  Use Default Gateway as Check Point= Yes
  Check Point= N/A
Probing Traffic Redirection Check Point= No
  Use Default Gateway as Check Point= N/A
  Check Point= N/A


Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

**Table 230** Menu 6.1: Route Assessment

| FIELD | DESCRIPTION |
|---|---|
| Probing WAN 1/2 Check Point | Press [SPACE BAR] and then press [ENTER] to choose **Yes** to test your ZyWALL's WAN accessibility.<br>If you do not select **No** in the **Use Default Gateway as Check Point** field and enter a domain name or IP address of a reliable nearby computer (for example, your ISP's DNS server address) in the **Check Point** field, the ZyWALL will use the default gateway IP address. |
| Probing Traffic Redirection Check Point | Press [SPACE BAR] and then press [ENTER] to choose **Yes** to test your ZyWALL's traffic redirect connection.<br>If you do not select **No** in the **Use Default Gateway as Check Point** field and enter a domain name or IP address of a reliable nearby computer (for example, your ISP's DNS server address) in the **Check Point** field, the ZyWALL will use the default gateway IP address. |
| When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel. | |

## 40.3 Traffic Redirect

To configure the parameters for traffic redirect, enter **2** in **Menu 6 - Route Setup** to open **Menu 6.2 - Traffic Redirect** as shown next.

**Figure 393** Menu 6.2: Traffic Redirect

```
              Menu 6.2 - Traffic Redirect

            Active= No
            Configuration:
              Backup Gateway IP Address= 0.0.0.0
              Metric= 14



            Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

**Table 231** Menu 6.2: Traffic Redirect

| FIELD | DESCRIPTION |
|---|---|
| Active | Press [SPACE BAR] and select Yes (to enable) or No (to disable) traffic redirect setup. The default is No. |
| Backup Gateway IP Address | Enter the IP address of your backup gateway in dotted decimal notation.<br>The ZyWALL automatically forwards traffic to this IP address if the ZyWALL's Internet connection terminates. |
| Metric | This field sets this route's priority among the routes the ZyWALL uses.<br>Enter a number from 1 to 15 to set this route's priority among the ZyWALL's routes (see Section  on page 171) The smaller the number, the higher priority the route has. |
| When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel. | |

# 40.4 Route Failover

This menu allows you to configure how the ZyWALL uses the route assessment ping check function.

**Figure 394** Menu 6.3: Route Failover

```
            Menu 6.3 - Route Failover

            Period= 5
            Timeout=: 3
            Fail Tolerance= 3


            Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

**Table 232** Menu 6.3: Route Failover

| FIELD | DESCRIPTION |
|---|---|
| Period | Type the number of seconds for the ZyWALL to wait between checks to see if it can connect to the WAN IP address (in the **Check Point** field of menu 6.1) or the default gateway. Allow more time if your destination IP address handles lots of traffic. |
| Timeout | Type the number of seconds for your ZyWALL to wait for a ping response from the IP address in the **Check Point** field of menu 6.1 before it times out. The WAN connection is considered "down" after the ZyWALL times out the number of times specified in the **Fail Tolerance** field. Use a higher value in this field if your network is busy or congested. |
| Fail Tolerance | Type the number of times your ZyWALL may attempt and fail to connect to the Internet before traffic is forwarded to the backup gateway. |
| When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel. | |

# 41

# Wireless Setup

Use menu 7 to set up your ZyWALL as the wireless access point.

## 41.1 Wireless LAN Setup

If you are configuring the ZyWALL from a computer connected to the wireless LAN and you change the ZyWALL's ESSID or WEP settings, you will lose your wireless connection when you press [ENTER] to confirm. You must then change the wireless settings of your computer to match the ZyWALL's new settings.

From the main menu, enter 7 to open **Menu 7 - WLAN Setup** to configure the Wireless LAN setup. To edit the wireless LAN configuration, enter 1 to open **Menu 7.1 - Wireless Setup** as shown next.

**Figure 395** Menu 7.1: Wireless Setup

```
            Menu 7.1 - Wireless Setup

            Enable Wireless LAN= No
            Bridge Channel= WLAN
            ESSID= ZyXEL
            Hide ESSID= No
            Channel ID= CH06 2437MHz
            RTS Threshold= 2432
            Frag. Threshold= 2432
            WEP= Disable
              Default Key= N/A
              Key1= N/A
              Key2= N/A
              Key3= N/A
              Key4= N/A
            Edit MAC Address Filter= No

            Press ENTER to Confirm or ESC to Cancel:
```

The settings of all client stations on the wireless LAN must match those of the ZyWALL.

Follow the instructions in the next table on how to configure the wireless LAN parameters.

**Table 233** Menu 7.1: Wireless Setup

| FIELD | DESCRIPTION |
|---|---|
| Enable Wireless LAN | Press [SPACE BAR] to select **Yes** to turn on the wireless LAN. The wireless LAN is off by default. Configure wireless LAN security features such as Mac filters and 802.1X before you turn on the wireless LAN. |
| Bridge Channel | Select **LAN** to use the wireless card as part of the LAN.<br>Select **DMZ** to use the wireless card as part of the DMZ.<br>Select **WLAN** to use the wireless card as part of the WLAN.<br>The ZyWALL restarts after you change the wireless card setting.<br><br>Note: If you set the wireless card to be part of the LAN or DMZ, you can still use wireless access, but not the WLAN interface in the firewall. The firewall will treat the wireless card as part of the LAN or DMZ respectively. |
| ESSID | (Extended Service Set IDentification) The ESSID identifies the AP to which the wireless stations associate. Wireless stations associating to the Access Point must have the same ESSID. Enter a descriptive name (up to 32 characters) for the wireless LAN. |
| Hide ESSID | Press [SPACE BAR] to select **Yes** to hide the ESSID in the outgoing beacon frame so a station cannot obtain the ESSID through passive scanning. |
| Channel ID | This allows you to set the operating frequency/channel depending on your particular region. Use the [SPACE BAR] to select a channel. |
| RTS Threshold | Use RTS/CTS 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>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. |
| Frag. Threshold | The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. |
| WEP | Select **Disable** to allow wireless stations to communicate with the access points without any data encryption.<br>Select **64-bit WEP** or **128-bit WEP** to enable data encryption. |
| Default Key | Enter the key number (1 to 4) in this field. Only one key can be enabled at any one time. This key must be the same on the ZyWALL and the wireless stations to communicate. |

**Table 233** Menu 7.1: Wireless Setup

| FIELD | DESCRIPTION |
|---|---|
| Key 1 to Key 4 | The WEP keys are used to encrypt data. Both the ZyWALL and the wireless stations must use the same WEP key for data transmission.<br>If you chose **64-bit WEP** in the **WEP Encryption** field, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F").<br>If you chose **128-bit WEP** in the **WEP Encryption** field, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").<br><br>Note: Enter "0x" before the key to denote a hexadecimal key. Don't enter "0x" before the key to denote an ASCII key. |
| Edit MAC Address Filter | Press [SPACE BAR] to select **Yes** and then press [ENTER] to display menu 7.1.1. |
| When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel. | |

## 41.1.1 MAC Address Filter Setup

Your ZyWALL checks the MAC address of the wireless station device against a list of allowed or denied MAC addresses. However, intruders could fake allowed MAC addresses so MAC-based authentication is less secure than EAP authentication.

Follow the steps below to create the MAC address table on your ZyWALL.

1. From the main menu, enter 7 to open **Menu 7 - WLAN Setup**.
2. Enter 1 to display **Menu 7.1 - Wireless Setup**.
3. In the **Edit MAC Address Filter** field, press [SPACE BAR] to select **Yes** and press [ENTER]. **Menu 7.1.1 - WLAN MAC Address Filter** displays as shown next.

**Figure 396** Menu 7.1.1: WLAN MAC Address Filter

```
            Menu 7.1.1 - WLAN MAC Address Filter

            Active= No
            Filter Action= Allowed Association
            MAC Address Filter
              Address  1= 00:00:00:00:00:00
              Address  2= 00:00:00:00:00:00
              Address  3= 00:00:00:00:00:00
              Address  4= 00:00:00:00:00:00
              Address  5= 00:00:00:00:00:00
              Address  6= 00:00:00:00:00:00
              Address  7= 00:00:00:00:00:00
              Address  8= 00:00:00:00:00:00
              Address  9= 00:00:00:00:00:00
              Address 10= 00:00:00:00:00:00
              Address 11= 00:00:00:00:00:00
              Address 12= 00:00:00:00:00:00

            Enter here to CONFIRM or ESC to CANCEL:
```

The following table describes the fields in this menu.

**Table 234** Menu 7.1.1: WLAN MAC Address Filter

| FIELD | DESCRIPTION |
|---|---|
| Active | To enable MAC address filtering, press [SPACE BAR] to select **Yes** and press [ENTER]. |
| Filter Action | Define the filter action for the list of MAC addresses in the MAC address filter table.<br>To deny access to the ZyWALL, press [SPACE BAR] to select **Deny Association** and press [ENTER]. MAC addresses not listed will be allowed to access the router.<br><br>The default action, **Allowed Association**, permits association with the ZyWALL. MAC addresses not listed will be denied access to the router. |
| MAC Address Filter | |
| Address 1..12 | Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the client computers that are allowed or denied access to the ZyWALL in these address fields. |
| When you have completed this menu, press [ENTER] at the prompt [Press ENTER to Confirm…] to save your configuration, or press [ESC] at any time to cancel. | |

## 41.2 TCP/IP Setup

For more detailed information about RIP setup, IP Multicast and IP alias, please refer to Chapter 7 on page 149.

### 41.2.1 IP Address

From the main menu, enter 7 to open **Menu 7 - WLAN Setup** to configure TCP/IP (RFC 1155).

**Figure 397** Menu 7: WLAN Setup

```
                Menu 7 - WLAN Setup

            1. Wireless Setup
            2. TCP/IP and DHCP Setup

             Enter Menu Selection Number:
```

From menu 7, select the submenu option **2. TCP/IP and DHCP Setup** and press [ENTER]. The screen now displays **Menu 7.2 - TCP/IP and DHCP Ethernet Setup**, as shown next.

**Figure 398** Menu 7.2: TCP/IP and DHCP Ethernet Setup

```
                Menu 7.2 - TCP/IP and DHCP Ethernet Setup


       DHCP= None                              TCP/IP Setup:
       Client IP Pool:
         Starting Address= N/A                 IP Address= 0.0.0.0
         Size of Client IP Pool= N/A           IP Subnet Mask= 0.0.0.0
                                               RIP Direction= None
                                                 Version= N/A
                                               Multicast= IGMP-v2
                                               Edit IP Alias= No


       DHCP Server Address= N/A



                      Press ENTER to Confirm or ESC to Cancel:
```

The DHCP and TCP/IP setup fields are the same as the ones in **Menu 3.2 - TCP/IP and DHCP Ethernet Setup**. Each public server will need a unique IP address. Refer to Section 37.4 on page 634 for information on how to configure these fields.

DMZ, WLAN and LAN IP addresses must be on separate subnets. You must also configure NAT for the WLAN port (see Chapter 44 on page 673) in menus 15.1 and 15.2.

## 41.2.2 IP Alias Setup

You must use menu 7.2 to configure the first network. Move the cursor to the **Edit IP Alias** field, press [SPACE BAR] to choose **Yes** and press [ENTER] to configure the second and third network.

Pressing [ENTER] opens **Menu 7.2.1 - IP Alias Setup**, as shown next.

**Figure 399** Menu 7.2.1: IP Alias Setup

```
                Menu 7.2.1 - IP Alias Setup

                   IP Alias 1= No
                     IP Address= N/A
                     IP Subnet Mask= N/A
                     RIP Direction= N/A
                       Version= N/A


                   IP Alias 2= No
                     IP Address= N/A
                     IP Subnet Mask= N/A
                     RIP Direction= N/A
                       Version= N/A


            Enter here to CONFIRM or ESC to CANCEL:
```

Refer to Table 226 on page 637 for instructions on configuring IP alias parameters.

# 42

# Remote Node Setup

This chapter shows you how to configure a remote node.

## 42.1 Introduction to Remote Node Setup

A remote node is required for placing calls to a remote gateway. A remote node represents both the remote gateway and the network behind it across a WAN connection. Note that when you use menu 4 to set up Internet access, you are actually configuring a remote node. The following describes how to configure **Menu 11.x (where x is 1 or 2) - Remote Node Profile**, **Menu 11.x.2 - Remote Node Network Layer Options** and **Menu 11.x.4 - Remote Node Filter**.

## 42.2 Remote Node Setup

From the main menu, select menu option 11 to open **Menu 11 - Remote Node Setup** (shown below).

On a ZyWALL with multiple WAN ports, enter **1** or **2** to open **Menu 11.x - Remote Node Profile** and configure the setup for your first or second WAN port. Enter **3** to open **Menu 11.3 Remote Node Profile (Backup ISP)** and configure the setup for your Dial Backup port connection (see Chapter 36 on page 619).

On a ZyWALL with a single WAN port and a 3G card, enter **1** to open **Menu 11.1 - Remote Node Profile** and configure the setup for your WAN port. Enter **2** to open **Menu 11.2 - Remote Node Profile (3G WAN)** and configure the setup for your 3G connection. Enter **3** to open **Menu 11.3 Remote Node Profile (Backup ISP)** and configure the setup for your Dial Backup port connection.

**Figure 400** Menu 11: Remote Node Setup

```
            Menu 11 - Remote Node Setup

            1. WAN_1 (ISP, SUA)
            2. WAN_2 (ISP, NAT)
            3. -Dial (BACKUP_ISP, SUA)



            Enter Node # to Edit:
```

# 42.3 Remote Node Profile Setup

The following explains how to configure the remote node profile menu. Not all fields are available on all models.

## 42.3.1 Ethernet Encapsulation

There are three variations of menu 11.x depending on whether you choose **Ethernet Encapsulation**, **PPPoE Encapsulation** or **PPTP Encapsulation**. You must choose the **Ethernet** option when the WAN port is used as a regular Ethernet. The first menu 11.x screen you see is for Ethernet encapsulation shown next.

**Figure 401** Menu 11.1: Remote Node Profile for Ethernet Encapsulation

```
                Menu 11.1 - Remote Node Profile

          Rem Node Name= WAN 1                 Route= IP
          Active= Yes

          Encapsulation= Ethernet              Edit IP= No
          Service Type= Standard               Session Options:
                                                 Schedules=
          Outgoing:                              Edit Filter Sets= No
            My Login= N/A
            My Password= N/A
            Retype to Confirm= N/A
            Server= N/A
            Relogin Every (min)=  N/A


          Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

**Table 235** Menu 11.1: Remote Node Profile for Ethernet Encapsulation

| FIELD | DESCRIPTION |
|---|---|
| Rem Node Name | Enter a descriptive name for the remote node. This field can be up to eight characters. |
| Active | Press [SPACE BAR] and then [ENTER] to select **Yes** (activate remote node) or **No** (deactivate remote node). |
| Encapsulation | **Ethernet** is the default encapsulation. Press [SPACE BAR] and then [ENTER] to change to **PPPoE** or **PPTP** encapsulation. |
| Service Type | Press [SPACE BAR] and then [ENTER] to select from **Standard**, **RR-Toshiba** (RoadRunner Toshiba authentication method), **RR-Manager** (RoadRunner Manager authentication method), **RR-Telstra** or **Telia Login**. Choose one of the RoadRunner methods if your ISP is Time Warner's RoadRunner; otherwise choose **Standard**. |
| Outgoing | |
| My Login | This field is applicable for **PPPoE** encapsulation only. Enter the login name assigned by your ISP when the ZyWALL calls this remote node. Some ISPs append this field to the **Service Name** field above (e.g., jim@poellc) to access the PPPoE server. |

**Table 235** Menu 11.1: Remote Node Profile for Ethernet Encapsulation (continued)

| FIELD | DESCRIPTION |
|---|---|
| My Password | Enter the password assigned by your ISP when the ZyWALL calls this remote node. Valid for **PPPoE** encapsulation only. |
| Retype to Confirm | Type your password again to make sure that you have entered it correctly. |
| Server | This field is valid only when **RoadRunner** is selected in the **Service Type** field. The ZyWALL will find the RoadRunner Server IP automatically if this field is left blank. If it does not, then you must enter the authentication server IP address here. |
| Relogin Every (min) | This field is available when you select **Telia Login** in the **Service Type** field.<br>The Telia server logs the ZyWALL out if the ZyWALL does not log in periodically. Type the number of minutes from 1 to 59 (30 recommended) for the ZyWALL to wait between logins. |
| Route | This field refers to the protocol that will be routed by your ZyWALL – IP is the only option for the ZyWALL. |
| Edit IP | This field leads to a “hidden” menu. Press [SPACE BAR] to select **Yes** and press [ENTER] to go to **Menu 11.x.2 - Remote Node Network Layer Options**. |
| Session Options | |
| Schedules | You can apply up to four schedule sets here. For more details please refer to Chapter 53 on page 757. |
| Edit Filter Sets | This field leads to another “hidden” menu. Use [SPACE BAR] to select **Yes** and press [ENTER] to open menu 11.x.4 to edit the filter sets. See Section 42.5 on page 666 for more details. |
| Once you have configured this menu, press [ENTER] at the message “Press ENTER to Confirm...” to save your configuration, or press [ESC] at any time to cancel. | |

## 42.3.2 PPPoE Encapsulation

The ZyWALL supports PPPoE (Point-to-Point Protocol over Ethernet). You can only use PPPoE encapsulation when you’re using the ZyWALL with a DSL modem as the WAN device. If you change the Encapsulation to **PPPoE,** then you will see the next screen.

**Figure 402** Menu 11.1: Remote Node Profile for PPPoE Encapsulation

```
                Menu 11.1 - Remote Node Profile

     Rem Node Name= WAN 1                  Route= IP
     Active= Yes

     Encapsulation= PPPoE                  Edit IP= No
     Service Type= Standard                Telco Option:
     Service Name=                           Allocated Budget(min)= 0
     Outgoing:                               Period(hr)= 0
       My Login=                             Schedules=
       My Password= ********                 Nailed-Up Connection= No
       Retype to Confirm= ********
       Authen= CHAP/PAP

                                             Session Options:
                                             Edit Filter Sets= No
                                             Idle Timeout(sec)= 100


                        Press ENTER to Confirm or ESC to Cancel:
```

#### 42.3.2.1 Outgoing Authentication Protocol

Generally speaking, you should employ the strongest authentication protocol possible, for obvious reasons. However, some vendor's implementation includes a specific authentication protocol in the user profile. It will disconnect if the negotiated protocol is different from that in the user profile, even when the negotiated protocol is stronger than specified. If you encounter a case where the peer disconnects right after a successful authentication, please make sure that you specify the correct authentication protocol when connecting to such an implementation.

#### 42.3.2.2 Nailed-Up Connection

A nailed-up connection is a dial-up line where the connection is always up regardless of traffic demand. The ZyWALL does two things when you specify a nailed-up connection. The first is that idle timeout is disabled. The second is that the ZyWALL will try to bring up the connection when turned on and whenever the connection is down. A nailed-up connection can be very expensive for obvious reasons.

Do not specify a nailed-up connection unless your telephone company offers flat-rate service or you need a constant connection and the cost is of no concern.

The following table describes the fields not already described in Table 235 on page 660.

#### 42.3.2.3 Metric

See Section  on page 171 for details on the **Metric** field.

**Table 236** Fields in Menu 11.1 (PPPoE Encapsulation Specific)

| FIELD | DESCRIPTION |
|---|---|
| Service Name | If you are using **PPPoE** encapsulation, then type the name of your PPPoE service here. Only valid with **PPPoE** encapsulation. |
| Authen | This field sets the authentication protocol used for outgoing calls.<br>Options for this field are:<br>**CHAP**/**PAP** - Your ZyWALL will accept either **CHAP** or **PAP** when requested by this remote node.<br>**CHAP** - accept CHAP only.<br>**PAP** - accept PAP only. |
| Telco Option | |
| Allocated Budget | The field sets a ceiling for outgoing call time for this remote node. The default for this field is 0 meaning no budget control. |
| Period(hr) | This field is the time period that the budget should be reset. For example, if we are allowed to call this remote node for a maximum of 10 minutes every hour, then the **Allocated Budget** is (10 minutes) and the **Period(hr)** is 1 (hour). |
| Schedules | You can apply up to four schedule sets here. For more details please refer to Chapter 53 on page 757. |
| Nailed-Up Connection | This field specifies if you want to make the connection to this remote node a nailed-up connection. More details are given earlier in this section. |
| Session Options | |
| Idle Timeout | Type the length of idle time (when there is no traffic from the ZyWALL to the remote node) in seconds that can elapse before the ZyWALL automatically disconnects the PPPoE connection. This option only applies when the ZyWALL initiates the call. |

### 42.3.3 PPTP Encapsulation

If you change the Encapsulation to **PPTP** in menu 11.1, then you will see the next screen.

**Figure 403** Menu 11.1: Remote Node Profile for PPTP Encapsulation

```
                Menu 11.1 - Remote Node Profile

     Rem Node Name= WAN 1                  Route= IP
     Active= Yes

     Encapsulation= PPTP                   Edit IP= No
     Service Type= Standard                Telco Option:
                                             Allocated Budget(min)= 0
     Outgoing:                               Period(hr)= 0
       My Login=                             Schedules=
       My Password= ********                 Nailed-Up Connection= No
       Retype to Confirm= ********
       Authen= CHAP/PAP
     PPTP:                                 Session Options:
       My IP Addr= 10.0.0.140                Edit Filter Sets= No
       My IP Mask= 255.255.255.0             Idle Timeout(sec)= 100
       Server IP Addr= 10.0.0.138
       Connection ID/Name=

                         Press ENTER to Confirm or ESC to Cancel:
```

The next table shows how to configure fields in menu 11.1 not previously discussed.

**Table 237** Menu 11.1: Remote Node Profile for PPTP Encapsulation

| FIELD | DESCRIPTION |
|---|---|
| Encapsulation | Press [SPACE BAR] and then [ENTER] to select **PPTP**. You must also go to menu 11.3 to check the IP Address setting once you have selected the encapsulation method. |
| My IP Addr | Enter the IP address of the WAN Ethernet port. |
| My IP Mask | Enter the subnet mask of the WAN Ethernet port. |
| Server IP Addr | Enter the IP address of the ANT modem. |
| Connection ID/ Name | Enter the connection ID or connection name in the ANT. It must follow the “c:id” and “n:name” format.<br>This field is optional and depends on the requirements of your DSL modem. |
| Schedules | You can apply up to four schedule sets here. For more details refer to Chapter 53 on page 757. |
| Nailed-Up Connections | Press [SPACE BAR] and then [ENTER] to select **Yes** if you want to make the connection to this remote node a nailed-up connection. |

## 42.4 Edit IP

Move the cursor to the **Edit IP** field in menu 11.1, then press [SPACE BAR] to select **Yes**. Press [ENTER] to open **Menu 11.1.2 - Remote Node Network Layer Options**. Not all fields are available on all models.

**Figure 404** Menu 11.1.2: Remote Node Network Layer Options for Ethernet Encapsulation

```
            Menu 11.1.2 - Remote Node Network Layer Options

              IP Address Assignment= Dynamic
              Rem IP Addr= N/A
              Rem Subnet Mask= N/A
              My WAN Addr= N/A

              Network Address Translation= SUA Only
              NAT Lookup Set= 255
              Metric= 1
              Private= No
              RIP Direction= None
                Version= N/A
              Multicast= None

               Enter here to CONFIRM or ESC to CANCEL:
```

This menu displays the **My WAN Addr** field for **PPPoE** and **PPTP** encapsulations and **Gateway IP Addr** field for **Ethernet** encapsulation. The following table describes the fields in this menu.

**Table 238** Remote Node Network Layer Options Menu Fields

| FIELD | DESCRIPTION |
|---|---|
| IP Address Assignment | If your ISP did not assign you an explicit IP address, press [SPACE BAR] and then [ENTER] to select **Dynamic**; otherwise select **Static** and enter the IP address & subnet mask in the following fields. |
| (Rem) IP Address | If you have a static IP Assignment, enter the IP address assigned to you by your ISP. |
| (Rem) IP Subnet Mask | If you have a static IP Assignment, enter the subnet mask assigned to you. |
| Gateway IP Addr | This field is applicable to **Ethernet** encapsulation only. Enter the gateway IP address assigned to you if you are using a static IP address. |
| My WAN Addr | This field is applicable to **PPPoE** and **PPTP** encapsulations only. Some implementations, especially the UNIX derivatives, require the WAN link to have a separate IP network number from the LAN and each end must have a unique address within the WAN network number. If this is the case, enter the IP address assigned to the WAN port of your ZyWALL.<br>Note that this is the address assigned to your local ZyWALL, not the remote router. |
| Network Address Translation | Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet).<br>Choose **None** to disable NAT.<br>Choose **SUA Only** if you have a single public IP address. SUA (Single User Account) is a subset of NAT that supports two types of mapping: **Many-to-One** and **Server**.<br>Choose **Full Feature** if you have multiple public IP addresses. **Full Feature** mapping types include: **One-to-One**, **Many-to-One** (SUA/PAT), **Many-to-Many Overload**, **Many- One-to-One** and **Server**. When you select **Full Feature** you must configure at least one address mapping set.<br>See Chapter 22 on page 435 for a full discussion on this feature. |

**Table 238** Remote Node Network Layer Options Menu Fields (continued)

| FIELD | DESCRIPTION |
|---|---|
| NAT Lookup Set | If you select **SUA Only** in the **Network Address Translation** field, it displays **255** and indicates the SMT will use the pre-configured **Set 255** (read only) in menu 15.1.<br>If you select **Full Feature** or **None** in the **Network Address Translation** field, it displays **1**, **2** or **3** and indicates the SMT will use the pre-configured **Set 1** in menu 15.1 for the first WAN port, **Set 2** in menu 15.1 for the second WAN port and **Set 3** for the Backup port.<br>Refer to Section 44.2 on page 675 for more information. |
| Metric | Enter a number from 1 to 15 to set this route's priority among the ZyWALL's routes (see Section on page 171). The smaller the number, the higher priority the route has. |
| Private | This field is valid only for PPTP/PPPoE encapsulation. This parameter determines if the ZyWALL will include the route to this remote node in its RIP broadcasts. If set to **Yes**, this route is kept private and not included in RIP broadcast. If **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts. |
| RIP Direction | Press [SPACE BAR] and then [ENTER] to select the RIP direction from **Both**/ **None**/**In Only**/**Out Only**. See Chapter 7 on page 149 for more information on RIP. The default for RIP on the WAN side is **None**. It is recommended that you do not change this setting. |
| Version | Press [SPACE BAR] and then [ENTER] to select the RIP version from **RIP-1**/**RIP-2B**/ **RIP-2M** or **None**. |
| Multicast | IGMP (Internet Group Management Protocol) is a network-layer protocol used to establish membership in a Multicast group. The ZyWALL supports both IGMP version 1 (**IGMP-v1**) and version 2 (**IGMP-v2**). Press [SPACE BAR] to enable IP Multicasting or select **None** to disable it. See Chapter 7 on page 149 for more information on this feature. |
| Once you have completed filling in **Menu 11.3 Remote Node Network Layer Options**, press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration and return to menu 11, or press [ESC] at any time to cancel. | |

## 42.5 Remote Node Filter

Move the cursor to the field **Edit Filter Sets** in menu 11.1, and then press [SPACE BAR] to set the value to **Yes**. Press [ENTER] to open **Menu 11.1.4 - Remote Node Filter**.

Use menu 11.1.4 to specify the filter set(s) to apply to the incoming and outgoing traffic between this remote node and the ZyWALL to prevent certain packets from triggering calls. You can specify up to 4 filter sets separated by commas, for example, 1, 5, 9, 12, in each filter field. Note that spaces are accepted in this field. For more information on defining the filters, please refer to Chapter 46 on page 695. For PPPoE or PPTP encapsulation, you have the additional option of specifying remote node call filter sets.

**Figure 405** Menu 11.1.4: Remote Node Filter (Ethernet Encapsulation)

```
            Menu 11.1.4 - Remote Node Filter

            Input Filter Sets:
              protocol filters=
                device filters=
            Output Filter Sets:
              protocol filters=
                device filters=

            Enter here to CONFIRM or ESC to CANCEL:
```

**Figure 406** Menu 11.1.4: Remote Node Filter (PPPoE or PPTP Encapsulation)

```
            Menu 11.1.4 - Remote Node Filter

            Input Filter Sets:
              protocol filters=
                device filters=
            Output Filter Sets:
              protocol filters=
                device filters=
            Call Filter Sets:
              protocol filters=
                device filters=


            Enter here to CONFIRM or ESC to CANCEL:
```

# 43

# IP Static Route Setup

This chapter shows you how to configure static routes with your ZyWALL.

## 43.1 IP Static Route Setup

Enter 12 from the main menu. Select one of the IP static routes as shown next to configure IP static routes in menu 12.1.

The first two static route entries are for default WAN1 and WAN2 routes on a ZyWALL with multiple WAN interfaces. You cannot modify or delete a static default route.
The default route is disabled after you change the static WAN IP address to a dynamic WAN IP address.

The “-” before a route name indicates the static route is inactive.

**Figure 407** Menu 12: IP Static Route Setup

```
                Menu 12 - IP Static Route Setup


  1. Reserved     16. ________     31. ________     46. ________
  2. Reserved     17. ________     32. ________     47. ________
  3. ________     18. ________     33. ________     48. ________
  4. ________     19. ________     34. ________     49. ________
  5. ________     20. ________     35. ________     50. ________
  6. ________     21. ________     36. ________
  7. ________     22. ________     37. ________
  8. ________     23. ________     38. ________
  9. ________     24. ________     39. ________
 10. ________     25. ________     40. ________
 11. ________     26. ________     41. ________
 12. ________     27. ________     42. ________
 13. ________     28. ________     43. ________
 14. ________     29. ________     44. ________
 15. ________     30. ________     45. ________

  Enter selection number:
```

Now, enter the index number of the static route that you want to configure.

**Figure 408** Menu 12. 1: Edit IP Static Route

```
          Menu 12.1 - Edit IP Static Route

          Route #: 3
          Route Name= ?
          Active= No
          Destination IP Address= ?
          IP Subnet Mask= ?
          Gateway IP Address= ?
          Metric= 2
          Private= No


          Press ENTER to CONFIRM or ESC to CANCEL:
```

`The following table describes the IP Static Route Menu fields.

**Table 239** Menu 12. 1: Edit IP Static Route

| FIELD | DESCRIPTION |
|---|---|
| Route # | This is the index number of the static route that you chose in menu 12. |
| Route Name | Enter a descriptive name for this route. This is for identification purposes only. |
| Active | This field allows you to activate/deactivate this static route. |

**Table 239** Menu 12. 1: Edit IP Static Route

| FIELD | DESCRIPTION |
|---|---|
| Destination IP Address | 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. |
| IP Subnet Mask | Enter the IP subnet mask for this destination. |
| Gateway IP Address | Enter the IP address of the gateway. The gateway is an immediate neighbor of your ZyWALL that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your ZyWALL; over the WAN, the gateway must be the IP address of one of the remote nodes. |
| Metric | Enter a number from 1 to 15 to set this route's priority among the ZyWALL's routes (see Section  on page 171). The smaller the number, the higher priority the route has. |
| Private | This parameter determines if the ZyWALL will include the route to this remote node in its RIP broadcasts. If set to **Yes**, this route is kept private and not included in RIP broadcast. If **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts. |
| Once you have completed filling in this menu, press [ENTER] at the message "Press ENTER to Confirm…" to save your configuration, or press [ESC] to cancel. | |

# 44

# Network Address Translation (NAT)

This chapter discusses how to configure NAT on the ZyWALL.

## 44.1 Using NAT

You must create a firewall rule in addition to setting up SUA/NAT, to allow traffic from the WAN to be forwarded through the ZyWALL.

### 44.1.1 SUA (Single User Account) Versus NAT

SUA (Single User Account) is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. See Section 44.2.1 on page 676 for a detailed description of the NAT set for SUA. The ZyWALL also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types.

Choose **SUA Only** if you have just one public WAN IP address for your ZyWALL.
Choose **Full Feature** if you have multiple public WAN IP addresses for your ZyWALL.

### 44.1.2 Applying NAT

You apply NAT via menu 4 or 11.1.2 as displayed next. The next figure shows you how to apply NAT for Internet access in menu 4. Enter 4 from the main menu to go to **Menu 4 - Internet Access Setup**.

**Figure 409** Menu 4: Applying NAT for Internet Access

```
            Menu 4 - Internet Access Setup

            ISP's Name= ChangeMe
            Encapsulation= Ethernet
              Service Type= Standard
              My Login= N/A
              My Password= N/A
              Retype to Confirm= N/A
              Login Server= N/A
              Relogin Every (min)=  N/A
            IP Address Assignment= Dynamic
              IP Address= N/A
              IP Subnet Mask= N/A
              Gateway IP Address= N/A
            Network Address Translation= SUA Only


            Press ENTER to Confirm or ESC to Cancel:
```

The following figure shows how you apply NAT to the remote node in menu 11.1.

1. Enter 11 from the main menu.
2. Enter 1 to open **Menu 11.1 - Remote Node Profile**.
3. Move the cursor to the **Edit IP** field, press [SPACE BAR] to select **Yes** and then press [ENTER] to bring up **Menu 11.1.2 - Remote Node Network Layer Options**.

**Figure 410** Menu 11.1.2: Applying NAT to the Remote Node

```
            Menu 11.1.2 - Remote Node Network Layer Options

            IP Address Assignment= Dynamic
            IP Address= N/A
            IP Subnet Mask= N/A
            Gateway IP Addr= N/A

            Network Address Translation= Full Feature
            NAT Lookup Set= 1
            Metric= 1
            Private= N/A
            RIP Direction= None
              Version= N/A
            Multicast= None


            Enter here to CONFIRM or ESC to CANCEL:
```

The following table describes the fields in this menu.

**Table 240** Applying NAT in Menus 4 & 11.1.2

| FIELD | DESCRIPTION | OPTIONS |
|---|---|---|
| Network Address Translation | When you select this option the SMT will use Address Mapping Set 1 (menu 15.1 - see Section 44.2.1 on page 676 for further discussion). You can configure any of the mapping types described in Chapter 22 on page 435. Choose **Full Feature** if you have multiple public WAN IP addresses for your ZyWALL.<br>When you select **Full Feature** you must configure at least one address mapping set. | Full Feature |
| | NAT is disabled when you select this option. | None |
| | When you select this option the SMT will use Address Mapping Set 255 (menu 15.1 - see Section 44.2.1 on page 676). Choose **SUA Only** if you have just one public WAN IP address for your ZyWALL. | SUA Only |

## 44.2 NAT Setup

Use the address mapping sets menus and submenus to create the mapping table used to assign global addresses to computers on the LAN, DMZ and WLAN. **Set 255** is used for SUA. When you select **Full Feature** in menu 4, menu 11.1.2 or menu 11.2.2, the SMT will use **Set 1** for the first WAN port and **Set 2** for the second WAN port. When you select **SUA Only**, the SMT will use the pre-configured **Set 255** (read only).

The server set is a list of LAN, DMZ and WLAN servers mapped to external ports. To use this set, a server rule must be set up inside the NAT address mapping set. Please see the section on port forwarding in Chapter 22 on page 435 for further information on these menus. To configure NAT, enter 15 from the main menu to bring up the following screen.

On a ZyWALL with two WAN interfaces, you can configure port forwarding and trigger port rules for the first WAN interface and separate sets of rules for the second WAN interface.

**Figure 411** Menu 15: NAT Setup

```
                Menu 15 - NAT Setup

                    1. Address Mapping Sets
                    2. Port Forwarding Setup
                    3. Trigger Port Setup



          Enter Menu Selection Number:
```

Configure DMZ, WLAN and LAN IP addresses in NAT menus 15.1 and 15.2. DMZ, WLAN and LAN IP addresses must be on separate subnets.

## 44.2.1 Address Mapping Sets

Enter 1 to bring up **Menu 15.1 - Address Mapping Sets**.

**Figure 412** Menu 15.1: Address Mapping Sets

```
            Menu 15.1 - Address Mapping Sets

                    1. NAT_SET
                    2. example
                  255. SUA (read only)




            Enter Menu Selection Number:
```

### 44.2.1.1 SUA Address Mapping Set

Enter 255 to display the next screen (see also Section 44.1.1 on page 673). The fields in this menu cannot be changed.

**Figure 413** Menu 15.1.255: SUA Address Mapping Rules

```
          Menu 15.1.255 - Address Mapping Rules

Set Name= SUA

Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
---  ---------------  ---------------  ---------------  ---------------  ---
1.   0.0.0.0          255.255.255.255  0.0.0.0                           M-1
2.                                    0.0.0.0                          Server
3.
4.
5.
6.
7.
8.
9.
10.

       Press ENTER to Confirm or ESC to Cancel:
```

The following table explains the fields in this menu.

Menu 15.1.255 is read-only.

**Table 241** SUA Address Mapping Rules

| FIELD | DESCRIPTION |
|---|---|
| Set Name | This is the name of the set you selected in menu 15.1 or enter the name of a new set you want to create. |
| Idx | This is the index or rule number. |
| Local Start IP | **Local Start IP** is the starting local IP address (ILA). |
| Local End IP | **Local End IP** is the ending local IP address (ILA). If the rule is for all local IPs, then the start IP is 0.0.0.0 and the end IP is 255.255.255.255. |
| Global Start IP | This is the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the **Global Start IP**. |
| Global End IP | This is the ending global IP address (IGA). |
| Type | These are the mapping types discussed above. **Server** allows us to specify multiple servers of different types behind NAT to this machine. See later for some examples. |
| Once you have finished configuring a rule in this menu, press [ENTER] at the message “Press ENTER to Confirm…” to save your configuration, or press [ESC] to cancel. | |

#### 44.2.1.2 User-Defined Address Mapping Sets

Now look at option 1 in menu 15.1. Enter 1 to bring up this menu. Look at the differences from the previous menu. Note the extra **Action** and **Select Rule** fields mean you can configure rules in this screen. Note also that the [?] in the **Set Name** field means that this is a required field and you must enter a name for the set.

The entire set will be deleted if you leave the **Set Name** field blank and press [ENTER] at the bottom of the screen.

**Figure 414** Menu 15.1.1: First Set

```
                    Menu 15.1.1 - Address Mapping Rules

 Set Name= NAT_SET

Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
---  ---------------  ---------------  ---------------  ---------------  --
 1.  0.0.0.0          255.255.255.255  0.0.0.0                          M-1
 2.                                    0.0.0.0                         Server
 3.
 4.
 5.
 6.
 7.
 8.
 9.
10.

                   Action= None          Select Rule= N/A

                   Press ENTER to Confirm or ESC to Cancel:
```

The Type, Local and Global Start/End IPs are configured in menu 15.1.1.1 (described later) and the values are displayed here.

#### 44.2.1.3 Ordering Your Rules

Ordering your rules is important because the ZyWALL applies the rules in the order that you specify. When a rule matches the current packet, the ZyWALL takes the corresponding action and the remaining rules are ignored. If there are any empty rules before your new configured rule, your configured rule will be pushed up by that number of empty rules. For example, if you have already configured rules 1 to 6 in your current set and now you configure rule number 9. In the set summary screen, the new rule will be rule 7, not 9.

Now if you delete rule 4, rules 5 to 7 will be pushed up by 1 rule, so as old rule 5 becomes rule 4, old rule 6 becomes rule 5 and old rule 7 becomes rule 6.

**Table 242** Fields in Menu 15.1.1

| FIELD | DESCRIPTION |
|---|---|
| Set Name | Enter a name for this set of rules. This is a required field. If this field is left blank, the entire set will be deleted. |
| Action | Press [SPACE BAR] to choose from **None**, **Edit**, **Insert Before**, **Delete**, **Go To Rule**, **Next Page** or **Previous Page** and then press [ENTER]. You must select a rule in the next field when you choose the **Edit**, **Insert Before**, **Delete** or **Go To Rule** commands.<br>**None** disables the **Select Rule** item.<br>Use **Edit** to create or edit a rule.<br>Use **Insert Before** to insert a rule before the rule selected.<br>Use **Delete** to delete the selected rule and then all the rules after the selected one will be advanced one rule.<br>Use **Go To Rule** to view the page where your desired rule is listed.<br>Select **Next Page** or **Previous Page** to view the next or previous page of rules (respectively). |
| Select Rule | When you choose **Edit**, **Insert Before** or **Delete** in the previous field the cursor jumps to this field to allow you to select the rule to apply the action in question. |

You must press [ENTER] at the bottom of the screen to save the whole set. You must do this again if you make any changes to the set – including deleting a rule. No changes to the set take place until this action is taken.

Selecting **Edit** in the **Action** field and then selecting a rule brings up the following menu, **Menu 15.1.1.1 - Address Mapping Rule** in which you can edit an individual rule and configure the **Type**, **Local** and **Global Start/End IPs**.

An IP End address must be numerically greater than its corresponding IP Start address.

**Figure 415** Menu 15.1.1.1: Editing/Configuring an Individual Rule in a Set

```
            Menu 15.1.1.1 Address Mapping Rule

                 Type= One-to-One

                 Local IP:
                   Start=
                   End  = N/A

                 Global IP:
                   Start=
                   End  = N/A

                 Server Mapping Set= N/A


            Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

**Table 243** Menu 15.1.1.1: Editing/Configuring an Individual Rule in a Set

| FIELD | DESCRIPTION |
|---|---|
| Type | Press [SPACE BAR] and then [ENTER] to select from a total of five types. These are the mapping types discussed in Chapter 22 on page 435. **Server** allows you to specify multiple servers of different types behind NAT to this computer. See Section 44.4.3 on page 685 for an example. |
| Local IP | Only local IP fields are **N/A** for server; Global IP fields MUST be set for **Server**. |
| Start | Enter the starting local IP address (ILA). |
| End | Enter the ending local IP address (ILA). If the rule is for all local IPs, then put the Start IP as 0.0.0.0 and the End IP as 255.255.255.255. This field is **N/A** for One-to-One and Server types. |
| Global IP | |
| Start | Enter the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the **Global IP Start**. Note that **Global IP Start** can be set to 0.0.0.0 only if the types are **Many-to-One** or **Server**. |
| End | Enter the ending global IP address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server types**. |
| Server Mapping Set | This field is available only when you select **Server** in the **Type** field. |
| Once you have finished configuring a rule in this menu, press [ENTER] at the message “Press ENTER to Confirm…” to save your configuration, or press [ESC] to cancel. | |

## 44.3 Configuring a Server behind NAT

If you do not assign a **Default Server** IP address, the ZyWALL discards all packets received for ports that are not specified here or in the remote management setup.

Follow these steps to configure a server behind NAT:

1. Enter 15 in the main menu to go to **Menu 15 - NAT Setup.**
2. Enter 2 to open menu 15.2.

**Figure 416** Menu 15.2: NAT Server Sets

```
                Menu 15.2 - NAT Server Sets

            1. Server Set 1
            2. Server Set 2


                  Enter Set Number to Edit:
```

3. Enter 1 or 2 to go to **Menu 15.2.x - NAT Server Setup** and configure the address mapping rules for the WAN 1 or WAN 2 interface on a ZyWALL with multiple WAN interfaces.

**Figure 417** Menu 15.2.x: NAT Server Sets

```
              Menu 15.2.1 - NAT Server Setup

            Default Server: 0.0.0.0
 Rule  Act.   Start Port   End Port    IP Address
-------------------------------------------------------
 001   No     0            0           0.0.0.0
 002   No     0            0           0.0.0.0
 003   No     0            0           0.0.0.0
 004   No     0            0           0.0.0.0
 005   No     0            0           0.0.0.0
 006   No     0            0           0.0.0.0
 007   No     0            0           0.0.0.0
 008   No     0            0           0.0.0.0
 009   No     0            0           0.0.0.0
 010   No     0            0           0.0.0.0


Select Command= None           Select Rule= N/A
      Press ENTER to Confirm or ESC to Cancel:
```

4 Select **Edit Rule** in the **Select Command** field; type the index number of the NAT server you want to configure in the **Select Rule** field and press [ENTER] to open **Menu 15.2.x.x - NAT Server Configuration** (see the next figure).

**Figure 418** 15.2.x.x: NAT Server Configuration

```
            15.2.1.2 - NAT Server Configuration

                 Wan= 1                          Index= 2

             -------------------------------------------------

                 Name= 1

                 Active= Yes

                 Start port= 21                  End port= 25

                 IP Address= 192.168.1.33

            Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this screen.

**Table 244** 15.2.x.x: NAT Server Configuration

| FIELD | DESCRIPTION |
|---|---|
| WAN | On a ZyWALL with two WAN ports, you can configure port forwarding and trigger port rules for the first WAN port and separate sets of rules for the second WAN port. This is the WAN port (server set) you select in menu 15.2. |
| Index | This is the index number of an individual port forwarding server entry. |
| Name | Enter a name to identify this port-forwarding rule. |
| Active | Press [SPACE BAR] and then [ENTER] to select **Yes** to enable the NAT server entry. |
| Start Port | Enter a port number in the **Start Port** field. To forward only one port, enter it again in the **End Port** field. To specify a range of ports, enter the last port to be forwarded in the **End Port** field. |
| End Port | |
| IP Address | Enter the inside IP address of the server. |
| When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel. | |

5 Enter a port number in the **Start Port** field. To forward only one port, enter it again in the **End Port** field. To specify a range of ports, enter the last port to be forwarded in the **End Port** field.

6 Enter the inside IP address of the server in the **IP Address** field. In the following figure, you have a computer acting as an FTP, Telnet and SMTP server (ports 21, 23 and 25) at 192.168.1.33.

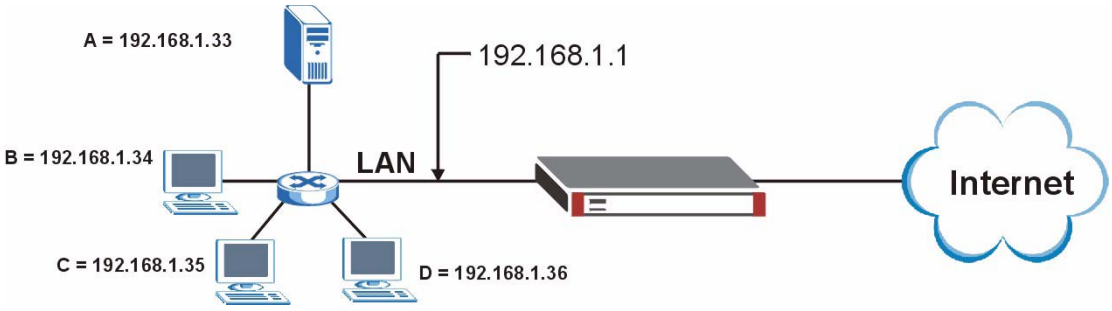
7 Press [ENTER] at the “Press ENTER to confirm …” prompt to save your configuration after you define all the servers or press [ESC] at any time to cancel.

**Figure 419** Menu 15.2.1: NAT Server Setup

```
                Menu 15.2.1 - NAT Server Setup

              Default Server: 0.0.0.0
 Rule  Act.   Start Port   End Port    IP Address
-------------------------------------------------------
 001   No     0            0           0.0.0.0
 002   Yes    21           25          192.168.1.33
 003   No     0            0           0.0.0.0
 004   No     0            0           0.0.0.0
 005   No     0            0           0.0.0.0
 006   No     0            0           0.0.0.0
 007   No     0            0           0.0.0.0
 008   No     0            0           0.0.0.0
 009   No     0            0           0.0.0.0
 010   No     0            0           0.0.0.0


Select Command= None           Select Rule= N/A
      Press ENTER to Confirm or ESC to Cancel:
```

You assign the private network IP addresses. The NAT network appears as a single host on the Internet. A is the FTP/Telnet/SMTP server.

**Figure 420** Server Behind NAT Example




## 44.4 General NAT Examples

The following are some examples of NAT configuration.

### 44.4.1 Internet Access Only

In the following Internet access example, you only need one rule where all your ILAs (Inside Local addresses) map to one dynamic IGA (Inside Global Address) assigned by your ISP.

**Figure 421** NAT Example 1

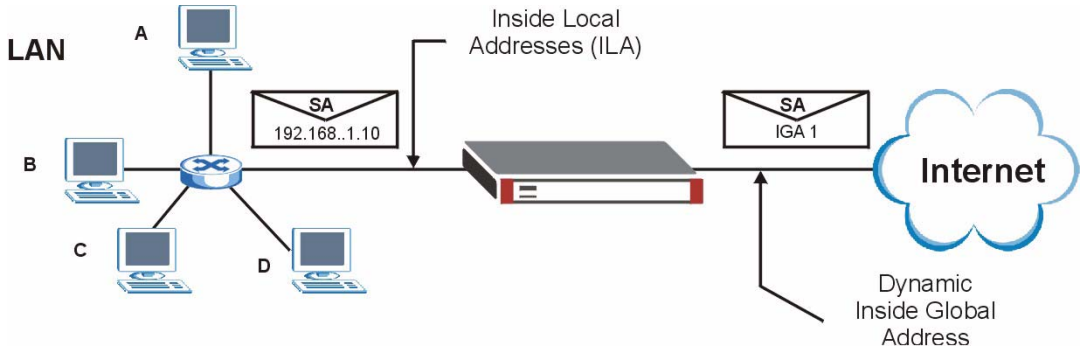


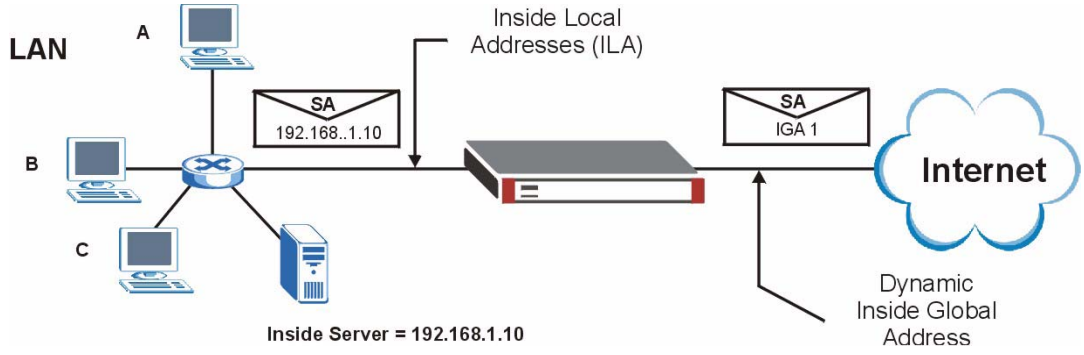

**Figure 422** Menu 4: Internet Access & NAT Example

```
            Menu 4 - Internet Access Setup

            ISP's Name= ChangeMe
            Encapsulation= Ethernet
              Service Type= Standard
              My Login= N/A
              My Password= N/A
              Retype to Confirm= N/A
              Login Server= N/A
              Relogin Every (min)=  N/A
            IP Address Assignment= Dynamic
              IP Address= N/A
              IP Subnet Mask= N/A
              Gateway IP Address= N/A
            Network Address Translation= SUA Only


            Press ENTER to Confirm or ESC to Cancel:
```

From menu 4 shown above, simply choose the **SUA Only** option from the **Network Address Translation** field. This is the Many-to-One mapping discussed in Section 44.4 on page 683. The **SUA Only** read-only option from the **Network Address Translation** field in menus 4 and 11.3 is specifically pre-configured to handle this case.

## 44.4.2 Example 2: Internet Access with a Default Server

**Figure 423** NAT Example 2




In this case, you do exactly as above (use the convenient pre-configured **SUA Only** set) and also go to menu 15.2.1 to specify the **Default Server** behind the NAT as shown in the next figure.

**Figure 424** Menu 15.2.1: Specifying an Inside Server

```
                Menu 15.2.1 - NAT Server Setup

                Default Server: 192.168.1.10
 Rule   Act.    Start Port   End Port    IP Address
-------------------------------------------------------
 001    No      0            0           0.0.0.0
 002    Yes     21           25          192.168.1.33
 003    No      0            0           0.0.0.0
 004    No      0            0           0.0.0.0
 005    No      0            0           0.0.0.0
 006    No      0            0           0.0.0.0
 007    No      0            0           0.0.0.0
 008    No      0            0           0.0.0.0
 009    No      0            0           0.0.0.0
 010    No      0            0           0.0.0.0


Select Command= None           Select Rule= N/A
      Press ENTER to Confirm or ESC to Cancel:
```

## 44.4.3 Example 3: Multiple Public IP Addresses With Inside Servers

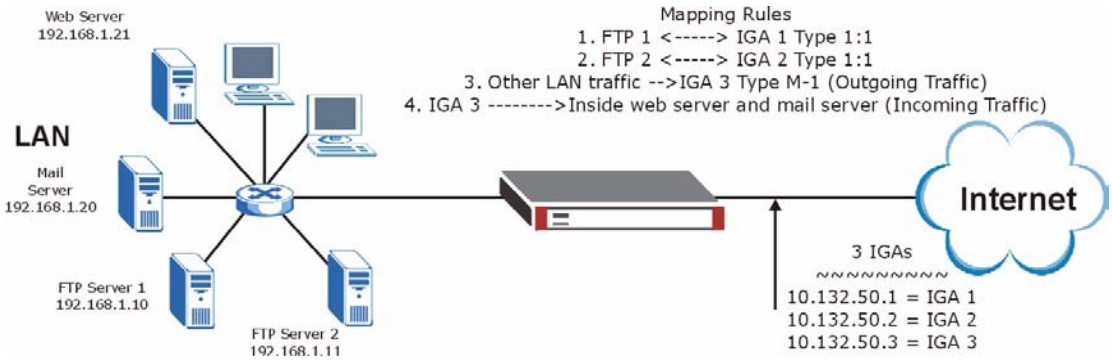
In this example, there are 3 IGAs from our ISP. There are many departments but two have their own FTP server. All departments share the same router. The example will reserve one IGA for each department with an FTP server and all departments use the other IGA. Map the FTP servers to the first two IGAs and the other LAN traffic to the remaining IGA. Map the third IGA to an inside web server and mail server. Four rules need to be configured, two bi-directional and two uni-directional as follows.

1. Map the first IGA to the first inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).

2 Map the second IGA to our second inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).
3 Map the other outgoing LAN traffic to IGA3 (**Many : 1** mapping).
4 You also map your third IGA to the web server and mail server on the LAN. Type **Server** allows you to specify multiple servers, of different types, to other computers behind NAT on the LAN.

The example situation looks somewhat like this:

**Figure 425** NAT Example 3




1 In this case you need to configure Address Mapping Set 1 from **Menu 15.1 - Address Mapping Sets**. Therefore you must choose the **Full Feature** option from the **Network Address Translation** field (in menu 4 or menu 11.3) in Figure 426 on page 687.
2 Then enter 15 from the main menu.
3 Enter 1 to configure the Address Mapping Sets.
4 Enter 1 to begin configuring this new set. Enter a Set Name, choose the **Edit Action** and then enter 1 for the **Select Rule** field. Press [ENTER] to confirm.
5 Select **Type** as **One-to-One** (direct mapping for packets going both ways), and enter the local **Start IP** as 192.168.1.10 (the IP address of FTP Server 1), the global **Start IP** as 10.132.50.1 (our first IGA). (See Figure 427 on page 687*)*.
6 Repeat the previous step for rules 2 to 4 as outlined above.
7 When finished, menu 15.1.1 should look like as shown in Figure 428 on page 688.

**Figure 426** Example 3: Menu 11.1.2

```
Menu 11.1.2 - Remote Node Network Layer Options

              IP Address Assignment= Dynamic
              IP Address= N/A
              IP Subnet Mask= N/A
              Gateway IP Addr= N/A


              Network Address Translation= SUA Only
              NAT Lookup Set= 255
              Metric= 1
              Private= N/A
              RIP Direction= None
                Version= N/A
              Multicast= None



               Enter here to CONFIRM or ESC to CANCEL:
```

The following figure shows how to configure the first rule.

**Figure 427** Example 3: Menu 15.1.1.1

```
          Menu 15.1.1.1 Address Mapping Rule

              Type= One-to-One

              Local IP:
                Start= 192.168.1.10
                End  = N/A

              Global IP:
                Start= 10.132.50.1
                End  = N/A

              Server Mapping Set= N/A

          Press ENTER to Confirm or ESC to Cancel:
```

**Figure 428** Example 3: Final Menu 15.1.1

```
                  Menu 15.1.1 - Address Mapping Rules

Set Name= Example3

Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
---  ---------------  ---------------  ---------------  ---------------  ---
 1. 192.168.1.10                       10.132.50.1                        1-1
 2  192.168.1.11                       10.132.50.2                        1-1
 3. 0.0.0.0           255.255.255.255  10.132.50.3                        M-1
 4.                                   10.132.50.3                      Server
 5.
 6.
 7.
 8.
 9.
10.

                Action= Edit          Select Rule=

               Press ENTER to Confirm or ESC to Cancel:
```

Now configure the IGA3 to map to our web server and mail server on the LAN.

1. Enter 15 from the main menu.
2. Enter 2 to go to menu 15.2.
3. (Enter 1 or 2 from menu 15.2 on a ZyWALL with multiple WAN ports) configure the menu as shown in Figure 429 on page 688.

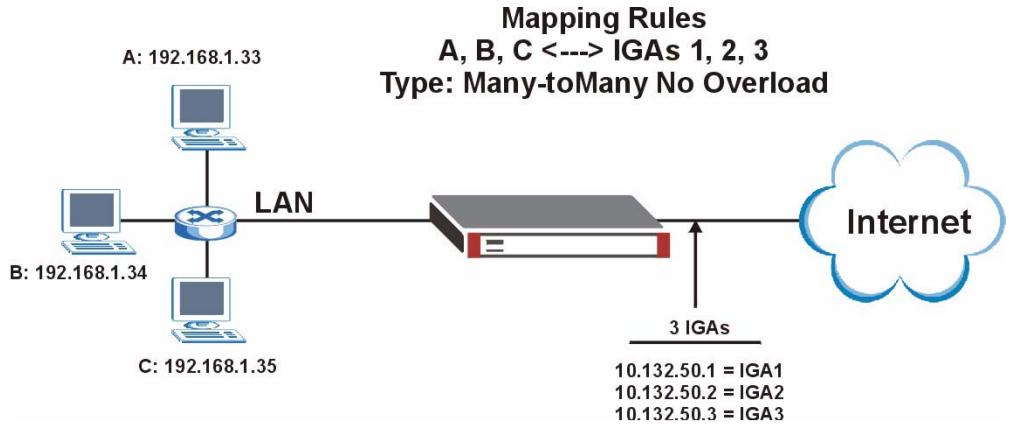
**Figure 429** Example 3: Menu 15.2.1

```
                        Menu 15.2.1 - NAT Server Setup

                   Default Server: 0.0.0.0
                Rule  Act.   Start Port   End Port    IP Address
               ------------------------------------------------------
               001   Yes    80           80          192.168.1.21
               002   Yes    25           25          192.168.1.20
               003   No     0            0           0.0.0.0
               004   No     0            0           0.0.0.0
               005   No     0            0           0.0.0.0
               006   No     0            0           0.0.0.0
               007   No     0            0           0.0.0.0
               008   No     0            0           0.0.0.0
               009   No     0            0           0.0.0.0
               010   No     0            0           0.0.0.0


              Select Command= None           Select Rule= N/A
                    Press ENTER to Confirm or ESC to Cancel:
```

### 44.4.4 Example 4: NAT Unfriendly Application Programs

Some applications do not support NAT Mapping using TCP or UDP port address translation. In this case it is better to use **Many-One-to-One** mapping as port numbers do *not* change for **Many-One-to-One** (and **One-to-One**) NAT mapping types. The following figure illustrates this.

**Figure 430** NAT Example 4




Other applications such as some gaming programs are NAT unfriendly because they embed addressing information in the data stream. These applications won't work through NAT even when using **One-to-One** and **Many-One-to-One** mapping types.

Follow the steps outlined in example 3 above to configure these two menus as follows.

**Figure 431** Example 4: Menu 15.1.1.1: Address Mapping Rule

```
                Menu 15.1.1.1 Address Mapping Rule

                      Type= Many-One-to-One

                      Local IP:
                        Start= 192.168.1.10
                        End  = 192.168.1.12

                      Global IP:
                        Start= 10.132.50.1
                        End  = 10.132.50.3

            Press ENTER to Confirm or ESC to Cancel:
```

After you've configured your rule, you should be able to check the settings in menu 15.1.1 as shown next.

**Figure 432** Example 4: Menu 15.1.1: Address Mapping Rules

```
                Menu 15.1.1 - Address Mapping Rules

  Set Name= Example4

Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
---  ---------------  ---------------  ---------------  ---------------  ---
 1.  192.168.1.10     192.168.1.12     10.132.50.1      10.132.50.3      M-1-1
 2.
 3.
 4.
 5.
 6.
 7.
 8.
 9.
10.

         Action= Edit          Select Rule=

         Press ENTER to Confirm or ESC to Cancel:
```

## 44.5 Trigger Port Forwarding

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 a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address.

Trigger port forwarding solves this problem by allowing computers on the LAN to dynamically take turns using the service. The ZyWALL records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a "trigger" port). When the ZyWALL's WAN port receives a response with a specific port number and protocol ("incoming" port), the ZyWALL forwards the traffic to the LAN IP address of the computer that sent the request. After that computer’s connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

### 44.5.1 Two Points To Remember About Trigger Ports

1. Trigger events only happen on data that is going coming from inside the ZyWALL and going to the outside.
2. If an application needs a continuous data stream, that port (range) will be tied up so that another computer on the LAN can’t trigger it.

Only one LAN computer can use a trigger port (range) at a time.

Enter 3 in menu 15 to display **Menu 15.3 - Trigger Ports**. For a ZyWALL with multiple WAN interfaces, enter 1 or 2 from menu 15.3 to go to **Menu 15.3.1** or **Menu 15.3.2 - Trigger Port Setup** and configure trigger port rules for the first or second WAN interface.

**Figure 433** Menu 15.3.1: Trigger Port Setup

```
                Menu 15.3.1 - Trigger Port Setup

                            Incoming                Trigger
     Rule     Name      Start Port   End Port   Start Port   End Port
     ------------------------------------------------------------
      1.  Real Audio         6970       7170         7070       7070
      2.                        0          0            0          0
      3.                        0          0            0          0
      4.                        0          0            0          0
      5.                        0          0            0          0
      6.                        0          0            0          0
      7.                        0          0            0          0
      8.                        0          0            0          0
      9.                        0          0            0          0
     10.                        0          0            0          0
     11.                        0          0            0          0
     12.                        0          0            0          0

                     Press ENTER to Confirm or ESC to Cancel:

     HTTP:80  FTP:21  Telnet:23  SMTP:25  POP3:110  PPTP:1723
```

The following table describes the fields in this menu.

**Table 245** Menu 15.3.1: Trigger Port Setup

| FIELD | DESCRIPTION |
|---|---|
| Rule | This is the rule index number. |
| Name | Enter a unique name for identification purposes. You may enter up to 15 characters in this field. All characters are permitted - including spaces. |
| Incoming | Incoming is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The ZyWALL forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service. |
| Start Port | Enter a port number or the starting port number in a range of port numbers. |
| End Port | Enter a port number or the ending port number in a range of port numbers. |
| Trigger | The trigger port is a port (or a range of ports) that causes (or triggers) the ZyWALL to record the IP address of the LAN computer that sent the traffic to a server on the WAN. |
| Start Port | Enter a port number or the starting port number in a range of port numbers. |

**Table 245** Menu 15.3.1: Trigger Port Setup (continued)

| FIELD | DESCRIPTION |
|---|---|
| End Port | Enter a port number or the ending port number in a range of port numbers. |
| Press [ENTER] at the message “Press ENTER to Confirm...” to save your configuration, or press [ESC] at any time to cancel. | |

# 45

# Introducing the ZyWALL Firewall

This chapter shows you how to get started with the ZyWALL firewall.

## 45.1 Using ZyWALL SMT Menus

From the main menu enter 21 to go to **Menu 21 - Filter Set and Firewall Configuration** to display the screen shown next.

**Figure 434** Menu 21: Filter and Firewall Setup

```
            Menu 21 - Filter and Firewall Setup

                     1. Filter Setup
                     2. Firewall Setup


            Enter Menu Selection Number:
```

### 45.1.1 Activating the Firewall

Enter option 2 in this menu to bring up the following screen. Press [SPACE BAR] and then [ENTER] to select **Yes** in the **Active** field to activate the firewall. The firewall must be active to protect against Denial of Service (DoS) attacks. Use the web configurator to configure firewall rules.

**Figure 435** Menu 21.2: Firewall Setup

```
                        Menu 21.2 - Firewall Setup

            The firewall protects against Denial of Service (DoS) attacks
            when it is active.

            Your network is vulnerable to attacks when the firewall is
            turned off.

            Refer to the User's Guide for details about the firewall
            default policies.

            You may define additional policy rules or modify existing ones
            but please exercise extreme caution in doing so.

            Active: Yes

            You can use the Web Configurator to configure the firewall.

                     Press ENTER to Confirm or ESC to Cancel:
```

Configure the firewall rules using the web configurator or CLI commands.

# 46

# Filter Configuration

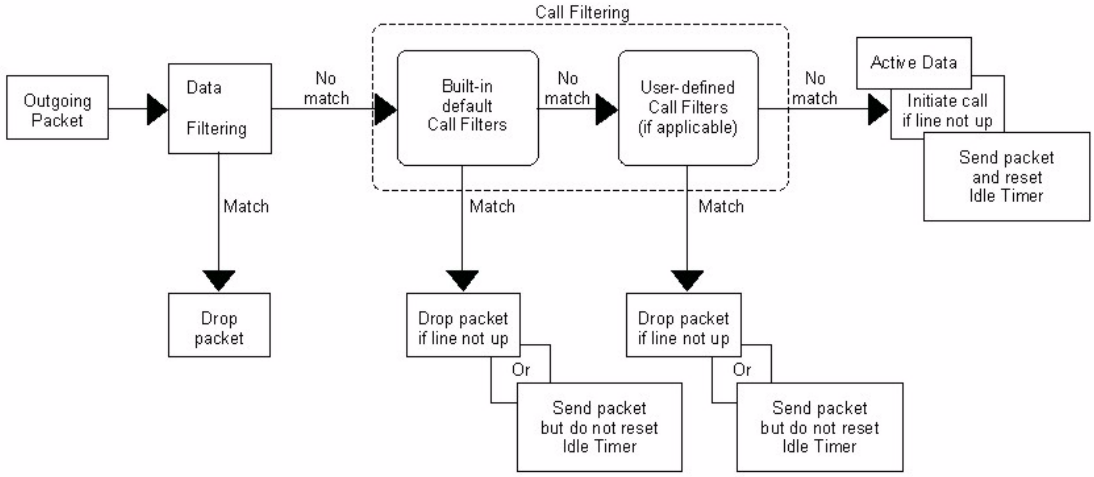
This chapter shows you how to create and apply filters.

## 46.1 Introduction to Filters

Your ZyWALL uses filters to decide whether to allow passage of a data packet and/or to make a call. There are two types of filter applications: data filtering and call filtering. Filters are subdivided into device and protocol filters, which are discussed later.

Data filtering screens the data to determine if the packet should be allowed to pass. Data filters are divided into incoming and outgoing filters, depending on the direction of the packet relative to a port. Data filtering can be applied on either the WAN side or the LAN side. Call filtering is used to determine if a packet should be allowed to trigger a call. Remote node call filtering is only applicable when using PPPoE encapsulation. Outgoing packets must undergo data filtering before they encounter call filtering as shown in the following figure.

**Figure 436** Outgoing Packet Filtering Process




For incoming packets, your ZyWALL applies data filters only. Packets are processed depending upon whether a match is found. The following sections describe how to configure filter sets.

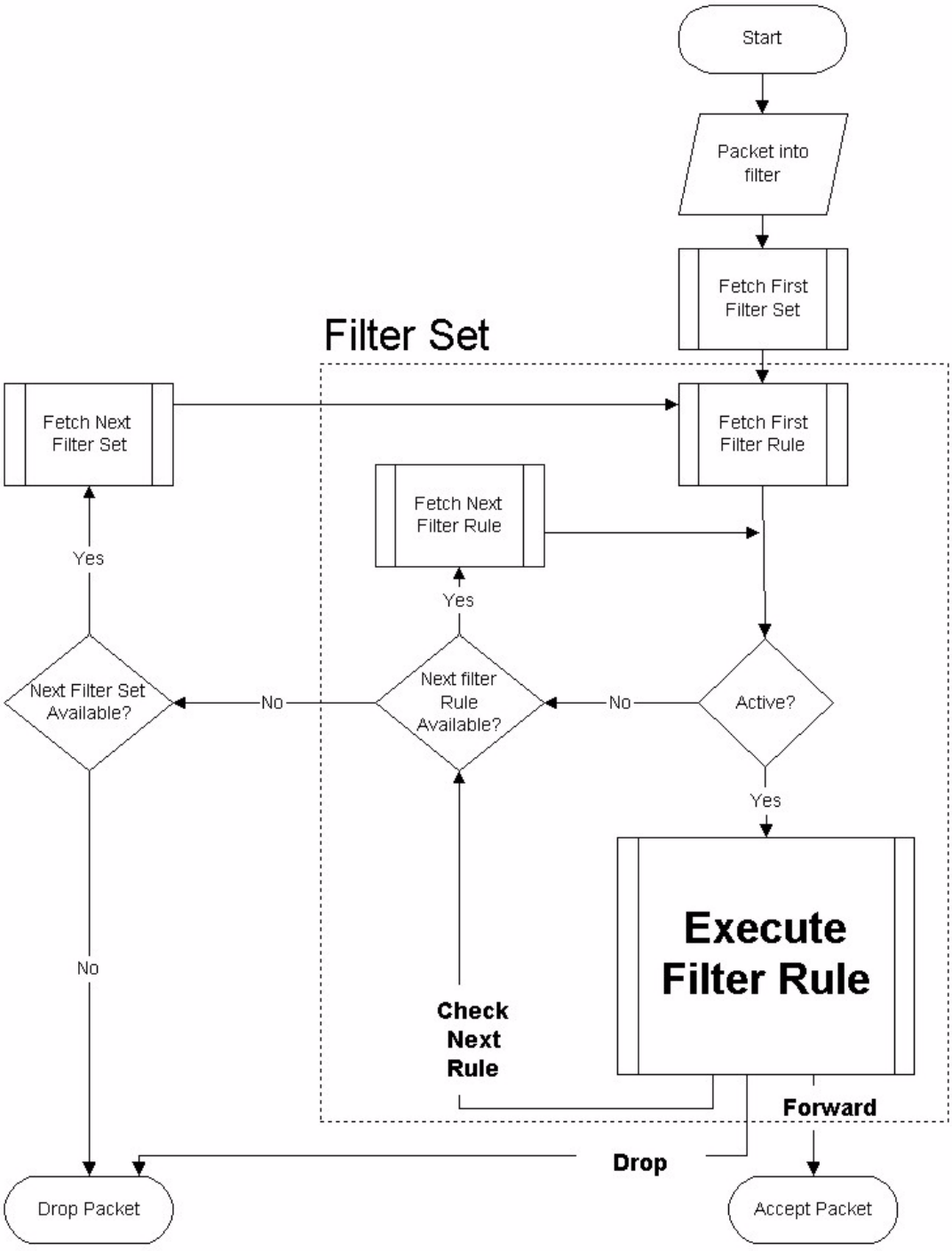
### 46.1.1 The Filter Structure of the ZyWALL

A filter set consists of one or more filter rules. Usually, you would group related rules, e.g., all the rules for NetBIOS, into a single set and give it a descriptive name. The ZyWALL allows you to configure up to twelve filter sets with six rules in each set, for a total of 72 filter rules in the system. You cannot mix device filter rules and protocol filter rules within the same set. You can apply up to four filter sets to a particular port to block multiple types of packets. With each filter set having up to six rules, you can have a maximum of 24 rules active for a single port.

Sets of factory default filter rules have been configured in menu 21 to prevent NetBIOS traffic from triggering calls and to prevent incoming telnet sessions. A summary of their filter rules is shown in the figures that follow.

The following figure illustrates the logic flow when executing a filter rule. See also Figure 441 on page 702 for the logic flow when executing an IP filter.

**Figure 437** Filter Rule Process




You can apply up to four filter sets to a particular port to block multiple types of packets. With each filter set having up to six rules, you can have a maximum of 24 rules active for a single port.

## 46.2 Configuring a Filter Set

The ZyWALL includes filtering for NetBIOS over TCP/IP packets by default. To configure another filter set, follow the procedure below.

1. Enter 21 in the main menu to open menu 21.

**Figure 438** Menu 21: Filter and Firewall Setup

```
            Menu 21 - Filter and Firewall Setup

                     1. Filter Setup
                     2. Firewall Setup




            Enter Menu Selection Number:
```

2. Enter 1 to bring up the following menu.

**Figure 439** Menu 21.1: Filter Set Configuration

```
                Menu 21.1 - Filter Set Configuration

    Filter                              Filter
    Set #        Comments               Set #        Comments
    ------  -----------------           ------  -----------------
     1      _________________            7      _________________
     2      _________________            8      _________________
     3      _________________            9      _________________
     4      _________________           10      _________________
     5      _________________           11      _________________
     6      _________________           12      _________________


         Enter Filter Set Number to Configure= 0

         Edit Comments= N/A

         Press ENTER to Confirm or ESC to Cancel:
```

3. Select the filter set you wish to configure (1-12) and press [ENTER].
4. Enter a descriptive name or comment in the **Edit Comments** field and press [ENTER].
5. Press [ENTER] at the message [Press ENTER to confirm] to open **Menu 21.1.x - Filter Rules Summary**.

This screen shows the summary of the existing rules in the filter set. The following tables contain a brief description of the abbreviations used in the previous menus.

**Table 246** Abbreviations Used in the Filter Rules Summary Menu

| FIELD | DESCRIPTION |
|---|---|
| A | Active: “Y” means the rule is active. “N” means the rule is inactive. |
| Type | The type of filter rule: “GEN” for Generic, “IP” for TCP/IP. |
| Filter Rules | These parameters are displayed here. |
| M | More.<br>“Y” means there are more rules to check which form a rule chain with the present rule. An action cannot be taken until the rule chain is complete.<br>“N” means there are no more rules to check. You can specify an action to be taken i.e., forward the packet, drop the packet or check the next rule. For the latter, the next rule is independent of the rule just checked. |
| m | Action Matched.<br>“F” means to forward the packet immediately and skip checking the remaining rules.<br>“D” means to drop the packet.<br>“N“ means to check the next rule. |
| n | Action Not Matched.<br>“F” means to forward the packet immediately and skip checking the remaining rules.<br>“D” means to drop the packet.<br>“N” means to check the next rule. |

The protocol dependent filter rules abbreviation are listed as follows:

**Table 247** Rule Abbreviations Used

| ABBREVIATION | DESCRIPTION |
|---|---|
| IP | |
| Pr | Protocol |
| SA | Source Address |
| SP | Source Port number |
| DA | Destination Address |
| DP | Destination Port number |
| GEN | |
| Off | Offset |
| Len | Length |

Refer to the next section for information on configuring the filter rules.

## 46.2.1 Configuring a Filter Rule

To configure a filter rule, type its number in **Menu 21.1.x - Filter Rules Summary** and press [ENTER] to open menu 21.1.x.x for the rule.

To speed up filtering, all rules in a filter set must be of the same class, i.e., protocol filters or generic filters. The class of a filter set is determined by the first rule that you create. When applying the filter sets to a port, separate menu fields are provided for protocol and device filter sets. If you include a protocol filter set in a device filter field or vice versa, the ZyWALL will warn you and will not allow you to save.

## 46.2.2 Configuring a TCP/IP Filter Rule

This section shows you how to configure a TCP/IP filter rule. TCP/IP rules allow you to base the rule on the fields in the IP and the upper layer protocol, for example, UDP and TCP headers.

To configure TCP/IP rules, select **TCP/IP Filter Rule** from the **Filter Type** field and press [ENTER] to open **Menu 21.1.x.x - TCP/IP Filter Rule**, as shown next.

**Figure 440** Menu 21.1.1.1: TCP/IP Filter Rule

```
            Menu 21.1.1.1 - TCP/IP Filter Rule

                        Filter #: 1,1
                        Filter Type= TCP/IP Filter Rule
                        Active= Yes
                        IP Protocol= 0     IP Source Route= No
                        Destination: IP Addr=
                                     IP Mask=
                                     Port #=
                                     Port # Comp= None
                             Source: IP Addr=
                                     IP Mask=
                                     Port #=
                                     Port # Comp= None
                        TCP Estab= N/A
                        More= No           Log= None
                        Action Matched= Check Next Rule
                        Action Not Matched= Check Next Rule


                        Press ENTER to Confirm or ESC to Cancel:
```

The following table describes how to configure your TCP/IP filter rule.

**Table 248** Menu 21.1.1.1: TCP/IP Filter Rule

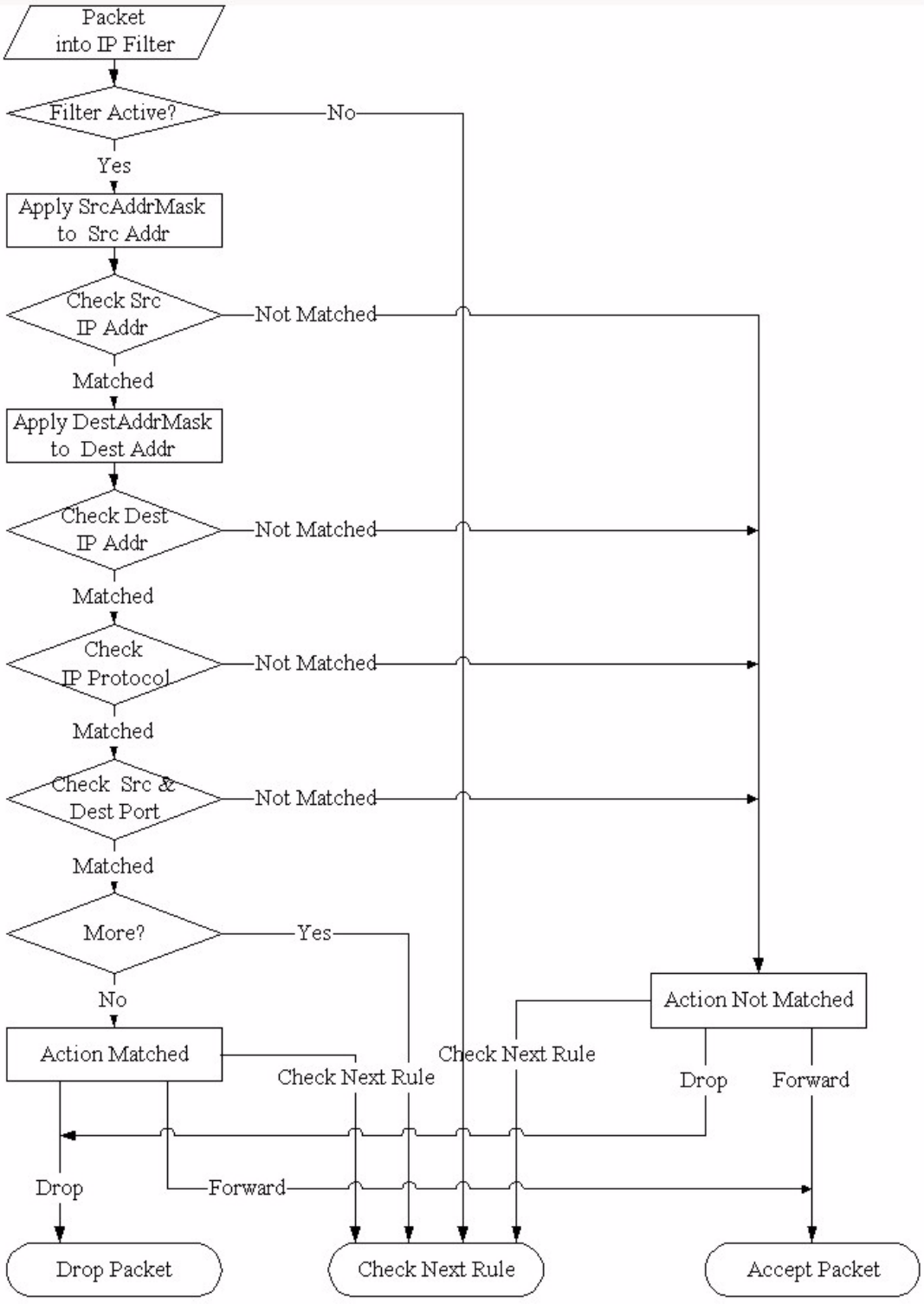
| FIELD | DESCRIPTION |
|---|---|
| Active | Press [SPACE BAR] and then [ENTER] to select **Yes** to activate the filter rule or **No** to deactivate it. |
| IP Protocol | Protocol refers to the upper layer protocol, e.g., TCP is 6, UDP is 17 and ICMP is 1. Type a value between 0 and 255. A value of 0 matches ANY protocol. |
| IP Source Route | Press [SPACE BAR] and then [ENTER] to select **Yes** to apply the rule to packets with an IP source route option. Otherwise the packets must not have a source route option. The majority of IP packets do not have source route. |
| Destination | |
| IP Addr | Enter the destination IP Address of the packet you wish to filter. This field is ignored if it is 0.0.0.0. |
| IP Mask | Enter the IP mask to apply to the **Destination: IP Addr**. |
| Port # | Enter the destination port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0. |

**Table 248** Menu 21.1.1.1: TCP/IP Filter Rule

| FIELD | DESCRIPTION |
|---|---|
| Port # Comp | Press [SPACE BAR] and then [ENTER] to select the comparison to apply to the destination port in the packet against the value given in **Destination: Port #**.<br>Options are **None**, **Equal**, **Not Equal**, **Less** and **Greater**. |
| Source | |
| IP Addr | Enter the source IP Address of the packet you wish to filter. This field is ignored if it is 0.0.0.0. |
| IP Mask | Enter the IP mask to apply to the **Source: IP Addr**. |
| Port # | Enter the source port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0. |
| Port # Comp | Press [SPACE BAR] and then [ENTER] to select the comparison to apply to the source port in the packet against the value given in **Source: Port #**.<br>Options are **None**, **Equal**, **Not Equal**, **Less** and **Greater**. |
| TCP Estab | This field is applicable only when the IP Protocol field is 6, TCP. Press [SPACE BAR] and then [ENTER] to select **Yes**, to have the rule match packets that want to establish a TCP connection (SYN=1 and ACK=0); if **No**, it is ignored. |
| More | Press [SPACE BAR] and then [ENTER] to select **Yes** or **No**. If **Yes**, a matching packet is passed to the next filter rule before an action is taken; if **No**, the packet is disposed of according to the action fields.<br>If **More** is **Yes**, then **Action Matched** and **Action Not Matched** will be **N/A**. |
| Log | Press [SPACE BAR] and then [ENTER] to select a logging option from the following:<br>**None** – No packets will be logged.<br>**Action Matched** - Only packets that match the rule parameters will be logged.<br>**Action Not Matched** - Only packets that do not match the rule parameters will be logged.<br>**Both** – All packets will be logged. |
| Action Matched | Press [SPACE BAR] and then [ENTER] to select the action for a matching packet.<br>Options are **Check Next Rule**, **Forward** and **Drop**. |
| Action Not Matched | Press [SPACE BAR] and then [ENTER] to select the action for a packet not matching the rule.<br>Options are **Check Next Rule**, **Forward** and **Drop**. |
| When you have **Menu 21.1.1.1 - TCP/IP Filter Rule** configured, press [ENTER] at the message “Press ENTER to Confirm” to save your configuration, or press [ESC] to cancel. This data will now be displayed on **Menu 21.1.1 - Filter Rules Summary**. | |

The following figure illustrates the logic flow of an IP filter.

**Figure 441** Executing an IP Filter




## 46.2.3 Configuring a Generic Filter Rule

This section shows you how to configure a generic filter rule. The purpose of generic rules is to allow you to filter non-IP packets. For IP, it is generally easier to use the IP rules directly.

For generic rules, the ZyWALL treats a packet as a byte stream as opposed to an IP or IPX packet. You specify the portion of the packet to check with the **Offset** (from 0) and the **Length** fields, both in bytes. The ZyWALL applies the Mask (bit-wise ANDing) to the data portion before comparing the result against the Value to determine a match. The **Mask** and **Value** are specified in hexadecimal numbers. Note that it takes two hexadecimal digits to represent a byte, so if the length is 4, the value in either field will take 8 digits, for example, FFFFFFFF.

To configure a generic rule, select **Generic Filter Rule** in the **Filter Type** field in menu 21.1.x.x and press [ENTER] to open Generic Filter Rule, as shown below.

**Figure 442** Menu 21.1.1.1: Generic Filter Rule

```
            Menu 21.1.1.1 - Generic Filter Rule

            Filter #: 1,1
            Filter Type= Generic Filter Rule
            Active= No
            Offset= 0
            Length= 0
            Mask= N/A
            Value= N/A
            More= No            Log= None
            Action Matched= Check Next Rule
            Action Not Matched= Check Next Rule

            Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in the **Generic Filter Rule** menu.

**Table 249** Generic Filter Rule Menu Fields

| FIELD | DESCRIPTION |
|---|---|
| Filter # | This is the filter set, filter rule co-ordinates, i.e., 2,3 refers to the second filter set and the third rule of that set. |
| Filter Type | Use [SPACE BAR] and then [ENTER] to select a rule type. Parameters displayed below each type will be different. TCP/IP filter rules are used to filter IP packets while generic filter rules allow filtering of non-IP packets.<br>Options are **Generic Filter Rule** and **TCP/IP Filter Rule**. |
| Active | Select **Yes** to turn on the filter rule or **No** to turn it off. |
| Offset | Enter the starting byte of the data portion in the packet that you wish to compare. The range for this field is from 0 to 255. |
| Length | Enter the byte count of the data portion in the packet that you wish to compare. The range for this field is 0 to 8. |
| Mask | Enter the mask (in Hexadecimal notation) to apply to the data portion before comparison. |
| Value | Enter the value (in Hexadecimal notation) to compare with the data portion. |
| More | If **Yes**, a matching packet is passed to the next filter rule before an action is taken; else the packet is disposed of according to the action fields.<br>If **More** is **Yes**, then Action Matched and Action Not Matched will be **No**. |

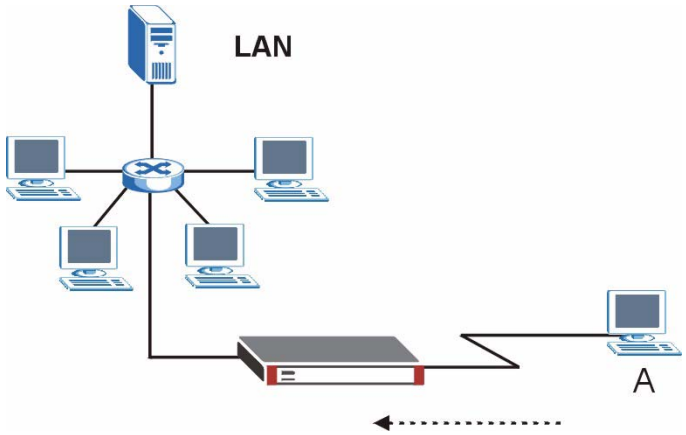
**Table 249** Generic Filter Rule Menu Fields

| FIELD | DESCRIPTION |
|---|---|
| Log | Select the logging option from the following:<br>**None** - No packets will be logged.<br>**Action Matched** - Only packets that match the rule parameters will be logged.<br>**Action Not Matched** - Only packets that do not match the rule parameters will be logged.<br>**Both** – All packets will be logged. |
| Action Matched | Select the action for a packet matching the rule.<br>Options are **Check Next Rule**, **Forward** and **Drop**. |
| Action Not Matched | Select the action for a packet not matching the rule.<br>Options are **Check Next Rule**, **Forward** and **Drop**. |
| Once you have completed filling in **Menu 21.1.1.1 - Generic Filter Rule**, press [ENTER] at the message “Press ENTER to Confirm” to save your configuration, or press [ESC] to cancel. This data will now be displayed on **Menu 21.1.1 - Filter Rules Summary**. | |

## 46.3 Example Filter

Here is an example to block outside users from accessing the ZyWALL via telnet.

**Figure 443** Telnet Filter Example




1. Enter 21 from the main menu to open **Menu 21 - Filter and Firewall Setup**.
2. Enter 1 to open Menu 21.1 - Filter Set Configuration.
3. Enter the index of the filter set you wish to configure (say 3) and press [ENTER].
4. Enter a descriptive name or comment in the **Edit Comments** field and press [ENTER].
5. Press [ENTER] at the message [Press ENTER to confirm] to open **Menu 21.1.3 - Filter Rules Summary**.
6. Enter 1 to configure the first filter rule (the only filter rule of this set). Make the entries in this menu as shown in the following figure.

**Figure 444** Example Filter: Menu 21.1.3.1

```
                          Menu 21.1.3.1 - TCP/IP Filter Rule

            Filter #: 3,1
            Filter Type= TCP/IP Filter Rule
            Active= Yes
            IP Protocol= 6      IP Source Route= No
            Destination: IP Addr= 0.0.0.0
                         IP Mask= 0.0.0.0
                         Port #= 23
                         Port # Comp= Equal
                 Source: IP Addr= 0.0.0.0
                         IP Mask= 0.0.0.0
                         Port #= 0
                         Port # Comp= None
            TCP Estab= No
            More= No             Log= None
            Action Matched= Drop
            Action Not Matched= Forward

                     Press ENTER to Confirm or ESC to Cancel:
            Press Space Bar to Toggle.
```

The port number for the telnet service (TCP protocol) is **23**. See *RFC 1060* for port numbers of well-known services.

When you press [ENTER] to confirm, you will see the following screen. Note that there is only one filter rule in this set.

**Figure 445** Example Filter Rules Summary: Menu 21.1.3

```
              Menu 21.1.3 - Filter Rules Summary

     # A Type                        Filter Rules              M m n
     - - ---- ------------------------------------------------ - - -
     1 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=23              N D F
     2 N
     3 N
     4 N7
     5 N
     6 N


     Enter Filter Rule Number (1-6) to Configure: 1
```

This shows you that you have configured and activated (**A = Y**) a TCP/IP filter rule (**Type = IP**, **Pr = 6**) for destination telnet ports (**DP = 23**).

**M = N** means an action can be taken immediately. The action is to drop the packet (**m = D**) if the action is matched and to forward the packet immediately (**n = F**) if the action is not matched no matter whether there are more rules to be checked (there aren't in this example).

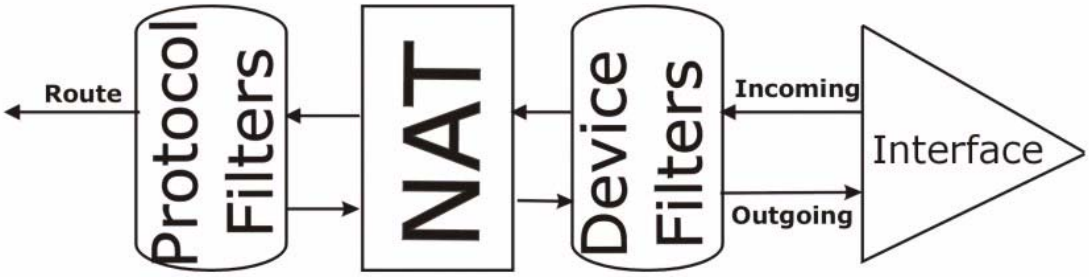
After you've created the filter set, you must apply it.

1. Enter 11 from the main menu to go to menu 11.
2. Enter 1 or 2 to open **Menu 11.x - Remote Node Profile**.
3. Go to the **Edit Filter Sets** field, press [SPACE BAR] to select **Yes** and press [ENTER].
4. This brings you to menu 11.1.4. Apply a filter set (our example filter set 3) as shown in Figure 449 on page 709.
5. Press [ENTER] to confirm after you enter the set numbers and to leave menu 11.1.4.

## 46.4 Filter Types and NAT

There are two classes of filter rules, **Generic Filter** (Device) rules and protocol filter (**TCP/IP**) rules. Generic filter rules act on the raw data from/to LAN and WAN. Protocol filter rules act on the IP packets. Generic and TCP/IP filter rules are discussed in more detail in the next section. When NAT (Network Address Translation) is enabled, the inside IP address and port number are replaced on a connection-by-connection basis, which makes it impossible to know the exact address and port on the wire. Therefore, the ZyWALL applies the protocol filters to the "native" IP address and port number before NAT for outgoing packets and after NAT for incoming packets. On the other hand, the generic, or device filters are applied to the raw packets that appear on the wire. They are applied at the point when the ZyWALL is receiving and sending the packets; i.e. the interface. The interface can be an Ethernet port or any other hardware port. The following diagram illustrates this.

**Figure 446** Protocol and Device Filter Sets




## 46.5 Firewall Versus Filters

Below are some comparisons between the ZyWALL's filtering and firewall functions.

### 46.5.1 Packet Filtering:

- The router filters packets as they pass through the router's interface according to the filter rules you designed.
- Packet filtering is a powerful tool, yet can be complex to configure and maintain, especially if you need a chain of rules to filter a service.
- Packet filtering only checks the header portion of an IP packet.

#### 46.5.1.1 When To Use Filtering

1. To block/allow LAN packets by their MAC addresses.
2. To block/allow special IP packets which are neither TCP nor UDP, nor ICMP packets.
3. To block/allow both inbound (WAN to LAN) and outbound (LAN to WAN) traffic between the specific inside host/network "A" and outside host/network "B". If the filter blocks the traffic from A to B, it also blocks the traffic from B to A. Filters cannot distinguish traffic originating from an inside host or an outside host by IP address.
4. To block/allow IP trace route.

### 46.5.2 Firewall

- The firewall inspects packet contents as well as their source and destination addresses. Firewalls of this type employ an inspection module, applicable to all protocols, that understands data in the packet is intended for other layers, from the network layer (IP headers) up to the application layer.
- The firewall performs stateful inspection. It takes into account the state of connections it handles so that, for example, a legitimate incoming packet can be matched with the outbound request for that packet and allowed in. Conversely, an incoming packet masquerading as a response to a non-existent outbound request can be blocked.
- The firewall uses session filtering, i.e., smart rules, that enhance the filtering process and control the network session rather than control individual packets in a session.
- The firewall provides e-mail service to notify you of routine reports and when alerts occur.

#### 46.5.2.1 When To Use The Firewall

1. To prevent DoS attacks and prevent hackers cracking your network.
2. A range of source and destination IP addresses as well as port numbers can be specified within one firewall rule making the firewall a better choice when complex rules are required.
3. To selectively block/allow inbound or outbound traffic between inside host/networks and outside host/networks. Remember that filters cannot distinguish traffic originating from an inside host or an outside host by IP address.
4. The firewall performs better than filtering if you need to check many rules.
5. Use the firewall if you need routine e-mail reports about your system or need to be alerted when attacks occur.
6. The firewall can block specific URL traffic that might occur in the future. The URL can be saved in an Access Control List (ACL) database.

## 46.6 Applying a Filter

This section shows you where to apply the filter(s) after you design it (them). The ZyWALL already has filters to prevent NetBIOS traffic from triggering calls, and block incoming telnet, FTP and HTTP connections.

If you do not activate the firewall, it is advisable to apply filters.

## 46.6.1 Applying LAN Filters

LAN traffic filter sets may be useful to block certain packets, reduce traffic and prevent security breaches. Go to menu 3.1 (shown next) and enter the number(s) of the filter set(s) that you want to apply as appropriate. You can choose up to four filter sets (from twelve) by entering their numbers separated by commas, e.g., 3, 4, 6, 11. Input filter sets filter incoming traffic to the ZyWALL and output filter sets filter outgoing traffic from the ZyWALL. For PPPoE or PPTP encapsulation, you have the additional option of specifying remote node call filter sets.

**Figure 447** Filtering LAN Traffic

```
                Menu 3.1 - LAN Port Filter Setup

          Input Filter Sets:
            protocol filters=
              device filters=
          Output Filter Sets:
            protocol filters=
              device filters=

          Press ENTER to Confirm or ESC to Cancel:
```

## 46.6.2 Applying DMZ Filters

DMZ traffic filter sets may be useful to block certain packets, reduce traffic and prevent security breaches. Go to menu 5.1 (shown next) and enter the number(s) of the filter set(s) that you want to apply as appropriate. You can choose up to four filter sets (from twelve) by entering their numbers separated by commas, e.g., 3, 4, 6, 11. Input filter sets filter incoming traffic to the ZyWALL and output filter sets filter outgoing traffic from the ZyWALL. The ZyWALL already has filters to prevent NetBIOS traffic from triggering calls, and block incoming telnet, FTP and HTTP connections.

**Figure 448** Filtering DMZ Traffic

```
                Menu 5.1 - DMZ Port Filter Setup

          Input Filter Sets:
            protocol filters=
              device filters=
          Output Filter Sets:
            protocol filters=
              device filters=

          Press ENTER to Confirm or ESC to Cancel:
```

### 46.6.3 Applying Remote Node Filters

Go to menu 11.1.4 (shown below – note that call filter sets are only present for PPPoE encapsulation) and enter the number(s) of the filter set(s) as appropriate. You can cascade up to four filter sets by entering their numbers separated by commas. The ZyWALL already has filters to prevent NetBIOS traffic from triggering calls, and block incoming telnet, FTP and HTTP connections.

**Figure 449** Filtering Remote Node Traffic

```
                Menu 11.1.4 - Remote Node Filter Setup

            Input Filter Sets:
              protocol filters=
                device filters=
            Output Filter Sets:
              protocol filters=
                device filters=

            Press ENTER to Confirm or ESC to Cancel:
```

# 47

# SNMP Configuration

This chapter explains SNMP configuration menu 22.

## 47.1 SNMP Configuration

To configure SNMP, enter 22 from the main menu to display **Menu 22 - SNMP Configuration** as shown next. The “community” for **Get**, **Set** and **Trap** fields is SNMP terminology for password.

**Figure 450** Menu 22: SNMP Configuration

```
            Menu 22 - SNMP Configuration

                    SNMP:
                      Get Community= public
                      Set Community= public
                      Trusted Host= 0.0.0.0
                      Trap:
                        Community= public
                        Destination= 0.0.0.0


            Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the SNMP configuration parameters.

**Table 250** SNMP Configuration Menu Fields

| FIELD | DESCRIPTION |
|---|---|
| Get Community | Type the Get community, which is the password for the incoming Get- and GetNext requests from the management station. |
| Set Community | Type the Set community, which is the password for incoming Set requests from the management station. |
| Trusted Host | If you enter a trusted host, your ZyWALL will only respond to SNMP messages from this address. A blank (default) field means your ZyWALL will respond to all SNMP messages it receives, regardless of source. |
| Trap | |
| Community | Type the Trap community, which is the password sent with each trap to the SNMP manager. |

**Table 250** SNMP Configuration Menu Fields (continued)

| FIELD | DESCRIPTION |
|---|---|
| Destination | Type the IP address of the station to send your SNMP traps to. |
| When you have completed this menu, press [ENTER] at the prompt “Press [ENTER] to confirm or [ESC] to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen. | |

## 47.2 SNMP Traps

The ZyWALL will send traps to the SNMP manager when any one of the following events occurs:

**Table 251** SNMP Traps

| TRAP # | TRAP NAME | DESCRIPTION |
|---|---|---|
| 0 | coldStart (defined in *RFC-1215*) | A trap is sent after booting (power on). |
| 1 | warmStart (defined in *RFC-1215*) | A trap is sent after booting (software reboot). |
| 4 | authenticationFailure (defined in *RFC-1215*) | A trap is sent to the manager when receiving any SNMP get or set requirements with the wrong community (password). |
| 6 | whyReboot (defined in ZYXEL-MIB) | A trap is sent with the reason of restart before rebooting when the system is going to restart (warm start). |
| 6a | For intentional reboot: | A trap is sent with the message "System reboot by user!" if reboot is done intentionally, (for example, download new files, CI command "sys reboot", etc.). |
| 6b | For fatal error: | A trap is sent with the message of the fatal code if the system reboots because of fatal errors. |

# 48

# System Information & Diagnosis

This chapter covers SMT menus 24.1 to 24.4.

## 48.1 Introduction to System Status

This chapter covers the diagnostic tools that help you to maintain your ZyWALL. These tools include updates on system status, port status and log and trace capabilities.

Select menu 24 in the main menu to open **Menu 24 - System Maintenance**, as shown below.

**Figure 451** Menu 24: System Maintenance

```
            Menu 24 - System Maintenance

               1.  System Status
               2.  System Information and Console Port Speed
               3.  Log and Trace
               4.  Diagnostic
               5.  Backup Configuration
               6.  Restore Configuration
               7.  Upload Firmware
               8.  Command Interpreter Mode
               9.  Call Control
               10. Time and Date Setting
               11. Remote Management Setup


            Enter Menu Selection Number:
```

## 48.2 System Status

The first selection, System Status, gives you information on the version of your system firmware and the status and statistics of the ports, as shown in the next figure. System Status is a tool that can be used to monitor your ZyWALL. Specifically, it gives you information on your system firmware version, number of packets sent and number of packets received.

To get to the System Status:

1. Enter number 24 to go to **Menu 24 - System Maintenance**.
2. In this menu, enter 1 to open **Menu 24.1 - System Maintenance - Status**.

**3** There are three commands in **Menu 24.1 - System Maintenance - Status**. Entering 1 or 2 drops the WAN1 or WAN2 connection, 9 resets the counters and [ESC] takes you back to the previous screen.

**Figure 452** Menu 24.1: System Maintenance: Status

```
                  Menu 24.1 - System Maintenance - Status          10:04:42
                                                          Wed. Aug. 08, 2007
Port   Status       TxPkts      RxPkts    Cols    Tx B/s    Rx B/s     Up Time
WAN1   100M/Full       630        3325       0         0         0     0:52:41
WAN2   Down              0           0       0         0         0     0:00:00
 LAN   100M/Full       106           0       0         0         0     0:52:41
WCRD   Down              0           0       0         0         0     0:00:00
 DMZ   100M/Full          0           0       0         0         0     0:52:41
WLAN   100M/Full          5           0       0         0         0     0:52:41

Port   Ethernet Address        IP Address           IP Mask       DHCP
WAN1  00:00:AA:77:89:26     172.23.37.207       255.255.0.0       None
WAN2  00:00:AA:77:89:28           0.0.0.0           0.0.0.0     Client
 LAN  00:00:AA:77:89:25       192.168.1.1     255.255.255.0     Server
WLAN  00:00:AA:77:89:29           0.0.0.0           0.0.0.0       None
 DMZ  00:00:AA:77:89:27           0.0.0.0           0.0.0.0       None

     System up Time:     0:52:46

                                Press Command:

             COMMANDS: 1, 2-Drop WAN1,2 9-Reset Counters   ESC-Exit
```

The following table describes the fields present in **Menu 24.1 - System Maintenance - Status**. These fields are READ-ONLY and meant for diagnostic purposes. The upper right corner of the screen shows the time and date according to the format you set in menu 24.10.

**Table 252** System Maintenance: Status Menu Fields

| FIELD | DESCRIPTION |
|---|---|
| Port | This field identifies an interface (WAN1, WAN2, LAN, WCRD (wireless LAN card), DMZ or WLAN) on the ZyWALL. |
| Status | For the LAN, DMZ, and WLAN Interfaces, this displays the port speed and duplex setting.<br>For the WAN interfaces, it displays the port speed and duplex setting if you're using Ethernet encapsulation or the remote node name (configured through the SMT) for a PPP connection and **Down** (line is down or not connected), **Idle** (line (ppp) idle), **Dial** (starting to trigger a call) or **Drop** (dropping a call) if you're using PPPoE encapsulation.<br>For the wireless card, it displays the transmission rate when a wireless LAN card is inserted and WLAN is enabled or **Down** when a wireless LAN is not inserted or WLAN is disabled.<br>Note: In Menu 24.1, **WCRD** only represents the WLAN card status. The **WCRD** status is always down when a TURBO card is installed. |
| TxPkts | This is the number of transmitted packets on this port. |
| RxPkts | This is the number of received packets on this port. |

**Table 252** System Maintenance: Status Menu Fields (continued)

| FIELD | DESCRIPTION |
|---|---|
| Cols | This is the number of collisions on this port. |
| Tx B/s | This field shows the transmission speed in Bytes per second on this port. |
| Rx B/s | This field shows the reception speed in Bytes per second on this port. |
| Up Time | This is the total amount of time the line has been up. |
| Ethernet Address | This is the MAC address of the port listed on the left. |
| IP Address | This is the IP address of the port listed on the left. |
| IP Mask | This is the IP mask of the port listed on the left. |
| DHCP | This is the DHCP setting of the port listed on the left. |
| System up Time | This is the total time the ZyWALL has been on. |
| CARD bridged to | This field shows whether the wireless card is set to be part of the LAN, DMZ or WLAN. |
| You may enter 1 to drop the WAN connection, 9 to reset the counters or [ESC] to return to menu 24. | |

## 48.3 System Information and Console Port Speed

This section describes your system and allows you to choose different console port speeds. To get to the System Information and Console Port Speed:

1. Enter 24 to go to **Menu 24 - System Maintenance**.
2. Enter 2 to open **Menu 24.2 - System Information and Console Port Speed**.
3. From this menu you have two choices as shown in the next figure:

**Figure 453** Menu 24.2: System Information and Console Port Speed

```
            Menu 24.2 - System Information and Console Port Speed

                   1. System Information
                   2. Console Port Speed

            Please enter selection:
```

### 48.3.1 System Information

System Information gives you information about your system as shown below. More specifically, it gives you information on your routing protocol, Ethernet address, IP address, etc.

**Figure 454** Menu 24.2.1: System Maintenance: Information

```
                Menu 24.2.1 - System Maintenance - Information

                   Name:
                   Routing: IP
                   ZyNOS F/W Version: V4.03(WM.0)b1 | 06/29/2007
                   Country Code: 255

                   LAN
                     Ethernet Address: 00:13:49:00:00:02
                     IP Address: 192.168.1.1
                     IP Mask: 255.255.255.0
                     DHCP: Server









                           Press ESC or RETURN to Exit:
```

The following table describes the fields in this screen.

**Table 253** Fields in System Maintenance: Information

| FIELD | DESCRIPTION |
|---|---|
| Name | This is the ZyWALL's system name + domain name assigned in menu 1. For example, System Name= xxx; Domain Name= baboo.mickey.com<br>Name= xxx.baboo.mickey.com |
| Routing | Refers to the routing protocol used. |
| ZyNOS F/W Version | Refers to the version of ZyXEL's Network Operating System software. |
| Country Code | Refers to the country code of the firmware. |
| LAN | |
| Ethernet Address | Refers to the Ethernet MAC (Media Access Control) address of your ZyWALL. |
| IP Address | This is the IP address of the ZyWALL in dotted decimal notation. |
| IP Mask | This shows the IP mask of the ZyWALL. |
| DHCP | This field shows the DHCP setting of the ZyWALL. |
| When finished viewing, press [ESC] or [ENTER] to exit. | |

## 48.3.2 Console Port Speed

You can change the speed of the console port through **Menu 24.2.2 – Console Port Speed**. Your ZyWALL supports 9600 (default), 19200, 38400, 57600, and 115200 bps for the console port. Press [SPACE BAR] and then [ENTER] to select the desired speed in menu 24.2.2, as shown next.

**Figure 455** Menu 24.2.2: System Maintenance: Change Console Port Speed

```
            Menu 24.2.2 - System Maintenance - Change Console Port Speed

                            Console Port Speed: 9600


                          Press ENTER to Confirm or ESC to Cancel:Press
            Space Bar to Toggle.
```

# 48.4 Log and Trace

There are two logging facilities in the ZyWALL. The first is the error logs and trace records that are stored locally. The second is the UNIX syslog facility for message logging.

## 48.4.1 Viewing Error Log

The first place you should look for clues when something goes wrong is the error/trace log. Follow the procedure below to view the local error/trace log:

1. Select option 24 from the main menu to open **Menu 24 - System Maintenance**.
2. From menu 24, select option 3 to open **Menu 24.3 - System Maintenance - Log and Trace**.
3. Select the first option from **Menu 24.3 - System Maintenance - Log and Trace** to display the error log in the system.

After the ZyWALL finishes displaying, you will have the option to clear the error log.

**Figure 456** Menu 24.3: System Maintenance: Log and Trace

```
            Menu 24.3 - System Maintenance - Log and Trace

            1. View Error Log
            2. UNIX Syslog

            4. Call-Triggering Packet


                   Please enter selection
```

Examples of typical error and information messages are presented in the following figure.

**Figure 457** Examples of Error and Information Messages

```
  52 Thu Jul  1 05:54:53 2004 PP05  ERROR Wireless LAN init fail, code=15
  53 Thu Jul  1 05:54:53 2004 PINI  INFO  Channel 0 ok
  54 Thu Jul  1 05:54:56 2004 PP05 -WARN  SNMP TRAP 3: interface 3: link up
  55 Thu Jul  1 05:54:56 2004 PP0d  INFO  LAN promiscuous mode <0>
  57 Thu Jul  1 05:54:56 2004 PP0d  INFO  LAN promiscuous mode <1>
  58 Thu Jul  1 05:54:56 2004 PINI  INFO  Last errorlog repeat 1 Times
  59 Thu Jul  1 05:54:56 2004 PINI  INFO  main: init completed
  60 Thu Jul  1 05:55:26 2004 PSSV -WARN  SNMP TRAP 0: cold start
  61 Thu Jul  1 05:56:56 2004 PINI  INFO  SMT Session Begin
  62 Thu Jul  1 07:50:58 2004 PINI  INFO  SMT Session End
  63 Thu Jul  1 07:53:28 2004 PINI  INFO  SMT Session Begin
  Clear Error Log (y/n):
```

## 48.4.2 Syslog Logging

The ZyWALL uses the syslog facility to log the CDR (Call Detail Record) and system messages to a syslog server. Syslog and accounting can be configured in **Menu 24.3.2 - System Maintenance - Syslog Logging**, as shown next.

**Figure 458** Menu 24.3.2: System Maintenance: Syslog Logging

```
            Menu 24.3.2 - System Maintenance - Syslog Logging

                  Syslog:
                  Active= No
                  Syslog Server IP Address= 0.0.0.0
                  Log Facility= Local 1


                Press ENTER to Confirm or ESC to Cancel:
```

You need to configure the syslog parameters described in the following table to activate syslog then choose what you want to log.

**Table 254** System Maintenance Menu Syslog Parameters

| FIELD | DESCRIPTION |
|---|---|
| Syslog: | |
| Active | Press [SPACE BAR] and then [ENTER] to turn syslog on or off. |
| Syslog Server IP Address | Enter the server n77777ame or IP address of the syslog server that will log the selected categories of logs. |
| Log Facility | Press [SPACE BAR] and then [ENTER] to select a location. The log facility allows you to log the messages to different files in the syslog server. Refer to the documentation of your syslog program for more details. |
| When finished configuring this screen, press [ENTER] to confirm or [ESC] to cancel. | |

Your ZyWALL sends five types of syslog messages. Some examples (not all ZyWALL specific) of these syslog messages with their message formats are shown next:

**1** CDR

| CDR Message Format |
| --- |
| SdcmdSyslogSend( SYSLOG_CDR, SYSLOG_INFO, String );<br>String = board xx line xx channel xx, call xx, str<br>board = the hardware board ID<br>line = the WAN ID in a board<br>Channel = channel ID within the WAN<br>call = the call reference number which starts from 1 and increments by 1 for each new call<br>str = C01 Outgoing Call dev xx ch xx (dev:device No. ch:channel No.)<br>L02 Tunnel Connected(L2TP)<br>C02 OutCall Connected xxxx (means connected speed) xxxxx (means Remote Call Number)<br>L02 Call Terminated<br>C02 Call Terminated<br>Jul 19 11:19:27 192.168.102.2 ZyXEL: board 0 line 0 channel 0, call 1, C01 Outgoing Call dev=2 ch=0 40002<br>Jul 19 11:19:32 192.168.102.2 ZyXEL: board 0 line 0 channel 0, call 1, C02 OutCall Connected 64000 40002<br>Jul 19 11:20:06 192.168.102.2 ZyXEL: board 0 line 0 channel 0, call 1, C02 Call Terminated |

**2** Packet triggered

| Packet triggered Message Format |
| --- |
| SdcmdSyslogSend( SYSLOG_PKTTRI, SYSLOG_NOTICE, String );<br>String = Packet trigger: Protocol=xx Data=xxxxxxxxxx…..x<br>Protocol: (1:IP 2:IPX 3:IPXHC 4:BPDU 5:ATALK 6:IPNG)<br>Data: We will send forty-eight Hex characters to the server<br>Jul 19 11:28:39 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1,<br>Data=4500003c100100001f010004c0a86614ca849a7b08004a5c020001006162636465666768696a6b6c6d6e6f7071727374<br>Jul 19 11:28:56 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1,<br>Data=4500002c1b0140001f06b50ec0a86614ca849a7b0427001700195b3e00000000600220008cd40000020405b4<br>Jul 19 11:29:06 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1,<br>Data=45000028240140001f06ac12c0a86614ca849a7b0427001700195b451d143013500400007 7600000 |

**3** Filter log

| Filter log Message Format |
| --- |
| SdcmdSyslogSend(SYSLOG_FILLOG, SYSLOG_NOTICE, String );<br>String = IP[Src=xx.xx.xx.xx Dst=xx.xx.xx.xx prot spo=xxxx dpo=xxxx] S04>R01mD<br>IP[…] is the packet header and S04>R01mD means filter set 4 (S) and rule 1 (R), match (m) drop (D).<br>Src: Source Address<br>Dst: Destination Address<br>prot: Protocol ("TCP","UDP","ICMP")<br>spo: Source port<br>dpo: Destination portMar 03 10:39:43 202.132.155.97 ZyXEL: GEN[ffffffffffnordff0080] }S05>R01mF<br>Mar 03 10:41:29 202.132.155.97 ZyXEL:<br>GEN[00a0c5f502fnord010080] }S05>R01mF<br>Mar 03 10:41:34 202.132.155.97 ZyXEL:<br>IP[Src=192.168.2.33 Dst=202.132.155.93 ICMP]}S04>R01mF<br>Mar 03 11:59:20 202.132.155.97 ZyXEL:<br>GEN[00a0c5f502fnord010080] }S05>R01mF<br>Mar 03 12:00:52 202.132.155.97 ZyXEL:<br>GEN[ffffffffffff0080] }S05>R01mF<br>Mar 03 12:00:57 202.132.155.97 ZyXEL:<br>GEN[00a0c5f502010080] }S05>R01mF<br>Mar 03 12:01:06 202.132.155.97 ZyXEL:<br>IP[Src=192.168.2.33 Dst=202.132.155.93 TCP spo=01170 dpo=00021]}S04>R01mF |

**4** PPP log

| PPP Log Message Format |
| --- |
| SdcmdSyslogSend( SYSLOG_PPPLOG, SYSLOG_NOTICE, String );<br>String = ppp:Proto Starting / ppp:Proto Opening / ppp:Proto Closing / ppp:Proto Shutdown<br>Proto = LCP / ATCP / BACP / BCP / CBCP / CCP / CHAP/ PAP / IPCP /<br>IPXCP<br>Jul 19 11:42:44 192.168.102.2 ZyXEL: ppp:LCP Closing<br>Jul 19 11:42:49 192.168.102.2 ZyXEL: ppp:IPCP Closing<br>Jul 19 11:42:54 192.168.102.2 ZyXEL: ppp:CCP Closing |

**5** Firewall log

| Firewall Log Message Format |
| --- |
| SdcmdSyslogSend(SYSLOG_FIREWALL, SYSLOG_NOTICE, buf);<br>buf = IP[Src=xx.xx.xx.xx : spo=xxxx Dst=xx.xx.xx.xx : dpo=xxxx \| prot \| rule \| action]<br>Src: Source Address<br>spo: Source port (empty means no source port information)<br>Dst: Destination Address<br>dpo: Destination port (empty means no destination port information)<br>prot: Protocol ("TCP","UDP","ICMP", "IGMP", "GRE", "ESP")<br>rule: <a,b> where a means "set" number; b means "rule" number.<br>Action: nothing(N) block (B) forward (F)<br>08-01-200011:48:41Local1.Notice192.168.10.10RAS: FW 172.21.1.80 :137 ->172.21.1.80 :137 \|UDP\|default permit:<2,0>\|B<br>08-01-200011:48:41Local1.Notice192.168.10.10RAS: FW 192.168.77.88 :520 ->192.168.77.88 :520 \|UDP\|default permit:<2,0>\|B<br>08-01-200011:48:39Local1.Notice192.168.10.10RAS: FW 172.21.1.50 ->172.21.1.50 \|IGMP<2>\|default permit:<2,0>\|B<br>08-01-200011:48:39Local1.Notice192.168.10.10RAS: FW 172.21.1.25 ->172.21.1.25 \|IGMP<2>\|default permit:<2,0>\|B |

## 48.4.3 Call-Triggering Packet

Call-Triggering Packet displays information about the packet that triggered a dial-out call in an easy readable format. Equivalent information is available in menu 24.1 in hex format. An example is shown next.

**Figure 459** Call-Triggering Packet Example

```
IP Frame: ENET0-RECV Size:  44/  44   Time: 17:02:44.262
 Frame Type:

   IP Header:
     IP Version              = 4
     Header Length           = 20
     Type of Service         = 0x00 (0)
     Total Length            = 0x002C (44)
     Identification          = 0x0002 (2)
     Flags                   = 0x00
     Fragment Offset         = 0x00
     Time to Live            = 0xFE (254)
     Protocol                = 0x06 (TCP)
     Header Checksum         = 0xFB20 (64288)
     Source IP               = 0xC0A80101 (192.168.1.1)
     Destination IP          = 0x00000000 (0.0.0.0)

   TCP Header:
     Source Port             = 0x0401 (1025)
     Destination Port        = 0x000D (13)
     Sequence Number         = 0x05B8D000 (95997952)
     Ack Number              = 0x00000000 (0)
     Header Length           = 24
     Flags                   = 0x02 (....S.)
     Window Size             = 0x2000 (8192)
     Checksum                = 0xE06A (57450)
     Urgent Ptr              = 0x0000 (0)
     Options                 =
         0000: 02 04 02 00

   RAW DATA:
     0000: 45 00 00 2C 00 02 00 00-FE 06 FB 20 C0 A8 01 01  E.........  ....
     0010: 00 00 00 00 04 01 00 0D-05 B8 D0 00 00 00 00 00
.................
     0020: 60 02 20 00 E0 6A 00 00-02 04 02 00
Press any key to continue...
```

## 48.5 Diagnostic

The diagnostic facility allows you to test the different aspects of your ZyWALL to determine if it is working properly. Menu 24.4 allows you to choose among various types of diagnostic tests to evaluate your system, as shown next. Not all fields are available on all models.

Follow the procedure below to get to **Menu 24.4 - System Maintenance - Diagnostic**.

1. From the main menu, select option 24 to open **Menu 24 - System Maintenance**.
2. From this menu, select option 4. Diagnostic. This will open **Menu 24.4 - System Maintenance - Diagnostic**.

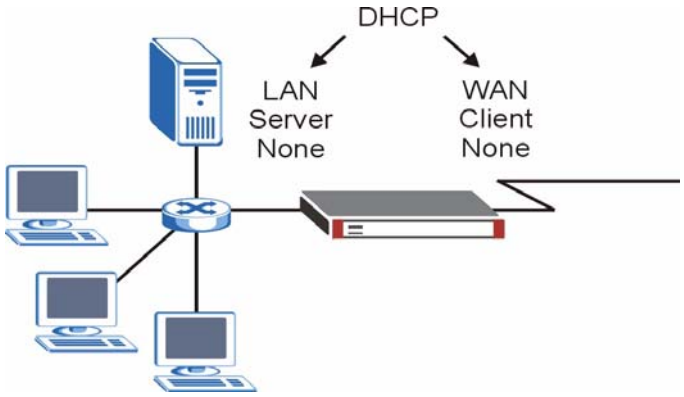
**Figure 460** Menu 24.4: System Maintenance: Diagnostic (ZyWALL 5)

```
            Menu 24.4 - System Maintenance - Diagnostic


           TCP/IP
             1. Ping Host
             2. WAN DHCP Release
             3. WAN DHCP Renewal
             4. PPPoE/PPTP/3G Setup Test

           System
             11. Reboot System


              Enter Menu Selection Number:

              WAN=
              Host IP Address= N/A
```

## 48.5.1 WAN DHCP

DHCP functionality can be enabled on the LAN or WAN as shown in Figure 461 on page 723. LAN DHCP has already been discussed. The ZyWALL can act either as a WAN DHCP client (**IP Address Assignment** field in menu 4 or menu 11.x.2 is **Dynamic** and the **Encapsulation** field in menu 4 or menu 11 is **Ethernet**) or **None**, (when you have a static IP). The **WAN Release** and **Renewal** fields in menu 24.4 conveniently allow you to release and/or renew the assigned WAN IP address, subnet mask and default gateway in a fashion similar to winipcfg.

**Figure 461** WAN & LAN DHCP




The following table describes the diagnostic tests available in menu 24.4 for your ZyWALL and associated connections.

**Table 255** System Maintenance Menu Diagnostic

| FIELD | DESCRIPTION |
|---|---|
| Ping Host | Enter 1 to ping any machine (with an IP address) on your LAN, DMZ, WLAN or WAN. Enter its IP address in the **Host IP Address** field below. |
| WAN DHCP Release | Enter 2 to release your WAN DHCP settings. |
| WAN DHCP Renewal | Enter 3 to renew your WAN DHCP settings. |
| Internet Setup Test<br>or<br>PPPoE/PPTP/3G Setup Test | Enter 4 to test the Internet setup. You can also test the Internet setup in **Menu 4 - Internet Access**. Please refer to Chapter 38 on page 639 for more details.<br>This feature is only available for a 3G connection or dial-up connections using PPPoE or PPTP encapsulation. |
| Reboot System | Enter 11 to reboot the ZyWALL. |
| WAN | If you entered 2, 3, or 4 in the **Enter Menu Selection Number** field, enter the number of the WAN interface in this field. |
| Host IP Address | If you entered 1in the **Enter Menu Selection Number** field, then enter the IP address of the computer you want to ping in this field. |
| Enter the number of the selection you would like to perform or press [ESC] to cancel. | |

# 49

# Firmware and Configuration File Maintenance

This chapter tells you how to back up and restore your configuration file as well as upload new firmware and a new configuration file.

## 49.1 Introduction

Use the instructions in this chapter to change the ZyWALL's configuration file or upgrade its firmware. After you configure your ZyWALL, you can backup the configuration file to a computer. That way if you later misconfigure the ZyWALL, you can upload the backed up configuration file to return to your previous settings. You can alternately upload the factory default configuration file if you want to return the ZyWALL to the original default settings. The firmware determines the ZyWALL's available features and functionality. You can download new firmware releases from your nearest ZyXEL FTP site to use to upgrade your ZyWALL's performance.

## 49.2 Filename Conventions

The configuration file (often called the romfile or rom-0) contains the factory default settings in the menus such as password, DHCP Setup, TCP/IP Setup, etc. It arrives from ZyXEL with a "rom" filename extension. Once you have customized the ZyWALL's settings, they can be saved back to your computer under a filename of your choosing.

ZyNOS (ZyXEL Network Operating System sometimes referred to as the "ras" file) is the system firmware and has a "bin" filename extension. With many FTP and TFTP clients, the filenames are similar to those seen next.

```
ftp> put firmware.bin ras
```

This is a sample FTP session showing the transfer of the computer file "firmware.bin" to the ZyWALL.

```
ftp> get rom-0 config.cfg
```

This is a sample FTP session saving the current configuration to the computer file "config.cfg".

If your (T)FTP client does not allow you to have a destination filename different than the source, you will need to rename them as the ZyWALL only recognizes "rom-0" and "ras". Be sure you keep unaltered copies of both files for later use.

The following table is a summary. Please note that the internal filename refers to the filename on the ZyWALL and the external filename refers to the filename not on the ZyWALL, that is, on your computer, local network or FTP site and so the name (but not the extension) may vary. After uploading new firmware, see the **ZyNOS F/W Version** field in **Menu 24.2.1 - System Maintenance - Information** to confirm that you have uploaded the correct firmware version. The AT command is the command you enter after you press "y" when prompted in the SMT menu to go into debug mode.

**Table 256** Filename Conventions

| FILE TYPE | INTERNAL NAME | EXTERNAL NAME | DESCRIPTION |
|---|---|---|---|
| Configuration File | Rom-0 | This is the configuration filename on the ZyWALL. Uploading the rom-0 file replaces the entire ROM file system, including your ZyWALL configurations, system-related data (including the default password), the error log and the trace log. | *.rom |
| Firmware | Ras | This is the generic name for the ZyNOS firmware on the ZyWALL. | *.bin |

## 49.3 Backup Configuration

The ZyWALL displays different messages explaining different ways to backup, restore and upload files in menus 24.5, 24.6, 24. 7.1 and 24.7.2 depending on whether you use the console port or Telnet.

Option 5 from **Menu 24 - System Maintenance** allows you to backup the current ZyWALL configuration to your computer. Backup is highly recommended once your ZyWALL is functioning properly. FTP is the preferred method for backing up your current configuration to your computer since it is faster. You can also perform backup and restore using menu 24 through the console port. Any serial communications program should work fine; however, you must use Xmodem protocol to perform the download/upload and you don't have to rename the files.

Please note that terms "download" and "upload" are relative to the computer. Download means to transfer from the ZyWALL to the computer, while upload means from your computer to the ZyWALL.

### 49.3.1 Backup Configuration

Follow the instructions as shown in the next screen.

**Figure 462** Telnet into Menu 24.5

```
Menu 24.5 - Backup Configuration

To transfer the configuration file to your workstation, follow
the procedure below:

   1. Launch the FTP client on your workstation.
   2. Type "open" and the IP address of your router. Then type
"admin" and SMT password as requested.
   3. Locate the 'rom-0' file.
   4. Type 'get rom-0' to back up the current router
configuration to your workstation.

For details on FTP commands, please consult the documentation
of your FTP client program.  For details on backup using TFTP
(note that you must remain in this menu to back up using TFTP),
please see your router manual.
```

## 49.3.2 Using the FTP Command from the Command Line

1. Launch the FTP client on your computer.
2. Enter “open”, followed by a space and the IP address of your ZyWALL.
3. Press [ENTER] when prompted for a username.
4. Enter your password as requested (the default is “1234”).
5. Enter “bin” to set transfer mode to binary.
6. Use “get” to transfer files from the ZyWALL to the computer, for example, “get rom-0 config.rom” transfers the configuration file on the ZyWALL to your computer and renames it “config.rom”. See earlier in this chapter for more information on filename conventions.
7. Enter “quit” to exit the ftp prompt.

## 49.3.3 Example of FTP Commands from the Command Line

**Figure 463** FTP Session Example

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> get rom-0 zyxel.rom
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 16384 bytes sent in 1.10Seconds
297.89Kbytes/sec.
ftp> quit
```

### 49.3.4 GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

**Table 257** General Commands for GUI-based FTP Clients

| COMMAND | DESCRIPTION |
|---|---|
| Host Address | Enter the address of the host server. |
| Login Type | Anonymous.<br>This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option.<br>Normal.<br>The server requires a unique User ID and Password to login. |
| Transfer Type | Transfer files in either ASCII (plain text format) or in binary mode. Configuration and firmware files should be transferred in binary mode |
| Initial Remote Directory | Specify the default remote directory (path). |
| Initial Local Directory | Specify the default local directory (path). |

### 49.3.5 File Maintenance Over WAN

TFTP, FTP and Telnet over the WAN will not work when:

1. The firewall is active (turn the firewall off in menu 21.2 or create a firewall rule to allow access from the WAN).
2. You have disabled Telnet service in menu 24.11.
3. You have applied a filter in menu 3.1 (LAN) or in menu 11.5 (WAN) to block Telnet service.
4. The IP you entered in the **Secure Client IP** field in menu 24.11 does not match the client IP. If it does not match, the ZyWALL will disconnect the Telnet session immediately.
5. You have an SMT console session running.

### 49.3.6 Backup Configuration Using TFTP

The ZyWALL supports the up/downloading of the firmware and the configuration file using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To backup the configuration file, follow the procedure shown next.

1. Use telnet from your computer to connect to the ZyWALL and log in. Because TFTP does not have any security checks, the ZyWALL records the IP address of the telnet client and accepts TFTP requests only from this address.
2. Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.
3. Enter command "`sys stdio 0`" to disable the SMT timeout, so the TFTP transfer will not be interrupted. Enter command "`sys stdio 5`" to restore the five-minute SMT timeout (default) when the file transfer is complete.

4 Launch the TFTP client on your computer and connect to the ZyWALL. Set the transfer mode to binary before starting data transfer.
5 Use the TFTP client (see the example below) to transfer files between the ZyWALL and the computer. The file name for the configuration file is “rom-0” (rom-zero, not capital o).

Note that the telnet connection must be active and the SMT in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use “get” to transfer from the ZyWALL to the computer and “binary” to set binary transfer mode.

### 49.3.7 TFTP Command Example

The following is an example TFTP command:

```
tftp [-i] host get rom-0 config.rom
```

Where “i” specifies binary image transfer mode (use this mode when transferring binary files), “host” is the ZyWALL IP address, “get” transfers the file source on the ZyWALL (rom-0, name of the configuration file on the ZyWALL) to the file destination on the computer and renames it config.rom.

### 49.3.8 GUI-based TFTP Clients

The following table describes some of the fields that you may see in GUI-based TFTP clients.

**Table 258** General Commands for GUI-based TFTP Clients

| COMMAND | DESCRIPTION |
|---|---|
| Host | Enter the IP address of the ZyWALL. 192.168.1.1 is the ZyWALL’s default IP address when shipped. |
| Send/Fetch | Use “Send” to upload the file to the ZyWALL and “Fetch” to back up the file on your computer. |
| Local File | Enter the path and name of the firmware file (*.bin extension) or configuration file (*.rom extension) on your computer. |
| Remote File | This is the filename on the ZyWALL. The filename for the firmware is “ras” and for the configuration file, is “rom-0”. |
| Binary | Transfer the file in binary mode. |
| Abort | Stop transfer of the file. |

Refer to Section 49.3.5 on page 728 to read about configurations that disallow TFTP and FTP over WAN.

### 49.3.9 Backup Via Console Port

Back up configuration via console port by following the HyperTerminal procedure shown next. Procedures using other serial communications programs should be similar.

1 Display menu 24.5 and enter “y” at the following screen.

**Figure 464** System Maintenance: Backup Configuration

```
Ready to backup Configuration via Xmodem.
Do you want to continue (y/n):
```

2 The following screen indicates that the Xmodem download has started.

**Figure 465** System Maintenance: Starting Xmodem Download Screen

```
You can enter ctrl-x to terminate operation any
time.
Starting XMODEM download...
```

3 Run the HyperTerminal program by clicking **Transfer**, then **Receive File** as shown in the following screen.

**Figure 466** Backup Configuration Example


Type a location for storing the configuration file or click **Browse** to look for one.

Choose the **Xmodem** protocol.

Then click **Receive**.

4 After a successful backup you will see the following screen. Press any key to return to the SMT menu.

**Figure 467** Successful Backup Confirmation Screen

```
** Backup Configuration completed. OK.
### Hit any key to continue.###
```

## 49.4 Restore Configuration

This section shows you how to restore a previously saved configuration. Note that this function erases the current configuration before restoring a previous back up configuration; please do not attempt to restore unless you have a backup configuration file stored on disk.

FTP is the preferred method for restoring your current computer configuration to your ZyWALL since FTP is faster. Please note that you must wait for the system to automatically restart after the file transfer is complete.

WARNING!
Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE YOUR ZyWALL. When the Restore Configuration process is complete, the ZyWALL will automatically restart.

## 49.4.1 Restore Using FTP

For details about backup using (T)FTP please refer to earlier sections on FTP and TFTP file upload in this chapter.

**Figure 468** Telnet into Menu 24.6

```
        Menu 24.6 - Restore Configuration

To transfer the firmware and the configuration file, follow the
procedure below:

1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your router.  Then type "admin" and
SMT password as requested.
3. Type "put backupfilename rom-0" where backupfilename is the name of
your backup configuration file on your workstation and rom-spt is the
remote file name on the router. This restores the configuration to
your router.
4. The system reboots automatically after a successful file transfer.

For details on FTP commands, please consult the documentation of your
FTP client program. For details on restoring using TFTP (note that you
must remain on this menu to restore using TFTP), please see your router
manual.
```

1. Launch the FTP client on your computer.
2. Enter “open”, followed by a space and the IP address of your ZyWALL.
3. Press [ENTER] when prompted for a username.
4. Enter your password as requested (the default is “1234”).
5. Enter “bin” to set transfer mode to binary.
6. Find the “rom” file (on your computer) that you want to restore to your ZyWALL.
7. Use “put” to transfer files from the ZyWALL to the computer, for example, “put config.rom rom-0” transfers the configuration file “config.rom” on your computer to the ZyWALL. See earlier in this chapter for more information on filename conventions.
8. Enter “quit” to exit the ftp prompt. The ZyWALL will automatically restart after a successful restore process.

## 49.4.2 Restore Using FTP Session Example

**Figure 469** Restore Using FTP Session Example

```
ftp> put config.rom rom-0
200 Port command okay
150 Opening data connection for STOR rom-0
226 File received OK
221 Goodbye for writing flash
ftp: 16384 bytes sent in 0.06Seconds 273.07Kbytes/sec.
ftp>quit
```

Refer to Section 49.3.5 on page 728 to read about configurations that disallow TFTP and FTP over WAN.

## 49.4.3 Restore Via Console Port

Restore configuration via console port by following the HyperTerminal procedure shown next. Procedures using other serial communications programs should be similar.

1 Display menu 24.6 and enter “y” at the following screen.

**Figure 470** System Maintenance: Restore Configuration

```
Ready to restore Configuration via Xmodem.
Do you want to continue (y/n):
```

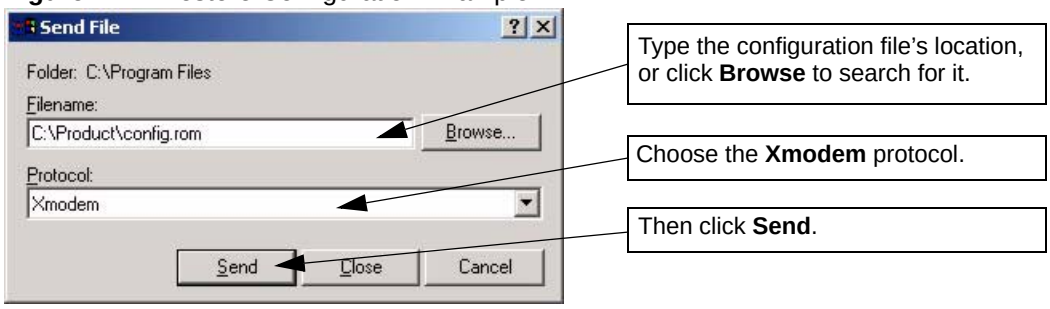
2 The following screen indicates that the Xmodem download has started.

**Figure 471** System Maintenance: Starting Xmodem Download Screen

```
Starting XMODEM download (CRC mode) ...CCCCCCCCC
```

3 Run the HyperTerminal program by clicking **Transfer**, then **Send File** as shown in the following screen.

**Figure 472** Restore Configuration Example



4 After a successful restoration you will see the following screen. Press any key to restart the ZyWALL and return to the SMT menu.

**Figure 473** Successful Restoration Confirmation Screen

```
            Save to ROM
            Hit any key to start system reboot.
```

## 49.5 Uploading Firmware and Configuration Files

This section shows you how to upload firmware and configuration files. You can upload configuration files by following the procedure in Section 49.4 on page 730 or by following the instructions in **Menu 24.7.2 - System Maintenance - Upload System Configuration File** (for console port).

Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE YOUR ZyWALL.

### 49.5.1 Firmware File Upload

FTP is the preferred method for uploading the firmware and configuration. To use this feature, your computer must have an FTP client.

When you telnet into the ZyWALL, you will see the following screens for uploading firmware and the configuration file using FTP.

**Figure 474** Telnet Into Menu 24.7.1: Upload System Firmware

```
 Menu 24.7.1 - System Maintenance - Upload System Firmware

 To upload the system firmware, follow the procedure below:

   1. Launch the FTP client on your workstation.
   2. Type "open" and the IP address of your system.  Then type "admin"
and SMT password as requested.
   3. Type "put firmwarefilename ras" where "firmwarefilename" is the
name of your firmware upgrade file on your workstation and "ras" is the
remote file name on the system.
   4. The system reboots automatically after a successful firmware
upload.

For details on FTP commands, please consult the documentation of your
FTP client program. For details on uploading system firmware using TFTP
(note that you must remain on this menu to upload system firmware using
TFTP), please see your manual.

Press ENTER to Exit:
```

## 49.5.2 Configuration File Upload

You see the following screen when you telnet into menu 24.7.2.

**Figure 475** Telnet Into Menu 24.7.2: System Maintenance

```
Menu 24.7.2 - System Maintenance - Upload System Configuration File

  To upload the system configuration file, follow the procedure below:

    1. Launch the FTP client on your workstation.
    2. Type "open" and the IP address of your system. Then type "admin"
and SMT password as requested.
    3. Type "put configurationfilename rom-0" where
"configurationfilename" is the name of your system configuration file on
your workstation, which will be transferred to the "rom-0" file on the
system.
    4. The system reboots automatically after the upload system
configuration file process is complete.

For details on FTP commands, please consult the documentation of your
FTP client program. For details on uploading configuration file using
TFTP (note that you must remain on this menu to upload configuration
file using TFTP), please see your manual.

Press ENTER to Exit:
```

To upload the firmware and the configuration file, follow these examples

### 49.5.3 FTP File Upload Command from the DOS Prompt Example

1. Launch the FTP client on your computer.
2. Enter “open”, followed by a space and the IP address of your ZyWALL.
3. Press [ENTER] when prompted for a username.
4. Enter your password as requested (the default is “1234”).
5. Enter “bin” to set transfer mode to binary.
6. Use “put” to transfer files from the computer to the ZyWALL, for example, “put firmware.bin ras” transfers the firmware on your computer (firmware.bin) to the ZyWALL and renames it “ras”. Similarly, “put config.rom rom-0” transfers the configuration file on your computer (config.rom) to the ZyWALL and renames it “rom-0”. Likewise “get rom-0 config.rom” transfers the configuration file on the ZyWALL to your computer and renames it “config.rom.” See earlier in this chapter for more information on filename conventions.
7. Enter “quit” to exit the ftp prompt.

### 49.5.4 FTP Session Example of Firmware File Upload

**Figure 476** FTP Session Example of Firmware File Upload

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> put firmware.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 1103936 bytes sent in 1.10Seconds
297.89Kbytes/sec.
ftp> quit
```

More commands (found in GUI-based FTP clients) are listed earlier in this chapter.

Refer to Section 49.3.5 on page 728 to read about configurations that disallow TFTP and FTP over WAN.

### 49.5.5 TFTP File Upload

The ZyWALL also supports the uploading of firmware files using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To transfer the firmware and the configuration file, follow the procedure shown next.

1. Use telnet from your computer to connect to the ZyWALL and log in. Because TFTP does not have any security checks, the ZyWALL records the IP address of the telnet client and accepts TFTP requests only from this address.

2. Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.
3. Enter the command "`sys stdio 0`" to disable the console timeout, so the TFTP transfer will not be interrupted. Enter "`command sys stdio 5`" to restore the five-minute console timeout (default) when the file transfer is complete.
4. Launch the TFTP client on your computer and connect to the ZyWALL. Set the transfer mode to binary before starting data transfer.
5. Use the TFTP client (see the example below) to transfer files between the ZyWALL and the computer. The file name for the firmware is "ras".

Note that the telnet connection must be active and the ZyWALL in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use "get" to transfer from the ZyWALL to the computer, "put" the other way around, and "binary" to set binary transfer mode.

## 49.5.6 TFTP Upload Command Example

The following is an example TFTP command:

```
tftp [-i] host put firmware.bin ras
```

Where "i" specifies binary image transfer mode (use this mode when transferring binary files), "host" is the ZyWALL's IP address, "put" transfers the file source on the computer (firmware.bin – name of the firmware on the computer) to the file destination on the remote host (ras - name of the firmware on the ZyWALL).

Commands that you may see in GUI-based TFTP clients are listed earlier in this chapter.

## 49.5.7 Uploading Via Console Port

FTP or TFTP are the preferred methods for uploading firmware to your ZyWALL. However, in the event of your network being down, uploading files is only possible with a direct connection to your ZyWALL via the console port. Uploading files via the console port under normal conditions is not recommended since FTP or TFTP is faster. Any serial communications program should work fine; however, you must use the Xmodem protocol to perform the download/upload.

## 49.5.8 Uploading Firmware File Via Console Port

1. Select 1 from **Menu 24.7 – System Maintenance – Upload Firmware** to display **Menu 24.7.1 - System Maintenance - Upload System Firmware**, and then follow the instructions as shown in the following screen.

**Figure 477** Menu 24.7.1 As Seen Using the Console Port

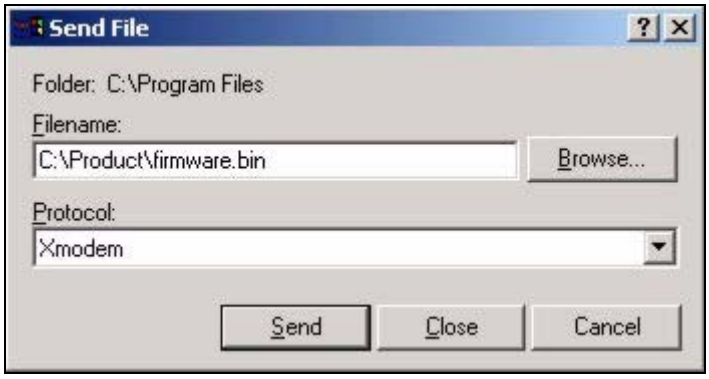
```
        Menu 24.7.1 - System Maintenance - Upload System Firmware

   To upload system firmware:
   1. Enter "y" at the prompt below to go into debug mode.
   2. Enter "atur" after "Enter Debug Mode" message.
   3. Wait for "Starting XMODEM upload" message before activating
   Xmodem upload on your terminal.
   4. After successful firmware upload, enter "atgo" to restart the router.

   Warning: Proceeding with the upload will erase the current system
   firmware.

           Do You Wish To Proceed:(Y/N)
```

2 After the "Starting Xmodem upload" message appears, activate the Xmodem protocol on your computer. Follow the procedure as shown previously for the HyperTerminal program. The procedure for other serial communications programs should be similar.

## 49.5.9 Example Xmodem Firmware Upload Using HyperTerminal

Click **Transfer**, then **Send File** to display the following screen.

**Figure 478** Example Xmodem Upload




After the firmware upload process has completed, the ZyWALL will automatically restart.

## 49.5.10 Uploading Configuration File Via Console Port

1 Select 2 from **Menu 24.7 – System Maintenance – Upload Firmware** to display **Menu 24.7.2 - System Maintenance - Upload System Configuration File**. Follow the instructions as shown in the next screen.

**Figure 479** Menu 24.7.2 As Seen Using the Console Port

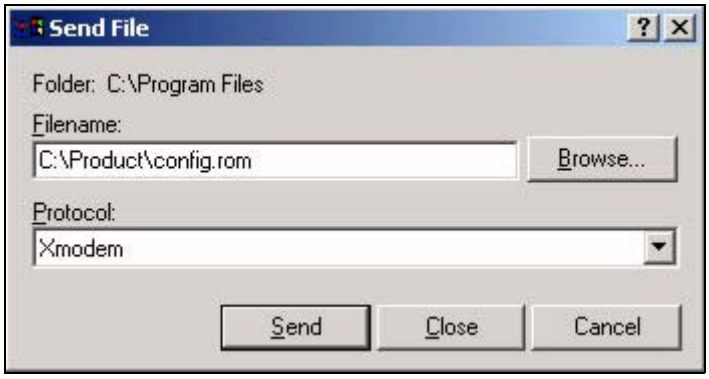
```
Menu 24.7.2 - System Maintenance - Upload System Configuration File

To upload system configuration file:
1. Enter "y" at the prompt below to go into debug mode.
2. Enter "atlc" after "Enter Debug Mode" message.
3. Wait for "Starting XMODEM upload" message before activating
   Xmodem upload on your terminal.
4. After successful firmware upload, enter "atgo" to restart
   the system.

Warning:
1. Proceeding with the upload will erase the current
configuration file.
2. The system's console port speed (Menu 24.2.2) may change when it is
restarted; please adjust your terminal's speed accordingly. The password
may change (menu 23), also.
3. When uploading the DEFAULT configuration file, the console
port speed will be reset to 9600 bps and the password to "1234".

         Do You Wish To Proceed:(Y/N)
```

2. After the "Starting Xmodem upload" message appears, activate the Xmodem protocol on your computer. Follow the procedure as shown previously for the HyperTerminal program. The procedure for other serial communications programs should be similar.
3. Enter “atgo” to restart the ZyWALL.

## 49.5.11 Example Xmodem Configuration Upload Using HyperTerminal

Click **Transfer**, then **Send File** to display the following screen.

**Figure 480** Example Xmodem Upload




After the configuration upload process has completed, restart the ZyWALL by entering “atgo”.

# 50

# System Maintenance Menus 8 to 10

This chapter leads you through SMT menus 24.8 to 24.10.

## 50.1 Command Interpreter Mode

The Command Interpreter (CI) is a part of the main router firmware. The CI provides much of the same functionality as the SMT, while adding some low-level setup and diagnostic functions. Enter the CI from the SMT by selecting menu 24.8. Access can be by Telnet or by a serial connection to the console port, although some commands are only available with a serial connection. See the CLI Reference Guide for information on the commands. Enter 8 from **Menu 24 - System Maintenance**.

Use of undocumented commands or misconfiguration can damage the unit and possibly render it unusable.

**Figure 481** Command Mode in Menu 24

```
            Menu 24 - System Maintenance

               1.  System Status
               2.  System Information and Console Port Speed
               3.  Log and Trace
               4.  Diagnostic
               5.  Backup Configuration
               6.  Restore Configuration
               7.  Upload Firmware
               8.  Command Interpreter Mode
               9.  Call Control
               10. Time and Date Setting
               11. Remote Management Setup


            Enter Menu Selection Number:
```

# 50.2 Call Control Support

The ZyWALL provides two call control functions: budget management and call history. Please note that this menu is only applicable when **Encapsulation** is set to **PPPoE** or **PPTP** in menu 4 or menu 11.1.

The budget management function allows you to set a limit on the total outgoing call time of the ZyWALL within certain times. When the total outgoing call time exceeds the limit, the current call will be dropped and any future outgoing calls will be blocked.

Call history chronicles preceding incoming and outgoing calls.

To access the call control menu, select option 9 in menu 24 to go to **Menu 24.9 - System Maintenance - Call Control**, as shown in the next table.

**Figure 482** Call Control

```
            Menu 24.9 - System Maintenance - Call Control

                1.Budget Management
                2.Call History

            Enter Menu Selection Number:
```

## 50.2.1 Budget Management

Menu 24.9.1 shows the budget management statistics for outgoing calls. Enter 1 from **Menu 24.9 - System Maintenance - Call Control** to bring up the following menu. Not all fields are available on all models.

**Figure 483** Budget Management

```
             Menu 24.9.1 - Budget Management

   Remote Node   Connection Time/Total Budget   Elapsed Time/Total Period

 1.WAN_1                  No Budget                  No Budget

 2.WAN_2                  No Budget                  No Budget

 3.Dial                   No Budget                  No Budget


              Reset Node (0 to update screen):
```

The total budget is the time limit on the accumulated time for outgoing calls to a remote node. When this limit is reached, the call will be dropped and further outgoing calls to that remote node will be blocked. After each period, the total budget is reset. The default for the total budget is 0 minutes and the period is 0 hours, meaning no budget control. You can reset the accumulated connection time in this menu by entering the index of a remote node. Enter 0 to update the screen. The budget and the reset period can be configured in menu 11.1 for the remote node.

**Table 259** Budget Management

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| Remote Node | Enter the index number of the remote node you want to reset (just one in this case) | 1 |
| Connection Time/ Total Budget | This is the total connection time that has gone by (within the allocated budget that you set in menu 11.1). | 5/10 means that 5 minutes out of a total allocation of 10 minutes have lapsed. |
| Elapsed Time/Total Period | The period is the time cycle in hours that the allocation budget is reset (see menu 11.1.) The elapsed time is the time used up within this period. | 0.5/1 means that 30 minutes out of the 1-hour time period has lapsed. |
| Enter “0” to update the screen or press [ESC] to return to the previous screen. | | |

## 50.2.2 Call History

This is the second option in **Menu 24.9 - System Maintenance - Call Control**. It displays information about past incoming and outgoing calls. Enter 2 from **Menu 24.9 - System Maintenance - Call Control** to bring up the following menu.

**Figure 484** Call History

```
Menu 24.9.2 - Call History

    Phone Number   Dir    Rate    #call   Max   Min  Total
 1.
 2.
 3.
 4.
 5.
 6.
 7.
 8.
 9.
10.

Enter Entry to Delete(0 to exit):
```

The following table describes the fields in this screen.

**Table 260** Call History

| FIELD | DESCRIPTION |
|---|---|
| Phone Number | The PPPoE service names are shown here. |
| Dir | This shows whether the call was incoming or outgoing. |

**Table 260** Call History

| FIELD | DESCRIPTION |
|---|---|
| Rate | This is the transfer rate of the call. |
| #call | This is the number of calls made to or received from that telephone number. |
| Max | This is the length of time of the longest telephone call. |
| Min | This is the length of time of the shortest telephone call. |
| Total | This is the total length of time of all the telephone calls to/from that telephone number. |
| You may enter an entry number to delete it or ‘”0” to exit. | |

## 50.3 Time and Date Setting

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 when you turn on your ZyWALL. Menu 24.10 allows you to update the time and date settings of your ZyWALL. The real time is then displayed in the ZyWALL error logs and firewall logs.

Select menu 24 in the main menu to open **Menu 24 - System Maintenance**, as shown next.

**Figure 485** Menu 24: System Maintenance

```
                Menu 24 - System Maintenance

          1.  System Status
          2.  System Information and Console Port Speed
          3.  Log and Trace
          4.  Diagnostic
          5.  Backup Configuration
          6.  Restore Configuration
          7.  Upload Firmware
          8.  Command Interpreter Mode
          9.  Call Control
         10. Time and Date Setting
         11. Remote Management Setup


             Enter Menu Selection Number:
```

Enter 10 to go to **Menu 24.10 - System Maintenance - Time and Date Setting** to update the time and date settings of your ZyWALL as shown in the following screen.

**Figure 486** Menu 24.10 System Maintenance: Time and Date Setting

```
            Menu 24.10 - System Maintenance - Time and Date Setting

            Time Protocol= NTP (RFC-1305)
            Time Server Address= 0.pool.ntp.org

            Current Time:                          08 : 24 : 26
            New Time (hh:mm:ss):                   N/A  N/A  N/A

            Current Date:                          2005 - 07 - 27
            New Date (yyyy-mm-dd):                 N/A    N/A  N/A

            Time Zone= GMT

            Daylight Saving= No
            Start Date (mm-nth-week-hr):           Jan. - 1st  - Sun. -  00
            End Date (mm-nth-week-hr):             Jan. - 1st  - Sun. -  00


              Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this screen.

**Table 261** Menu 24.10 System Maintenance: Time and Date Setting

| FIELD | DESCRIPTION |
|---|---|
| Time Protocol | Enter the time service protocol that your timeserver uses. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main differences between them are the format.<br>**Daytime (RFC 867)** format is day/month/year/time zone of the server.<br>**Time (RFC-868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0.<br>The default, **NTP (RFC-1305)**, is similar to **Time (RFC-868)**.<br>Select **Manual** to enter the new time and new date manually. |
| Time Server Address | Enter the IP address or domain name of your timeserver. Check with your ISP/ network administrator if you are unsure of this information. |
| Current Time | This field displays an updated time only when you reenter this menu. |
| New Time | Enter the new time in hour, minute and second format. This field is available when you select **Manual** in the **Time Protocol** field. |
| Current Date | This field displays an updated date only when you reenter this menu. |
| New Date | Enter the new date in year, month and day format. This field is available when you select **Manual** in the **Time Protocol** field. |
| Time Zone | Press [SPACE BAR] and then [ENTER] to set the time difference between your time zone and Greenwich Mean Time (GMT). |
| Daylight Saving | Daylight Saving Time 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 daylight time in the evenings. If you use daylight savings time, then choose **Yes**. |

**Table 261** Menu 24.10 System Maintenance: Time and Date Setting

| FIELD | DESCRIPTION |
|---|---|
| Start Date (mm-nth-week-hr) | Configure the day and time when Daylight Saving Time starts if you selected **Yes** in the **Daylight Saving** field. The **hr** 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 **Mar.**, **2nd**, **Sun.** and type 02 in the **hr** 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 **Mar.**, **Last**, **Sun.** The time you type in the **hr** field depends on your time zone. In Germany for instance, you would type 02 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1). |
| End Date (mm-nth-week-hr) | Configure the day and time when Daylight Saving Time ends if you selected **Yes** in the **Daylight Saving** field. The **hr** field uses the 24 hour format. Here are a couple of examples:<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 **Nov.**, **First**, **Sun.** and type 02 in the **hr** field.<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 **Oct.**, **Last**, **Sun.** The time you type in the **hr** field depends on your time zone. In Germany for instance, you would type 02 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1). |
| Once you have filled in this menu, press [ENTER] at the message “Press ENTER to Confirm or ESC to Cancel“ to save your configuration, or press [ESC] to cancel. | |

# 51

# Remote Management

This chapter covers remote management found in SMT menu 24.11.

## 51.1 Remote Management

Remote management allows you to determine which services/protocols can access which ZyWALL interface (if any) from which computers.

When you configure remote management to allow management from any network except the LAN, you still need to configure a firewall rule to allow access. See Chapter 13 on page 251 for details on configuring firewall rules.

You can also disable a service on the ZyWALL by not allowing access for the service/protocol through any of the ZyWALL interfaces.

To disable remote management of a service, select **Disable** in the corresponding **Access** field.

Enter 11 from menu 24 to bring up **Menu 24.11 - Remote Management Control**.

**Figure 487** Menu 24.11 – Remote Management Control

```
                Menu 24.11 - Remote Management Control

     TELNET Server:     Port = 23         Access = Disable
                        Secure Client IP = 0.0.0.0
     FTP Server:        Port = 21         Access = LAN+WAN1+DMZ+WLAN+WAN2
                        Secure Client IP = 0.0.0.0
     SSH Server:        Certificate = auto_generated_self_signed_cert
                        Port = 22         Access = LAN+WAN1+DMZ+WLAN+WAN2
                        Secure Client IP = 0.0.0.0
     HTTPS Server:      Certificate = auto_generated_self_signed_cert
                        Authenticate Client Certificates = No
                        Port = 443        Access = LAN+WAN1+DMZ+WLAN+WAN2
                        Secure Client IP = 0.0.0.0
     HTTP Server:       Port = 80         Access = LAN+WAN1+DMZ+WLAN+WAN2
                        Secure Client IP = 0.0.0.0
     SNMP Service:      Port = 161        Access = LAN+WAN1+DMZ+WLAN+WAN2
                        Secure Client IP = 0.0.0.0
     DNS Service:       Port = 53         Access = LAN+WAN1+DMZ+WLAN+WAN2
                        Secure Client IP = 0.0.0.0

                Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this screen.

**Table 262** Menu 24.11 – Remote Management Control

| FIELD | DESCRIPTION |
|---|---|
| Telnet Server<br>FTP Server<br>SSH Server<br>HTTPS Server<br>HTTP Server<br>SNMP Service<br>DNS Service | Each of these read-only labels denotes a service that you may use to remotely manage the ZyWALL. |
| Port | This field shows the port number for the service or protocol. You may change the port number if needed, but you must use the same port number to access the ZyWALL. |
| Access | Select the access interface (if any) by pressing [SPACE BAR], then [ENTER] to choose from: **LAN**, **WAN**, **LAN+WAN**, **DMZ**, **LAN+DMZ**, **WAN+DMZ**, **LAN+WAN+DMZ**, **WLAN**, **LAN+WLAN**, **WAN+WLAN**, **LAN+WAN+WLAN**, **DMZ+WLAN**, **LAN+DMZ+WLAN**, **WAN+DMZ+WLAN**, **LAN+WAN+DMZ+WLAN** or **Disable**. |
| Secure Client IP | The default 0.0.0.0 allows any client to use this service to remotely manage the ZyWALL. Enter an IP address to restrict access to a client with a matching IP address. |
| Certificate | Press [SPACE BAR] and then [ENTER] to select the certificate that the ZyWALL will use to identify itself. The ZyWALL is the SSL server and must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the ZyWALL). |

**Table 262** Menu 24.11 – Remote Management Control (continued)

| FIELD | DESCRIPTION |
|---|---|
| Authenticate Client Certificates | Select **Yes** by pressing [SPACE BAR], then [ENTER] 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 27.2.5 on page 496 for details). |
| Once you have filled in this menu, press [ENTER] at the message "Press ENTER to Confirm or ESC to Cancel" to save your configuration, or press [ESC] to cancel. | |

## 51.1.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

1. A filter in menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a Telnet, FTP or Web service.
2. You have disabled that service in menu 24.11.
3. The IP address in the **Secure Client IP** field (menu 24.11) does not match the client IP address. If it does not match, the ZyWALL will disconnect the session immediately.
4. There is an SMT console session running.
5. There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.
6. There is a firewall rule that blocks it.

# 52

# IP Policy Routing

This chapter covers setting and applying policies used for IP routing.

## 52.1 IP Routing Policy Summary

Menu 25 shows the summary of a policy rule, including the criteria and the action of a single policy, and whether a policy is active or not. Each policy contains two lines. The former part is the criteria of the incoming packet and the latter is the action. Between these two parts, separator "|" means the action is taken on criteria matched and separator "=" means the action is taken on criteria not matched.

**Figure 488** Menu 25: Sample IP Routing Policy Summary

```
                    Menu 25 - IP Routing Policy Summary

#   A                         Criteria/Action
--- - ------------------------------------------------------
001 N SA=1.1.1.1-1.1.1.1 DA=2.2.2.2-2.2.2.5
      SP=20-25 DP=20-25 P=6 T=NM PR=0      |GW=192.168.1.1 T=MT PR=0
002 N ____________________________________________________________
      ____________________________________________________________
003 N ____________________________________________________________
      ____________________________________________________________
004 N ____________________________________________________________
      ____________________________________________________________
005 N ____________________________________________________________
      ____________________________________________________________
006 N ____________________________________________________________
      ____________________________________________________________

             Select Command= None           Select Rule= N/A
                   Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

The following table describes the fields in this screen.

**Table 263** Menu 25: Sample IP Routing Policy Summary

| FIELD | DESCRIPTION |
|---|---|
| # | This is the policy index number. |
| A | This displays whether a policy is active (**Y**) or not (**N**). |

**Table 263** Menu 25: Sample IP Routing Policy Summary (continued)

| FIELD | DESCRIPTION |
|---|---|
| Criteria/Action | This displays the details about to which packets the policy applies and how the policy has the ZyWALL handle those packets. Refer to Table 264 on page 750 for detailed information. |
| Select Command | Press [SPACE BAR] to choose from **None**, **Edit**, **Delete**, **Go To Rule**, **Next Page** or **Previous Page** and then press [ENTER]. You must select a rule in the next field when you choose the **Edit**, **Delete** or **Go To** commands.<br>Select **None** and then press [ENTER] to go to the "Press ENTER to Confirm…" prompt.<br>Use **Edit** to create or edit a rule. Use **Delete** to remove a rule. To edit or delete a rule, first make sure you are on the correct page. When a rule is deleted, subsequent rules do not move up in the page list.<br>Use **Go To Rule** to view the page where your desired rule is listed.<br>Select **Next Page** or **Previous Page** to view the next or previous page of rules (respectively). |
| Select Rule | Type the policy index number you wish to edit or delete and then press [ENTER]. |
| When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel. | |

**Table 264** IP Routing Policy Setup

| ABBREVIATION | | MEANING |
|---|---|---|
| **Criterion** | SA | Source IP Address |
| SP | | Source Port |
| DA | | Destination IP Address |
| DP | | Destination Port |
| P | | IP layer 4 protocol number (TCP=6, UDP=17…) |
| T | | Type of service of incoming packet |
| PR | | Precedence of incoming packet |
| **Action** | GW | Gateway IP address |
| T | | Outgoing Type of service |
| P | | Outgoing Precedence |
| **Service** | NM | Normal |
| MD | | Minimum Delay |
| MT | | Maximum Throughput |
| MR | | Maximum Reliability |
| MC | | Minimum Cost |

## 52.2 IP Routing Policy Setup

To setup a routing policy, perform the following procedures:

1 Type 25 in the main menu to open **Menu 25 - IP Routing Policy Summary**.

2 Select **Edit** in the **Select Command** field; type the index number of the rule you want to configure in the **Select Rule** field and press [ENTER] to open **Menu 25.1 - IP Routing Policy Setup** (see the next figure).

**Figure 489** Menu 25.1: IP Routing Policy Setup

```
            Menu 25.1 - IP Routing Policy Setup

     Rule Index= 1                            Active= Yes
     Criteria:
       IP Protocol    = 6
       Type of Service= Normal                Packet length= 40
       Precedence     = 0                       Len Comp= Equal
       Source:
         addr start= 1.1.1.1                  end= 1.1.1.1
         port start= 20                       end= 25
       Destination:
         addr start= 2.2.2.2                  end= 2.2.2.5
         port start= 20                       end= 25
      Action= Matched
        Gateway Type= IP Address
        Gateway addr   = 192.168.1.1          Redirect packet= N/A
        Type of Service= Max Thruput          Log= No
        Precedence     = 0
     Edit policy to packets received from= No

                        Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this screen.

**Table 265** Menu 25.1: IP Routing Policy Setup

| FIELD | DESCRIPTION |
|---|---|
| Rule Index | This is the index number of the routing policy selected in **Menu 25 - IP Routing Policy Summary**. |
| Active | Press [SPACE BAR] and then [ENTER] to select **Yes** to activate the policy. |
| Criteria | |
| IP Protocol | Enter a number that represents an IP layer 4 protocol, for example, UDP=17, TCP=6, ICMP=1 and Don't care=0. |
| Type of Service | Prioritize incoming network traffic by choosing from **Don't Care**, **Normal**, **Min Delay**, **Max Thruput** or **Max Reliable**. |
| Precedence | Precedence value of the incoming packet. Press [SPACE BAR] and then [ENTER] to select a value from **0** to **7** or **Don't Care**. |
| Packet Length | Type the length of incoming packets (in bytes). The operators in the **Len Comp** (next field) apply to packets of this length. |
| Len Comp | Press [SPACE BAR] and then [ENTER] to choose from **Equal**, **Not Equal**, **Less**, **Greater**, **Less or Equal** or **Greater or Equal**. |
| Source | |
| addr start / end | Source IP address range from start to end. |
| port start / end | Source port number range from start to end; applicable only for TCP/UDP. |
| Destination | |

**Table 265** Menu 25.1: IP Routing Policy Setup

| FIELD | DESCRIPTION |
|---|---|
| addr start / end | Destination IP address range from start to end. |
| port start / end | Destination port number range from start to end; applicable only for TCP/UDP. |
| Action | Specifies whether action should be taken on criteria Matched or Not Matched. |
| Gateway Type | Press [SPACE BAR] and then [ENTER] to select **IP Address** and enter the IP address of the gateway if you want to specify the IP address of the gateway. The gateway is an immediate neighbor of your ZyWALL that will forward the packet to the destination. The gateway must be a router on the same segment as your ZyWALL's LAN or WAN port.<br>Press [SPACE BAR] and then [ENTER] to select **Remote Node** to have the ZyWALL send traffic that matches the policy route through a specific WAN port. |
| Gateway addr | This field displays if you selected **IP Address** in the **Gateway Type** field. Defines the outgoing gateway address. The gateway must be on the same subnet as the ZyWALL if it is on the LAN, otherwise, the gateway must be the IP address of a remote node. The default gateway is specified as 0.0.0.0. |
| Remote Node Idx | This field displays if you selected **Remote Node** in the **Gateway Type** field. Type **1** for WAN port 1 or 2 for WAN port 2. |
| Redirect Packet | This field applies if you selected **Remote Node** in the **Gateway Type** field.<br>Press [SPACE BAR] and then [ENTER] to select **Yes** to have the ZyWALL send traffic that matches the policy route through the other WAN interface if it cannot send the traffic through the WAN interface you selected. |
| Type of Service | Set the new TOS value of the outgoing packet. Prioritize incoming network traffic by choosing **Don't Care**, **Normal**, **Min Delay**, **Max Thruput**, **Max Reliable** or **Min Cost**. |
| Precedence | Set the new outgoing packet precedence value. Values are **0** to **7** or **Don't Care**. |
| Log | Press [SPACE BAR] and then [ENTER] to select **Yes** to make an entry in the system log when a policy is executed. |
| Edit policy to packets received from | Press [SPACE BAR] and then [ENTER] to select **Yes** or **No** (default). Select **Yes** to configure Menu 25.1.1: IP Routing Policy Setup discussed next. |
| When you have completed this menu, press [ENTER] at the prompt "Press [ENTER] to confirm or [ESC] to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen. | |

## 52.2.1 Applying Policy to Packets

To apply the policy to packets received on the selected interface(s), go to **Menu 25.1: IP Routing Policy Setup** and press [SPACE BAR] to select **Yes** in the **Edit policy to packets received from** field. Press [ENTER] to display **Menu 25.1.1 - IP Routing Policy Setup** (shown next).

**Figure 490** Menu 25.1.1: IP Routing Policy Setup

```
            Menu 25.1.1 - IP Routing Policy Setup

                       Apply policy to packets received from:
                         LAN= No
                         DMZ= No
                         WLAN= No
                         ALL WAN= Yes
                           Selected Remote Node index= N/A

          Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this screen.

**Table 266** Menu 25.1.1: IP Routing Policy Setup

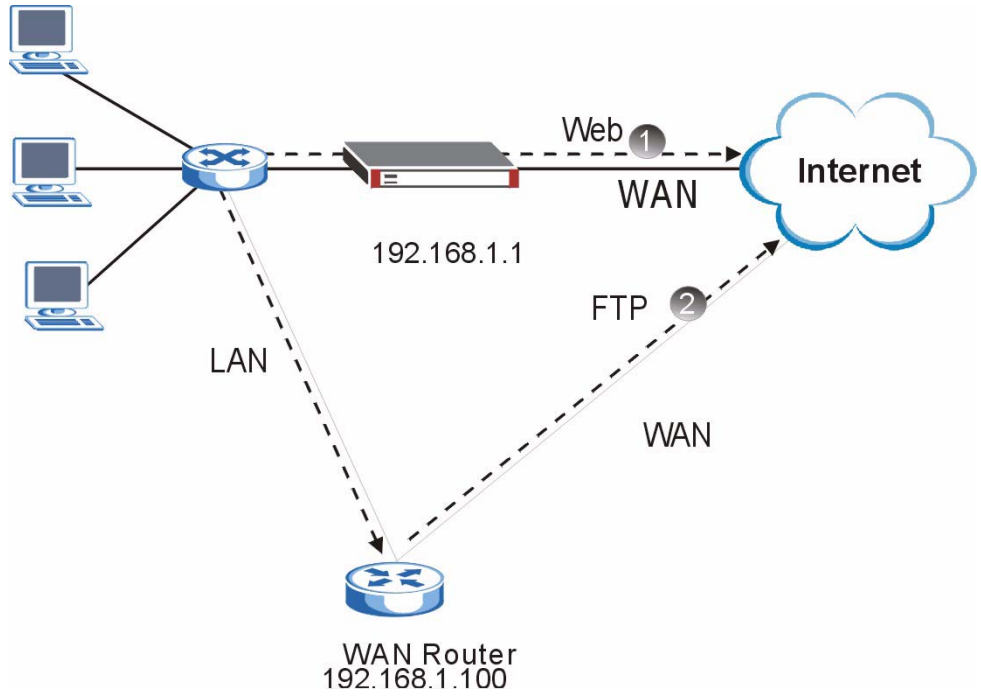
| FIELD | DESCRIPTION |
|---|---|
| LAN/DMZ/WLAN/ ALL WAN | Press [SPACE BAR] to select **Yes** or **No**. Choose **Yes** and press [ENTER] to apply the policy to packets received on the specific interface(s). |
| Selected Remote Node index | If you select **No** in the **ALL WAN** field, enter the number of the WAN interface. |
| When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel. | |

## 52.3 IP Policy Routing Example

If a network has both Internet and remote node connections, you can route Web packets to the Internet using one policy and route FTP packets to a remote network using another policy. See the next figure.

Route 1 represents the default IP route and route 2 represents the configured IP route.

**Figure 491** Example of IP Policy Routing




To force Web packets coming from clients with IP addresses of 192.168.1.33 to 192.168.1.64 to be routed to the Internet via the WAN port of the ZyWALL, follow the steps as shown next.

**1** Create a rule in **Menu 25.1 - IP Routing Policy Setup** as shown next.

**Figure 492** IP Routing Policy Example 1

```
            Menu 25.1 - IP Routing Policy Setup

            Rule Index= 1                              Active= Yes
            Criteria:
              IP Protocol    = 6
              Type of Service= Don't Care              Packet length= 10
              Precedence     = Don't Care                Len Comp= Equal
              Source:
                addr start= 192.168.1.33       end= 192.168.1.64
                port start= 0                  end= N/A
              Destination:
                addr start= 0.0.0.0                    end= N/A
                port start= 80                         end= 80
            Action= Matched
               Gateway Type= IP Address
               Gateway addr   = 192.168.1.1             Redirect packet= N/A
               Type of Service= Max Thruput             Log= No
               Precedence     = 0
            Edit policy to packets received from= No

                                Press ENTER to Confirm or ESC to Cancel:
```

2 Select **Yes** in the **LAN** field in menu 25.1.1 to apply the policy to packets received on the LAN port.
3 Check **Menu 25 - IP Routing Policy Summary** to see if the rule is added correctly.
4 Create another rule in menu 25.1 for this rule to route packets from any host (IP=0.0.0.0 means any host) with protocol TCP and port FTP access through another gateway (192.168.1.100).

**Figure 493** IP Routing Policy Example 2

```
 Menu 25.1 - IP Routing Policy Setup

Rule Index= 2                              Active= No
Criteria:
  IP Protocol    = 6
  Type of Service= Don't Care              Packet length= 10
  Precedence     = Don't Care                Len Comp= Equal
  Source:
    addr start= 0.0.0.0                    end= N/A
    port start= 0                          end= N/A
  Destination:
    addr start= 0.0.0.0                    end= N/A
    port start= 20                         end= 21
Action= Matched
   Gateway Type= IP Address
   Gateway addr   = 192.168.1.100     Redirect packet= N/A
   Type of Service= Don't Care        Log= No
   Precedence     = Don't Care
Edit policy to packets received from= No

                     Press ENTER to Confirm or ESC to Cancel:
```

5 Select **Yes** in the **LAN** field in menu 25.1.1 to apply the policy to packets received on the LAN port.
6 Check **Menu 25 - IP Routing Policy Summary** to see if the rule is added correctly.

# 53

# Call Scheduling

Call scheduling allows you to dictate when a remote node should be called and for how long.

## 53.1 Introduction to Call Scheduling

The call scheduling feature allows the ZyWALL to manage a remote node and dictate when a remote node should be called and for how long. This feature is similar to the scheduler in a video cassette recorder (you can specify a time period for the VCR to record). You can apply up to 4 schedule sets in **Menu 11.1 - Remote Node Profile**. From the main menu, enter 26 to access **Menu 26 - Schedule Setup** as shown next.

**Figure 494** Schedule Setup

```
                    Menu 26 - Schedule Setup

Schedule                          Schedule
Set #     Name                    Set #     Name
------    --------------------    ------    --------------------
1         ____________________    7         ____________________
2         ____________________    8         ____________________
3         ____________________    9         ____________________
4         ____________________    10        ____________________
5         ____________________    11        ____________________
6         ____________________    12        ____________________

Enter Schedule Set Number to Configure= 0
Edit Name= N/A
Press ENTER to Confirm or ESC to Cancel:
```

Lower numbered sets take precedence over higher numbered sets thereby avoiding scheduling conflicts. For example, if sets 1, 2, 3 and 4 are applied in the remote node, then set 1 will take precedence over set 2, 3 and 4 as the ZyWALL, by default, applies the lowest numbered set first. Set 2 will take precedence over set 3 and 4, and so on.

You can design up to 12 schedule sets but you can only apply up to four schedule sets for a remote node.

To delete a schedule set, enter the set number and press [SPACE BAR] and then [ENTER] or [DEL] in the Edit Name field.

To set up a schedule set, select the schedule set you want to setup from menu 26 (1-12) and press [ENTER] to see **Menu 26.1 - Schedule Set Setup** as shown next.

**Figure 495** Schedule Set Setup

```
            Menu 26.1 - Schedule Set Setup

            Active= Yes
            How Often= Once
            Start Date(yyyy-mm-dd) = N/A
            Once:
              Date(yyyy-mm-dd)= 2000 - 01 - 01
            Weekdays:
              Sunday= N/A
              Monday= N/A
              Tuesday= N/A
              Wednesday= N/A
              Thursday= N/A
              Friday= N/A
              Saturday= N/A
            Start Time (hh:mm)= 00 : 00
            Duration (hh:mm)= 00 : 00
            Action= Forced On

            Press ENTER to Confirm or ESC to Cancel:
            Press Space Bar to Toggle
```

If a connection has been already established, your ZyWALL will not drop it. Once the connection is dropped manually or it times out, then that remote node can't be triggered up until the end of the **Duration**.

**Table 267** Schedule Set Setup

| FIELD | DESCRIPTION |
|---|---|
| Active | Press [SPACE BAR] to select **Yes** or **No**. Choose **Yes** and press [ENTER] to activate the schedule set. |
| How Often | Should this schedule set recur weekly or be used just once only? Press [SPACE BAR] and then [ENTER] to select **Once** or **Weekly**. Both these options are mutually exclusive. If **Once** is selected, then all weekday settings are **N/A**. When **Once** is selected, the schedule rule deletes automatically after the scheduled time elapses. |
| Start Date | Enter the start date when you wish the set to take effect in year -month-date format. Valid dates are from the present to 2036-February-5. |
| Once: | |
| Date | If you selected **Once** in the **How Often** field above, then enter the date the set should activate here in year-month-date format. |
| Weekdays: | |

**Table 267** Schedule Set Setup (continued)

| FIELD | DESCRIPTION |
|---|---|
| Day | If you selected **Weekly** in the **How Often** field above, then select the day(s) when the set should activate (and recur) by going to that day(s) and pressing [SPACE BAR] to select **Yes**, then press [ENTER]. |
| Start Time | Enter the start time when you wish the schedule set to take effect in hour-minute format. |
| Duration | The duration determines how long the ZyWALL is to apply the action configured in the **Action** field. Enter the maximum length of time in hour-minute format. |
| Action | **Forced On** means that the connection is maintained whether or not there is a demand call on the line and will persist for the time period specified in the **Duration** field.<br>**Forced Down** means that the connection is blocked whether or not there is a demand call on the line.<br>**Enable Dial-On-Demand** means that this schedule permits a demand call on the line.<br>**Disable Dial-On-Demand** means that this schedule prevents a demand call on the line. |
| When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel. | |

Once your schedule sets are configured, you must then apply them to the desired remote node(s). Enter 11 from the Main Menu and then enter the target remote node index. Press [SPACE BAR] and then [ENTER] to select **PPPoE** in the **Encapsulation** field to make the schedule sets field available as shown next.

**Figure 496** Applying Schedule Set(s) to a Remote Node (PPPoE)

```
                    Menu 11.1 - Remote Node Profile

          Rem Node Name= ChangeMe        Route= IP
          Active= Yes

          Encapsulation= PPPoE           Edit IP= No
          Service Type= Standard         Telco Option:
          Service Name=                    Allocated Budget(min)= 0
          Outgoing=                        Period(hr)= 0
            My Login=                      Schedules= 1,2,3,4
            My Password= ********          Nailed-Up Connection= No
            Authen= CHAP/PAP
                                         Session Options:
                                           Edit Filter Sets= No
                                           Idle Timeout(sec)= 100


              Press ENTER to Confirm or ESC to Cancel:
```

You can apply up to four schedule sets, separated by commas, for one remote node. Change the schedule set numbers to your preference(s).

**Figure 497** Applying Schedule Set(s) to a Remote Node (PPTP)

```
                    Menu 11.1 - Remote Node Profile

          Rem Node Name= ChangeMe              Route= IP
          Active= Yes

          Encapsulation= PPTP                Edit IP= No
          Service Type= Standard              Telco Option:
                                                Allocated Budget(min)= 0
          Outgoing=                             Period(hr)= 0
            My Login=                           Schedules= 1,2,3,4
            My Password= ********               Nailed-up Connections= No
            Retype to Confirm= ********
            Authen= CHAP/PAP
          PPTP:                                 Session Options:
            My IP Addr=                           Edit Filter Sets= No
            My IP Mask=                           Idle Timeout(sec)= 100
            Server IP Addr=
            Connection ID/Name=


           Press ENTER to Confirm or ESC to Cancel:
```

# PART VII
# Troubleshooting and Product Specifications

# 54

# Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware Connections, and LEDs
- ZyWALL Access and Login
- Internet Access
- Wireless Router/AP Troubleshooting
- UPnP

## 54.1 Power, Hardware Connections, and LEDs

### The ZyWALL does not turn on. None of the LEDs turn on.

1. Make sure the ZyWALL is turned on.
2. Make sure you are using the power adaptor or cord included with the ZyWALL.
3. Make sure the power adaptor or cord is connected to the ZyWALL and plugged in to an appropriate power source. Make sure the power source is turned on.
4. Turn the ZyWALL off and on or disconnect and re-connect the power adaptor or cord to the ZyWALL.
5. If the problem continues, contact the vendor.

### One of the LEDs does not behave as expected.

1. Make sure you understand the normal behavior of the LED. See Section 2.6 on page 59.
2. Check the hardware connections. See the Quick Start Guide.
3. Inspect your cables for damage. Contact the vendor to replace any damaged cables.
4. Turn the ZyWALL off and on or disconnect and re-connect the power adaptor or cord to the ZyWALL.
5. If the problem continues, contact the vendor.

## 54.2 ZyWALL Access and Login

### I forgot the LAN IP address for the ZyWALL.

1. The default LAN IP address is **192.168.1.1**.
2. Use the console port to log in to the ZyWALL.
3. If you changed the IP address and have forgotten it, you might get the IP address of the ZyWALL by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start** > **Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the ZyWALL (it depends on the network), so enter this IP address in your Internet browser.
4. If this does not work, you have to reset the device to its factory defaults. See Section 3.3 on page 63.

### I forgot the password.

1. The default password is **1234**.
2. If this does not work, you have to reset the device to its factory defaults. See Section 3.3 on page 63.

### I cannot see or access the **Login** screen in the web configurator.

1. Make sure you are using the correct IP address.
   - The default IP address is 192.168.1.1.
   - Use the ZyWALL's LAN IP address when configuring from the LAN.
   - Use the ZyWALL's WAN IP address when configuring from the WAN.
   - If you changed the LAN IP address (Section 7.2 on page 152), use the new IP address.
   - If you changed the LAN IP address and have forgotten it, see the troubleshooting suggestions for I forgot the LAN IP address for the ZyWALL.
2. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 2.6 on page 59.
3. Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled. See Appendix B on page 785.
4. Make sure your computer's Ethernet adapter is installed and functioning properly.
5. Make sure your computer is in the same subnet as the ZyWALL. (If you know that there are routers between your computer and the ZyWALL, skip this step.)

- If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. See Appendix D on page 795. Your ZyWALL is a DHCP server by default.

6 Reset the device to its factory defaults, and try to access the ZyWALL with the default IP address. See Section 3.3 on page 63.

7 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

**Advanced Suggestions**

- Try to access the ZyWALL using another service, such as Telnet. If you can access the ZyWALL, check the remote management settings, firewall rules, and SMT filters to find out why the ZyWALL does not respond to HTTP.
- If your computer is connected to the **WAN** port or is connected wirelessly, use a computer that is connected to a **LAN** port.
- You may also need to clear your Internet browser's cache.

  In Internet Explorer, click **Tools** and then **Internet Options** to open the **Internet Options** screen.

  In the **General** tab, click **Delete** Files. In the pop-up window, select the **Delete all offline content** check box and click **OK**. Click **OK** in the **Internet Options** screen to close it.
- If you disconnect your computer from one device and connect it to another device that has the same IP address, your computer's ARP (Address Resolution Protocol) table may contain an entry that maps the management IP address to the previous device's MAC address).

  In Windows, use **arp -d** at the command prompt to delete all entries in your computer's ARP table.

## I can see the **Login** screen, but I cannot log in to the ZyWALL.

1 Make sure you have entered the user name and password correctly. The default user name is **admin**, and the default password is **1234**. These fields are case-sensitive, so make sure [Caps Lock] is not on.

2 You cannot log in to the web configurator while someone is using the SMT, Telnet, or the console port to access the ZyWALL. Log out of the ZyWALL in the other session, or ask the person who is logged in to log out.

3 Turn the ZyWALL off and on or disconnect and re-connect the power adaptor or cord to the ZyWALL.

4 If this does not work, you have to reset the device to its factory defaults. See Section 3.3 on page 63.

## I cannot access the SMT. / I cannot Telnet to the ZyWALL.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

### I cannot use FTP to upload / download the configuration file. / I cannot use FTP to upload new firmware.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

## 54.3 Internet Access

### I cannot get a WAN IP address from the ISP.

1. The ISP provides the WAN IP address after authenticating you. Authentication may be through the user name and password, the MAC address or the host name.

   The username and password apply to PPPoE and PPPoA encapsulation only. Make sure that you have entered the correct **Service Type**, **User Name** and **Password** (be sure to use the correct casing). Refer to the WAN setup chapter (web configurator or SMT).
2. Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.
3. If the problem continues, contact your ISP.

### I cannot access the Internet.

1. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 2.6 on page 59.
2. Make sure you entered your ISP account information correctly in the wizard, WAN screen or SMT menu. These fields are case-sensitive, so make sure [Caps Lock] is not on.
3. If you are trying to access the Internet wirelessly, make sure the wireless settings in the wireless client are the same as the settings in the AP.
4. Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.
5. If the problem continues, contact your ISP.

### I cannot access the Internet anymore. I had access to the Internet (with the ZyWALL), but my Internet connection is not available anymore.

1. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 2.6 on page 59.
2. Check the schedule rules. Refer to Chapter 53 on page 757 (SMT).
3. If you use PPPoA or PPPoE encapsulation, check the idle time-out setting. Refer to the Chapter 9 on page 169 (web configurator) or Chapter 38 on page 639 (SMT).
4. Reboot the ZyWALL.
5. If the problem continues, contact your ISP.

### The Internet connection is slow or intermittent.

1. There might be a lot of traffic on the network. Look at the LEDs, and check Section 2.6 on page 59. If the ZyWALL is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
2. Check the signal strength. If the signal strength is low, try moving the ZyWALL closer to the AP if possible, and look around to see if there are any devices that might be interfering with the wireless network (for example, microwaves, other wireless networks, and so on).
3. Reboot the ZyWALL.
4. If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

**Advanced Suggestions**

- Check the settings for bandwidth management. If it is disabled, you might consider activating it. If it is enabled, you might consider changing the allocations.

## 54.4 Wireless Router/AP Troubleshooting

### I cannot access the ZyWALL or ping any computer from the WLAN.

1. Make sure the wireless LAN is enabled on the ZyWALL
2. Make sure the wireless adapter on the wireless station is working properly.
3. Make sure the wireless adapter (installed on your computer) is IEEE 802.11 compatible and supports the same wireless standard as the ZyWALL.
4. Make sure your computer (with a wireless adapter installed) is within the transmission range of the ZyWALL.

5 Check that both the ZyWALL and your wireless station are using the same wireless and wireless security settings.
6 Make sure traffic between the WLAN and the LAN is not blocked by the firewall on the ZyWALL.
7 Make sure you allow the ZyWALL to be remotely accessed through the WLAN interface. Check your remote management settings.

## 54.5 UPnP

When using UPnP and the ZyWALL reboots, my computer cannot detect UPnP and refresh **My Network Places > Local Network**.

1 Disconnect the Ethernet cable from the ZyWALL's LAN port or from your computer.
2 Re-connect the Ethernet cable.

The **Local Area Connection** icon for UPnP disappears in the screen.

Restart your computer.

I cannot open special applications such as white board, file transfer and video when I use the MSN messenger.

1 Wait more than three minutes.
2 Restart the applications.

# 55

# Product Specifications

The following tables summarize the ZyWALL's hardware and firmware features.

**Table 268** Hardware Specifications

| | |
|---|---|
| Dimensions | ZyWALL 70: 355(L) x 200(D) x 55(H) mm<br>ZyWALL 5 and ZyWALL 35: 242.0(W) x 175.0(D) x 35.5(H) mm |
| Weight | ZyWALL 70: 2,600g<br>ZyWALL 5 and ZyWALL 35: 1,200g |
| Power Specification | ZyWALL 70: 100 ~ 240 VAC<br>ZyWALL 5 and ZyWALL 35: 12V DC |
| Fuse Specifications | ZyWALL 70: T 0.5 Amp, 250 VAC |
| Ethernet Interface | |
| LAN | ZyWALL 70: One auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet port<br>ZyWALL 5 and 35: Four LAN/DMZ/WLAN auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet ports. |
| WAN | ZyWALL 35 and 70: Dual auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet ports<br>ZyWALL 5: One auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet port |
| DMZ | ZyWALL 70: Four DMZ/WLAN auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet ports.<br>ZyWALL 5 and 35: Four LAN/DMZ/WLAN auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet ports. |
| Reset Button | Restores factory default settings |
| Console | RS-232 DB9F |
| Dial Backup | RS-232 DB9M |
| Extension Card Slot | For installing an optional ZyXEL wireless LAN card, 3G card or a ZyWALL Turbo extension card |
| Operating Temperature | 0º C ~ 50º C |
| Storage Temperature | -30º C ~ 60º C |
| Operating Humidity | 20% ~ 95% RH (non-condensing) |
| Storage Humidity | 20% ~ 95% RH (non-condensing) |
| Certifications | EMC: FCC Class B, CE-EMC Class B, C-Tick Class B, VCCI Class B<br>Safety: CSA International, CE EN60950-1 |
| MTBF (Mean Time Between Failures) (Bellcore model) | ZyWALL 70: 40.9 years<br>ZyWALL 35: 41.8 years<br>ZyWALL 5: 41.7 years |

**Table 269** Firmware Specifications

| FEATURE | DESCRIPTION |
|---|---|
| Default IP Address | 192.168.1.1 |
| Default Subnet Mask | 255.255.255.0 (24 bits) |
| Default Password | 1234 |
| Default DHCP Pool | 192.168.1.33 to 192.168.1.160 |
| Device Management | Use the web configurator to easily configure the rich range of features on the ZyWALL. |
| Wireless Functionality | Allow the IEEE 802.11b and/or IEEE 802.11g wireless clients to connect to the ZyWALL wirelessly. Enable wireless security (WEP, WPA(2), WPA(2)-PSK) and/or MAC filtering to protect your wireless network. |
| Firmware Upgrade | Download new firmware (when available) from the ZyXEL web site and use the web configurator, an FTP or a TFTP tool to put it on the ZyWALL.<br><br>Note: Only upload firmware for your specific model! |
| Configuration Backup & Restoration | Make a copy of the ZyWALL's configuration. You can put it back on the ZyWALL later if you decide to revert back to an earlier configuration. |
| Network Address Translation (NAT) | Each computer on your network must have its own unique IP address. Use NAT to convert your public IP address(es) to multiple private IP addresses for the computers on your network. |
| Port Forwarding | If you have a server (mail or web server for example) on your network, you can use this feature to let people access it from the Internet. |
| DHCP (Dynamic Host Configuration Protocol) | Use this feature to have the ZyWALL assign IP addresses, an IP default gateway and DNS servers to computers on your network. |
| Dynamic DNS Support | With Dynamic DNS (Domain Name System) support, you can use a fixed URL, www.zyxel.com for example, with a dynamic IP address. You must register for this service with a Dynamic DNS service provider. |
| IP Multicast | IP multicast is used to send traffic to a specific group of computers. The ZyWALL supports versions 1 and 2 of IGMP (Internet Group Management Protocol) used to join multicast groups (see RFC 2236). |
| IP Alias | IP alias allows you to subdivide a physical network into logical networks over the same Ethernet interface with the ZyWALL itself as the gateway for each subnet. |
| Time and Date | Get the current time and date from an external server when you turn on your ZyWALL. You can also set the time manually. These dates and times are then used in logs. |
| Logging and Tracing | Use packet tracing and logs for troubleshooting. You can send logs from the ZyWALL to an external syslog server. |
| PPPoE | PPPoE mimics a dial-up Internet access connection. |
| PPTP Encapsulation | Point-to-Point Tunneling Protocol (PPTP) enables secure transfer of data through a Virtual Private Network (VPN). The ZyWALL supports one PPTP connection at a time. |
| Universal Plug and Play (UPnP) | A UPnP-enabled device can dynamically join a network, obtain an IP address and convey its capabilities to other devices on the network. |
| RoadRunner Support | The ZyWALL supports Time Warner's RoadRunner Service in addition to standard cable modem services. |

**Table 269** Firmware Specifications

| FEATURE | DESCRIPTION |
|---|---|
| Firewall | You can configure firewall on the ZyXEL Device for secure Internet access. When the firewall is on, by default, all incoming traffic from the Internet to your network is blocked unless it is initiated from your network. This means that probes from the outside to your network are not allowed, but you can safely browse the Internet and download files for example. |
| Content Filter | The ZyWALL blocks or allows access to web sites that you specify and blocks access to web sites with URLs that contain keywords that you specify. You can define time periods and days during which content filtering is enabled. You can also include or exclude particular computers on your network from content filtering.<br>You can also subscribe to category-based content filtering that allows your ZyWALL to check web sites against an external database. |
| IPSec VPN | This allows you to establish a secure Virtual Private Network (VPN) tunnel to connect with business partners and branch offices using data encryption and the Internet without the expense of leased site-to-site lines. The ZyWALL VPN is based on the IPSec standard and is fully interoperable with other IPSec-based VPN products. |
| Bandwidth Management | You can efficiently manage traffic on your network by reserving bandwidth and giving priority to certain types of traffic and/or to particular computers. |
| Remote Management | This allows you to decide whether a service (HTTP or FTP traffic for example) from a computer on a network (LAN or WAN for example) can access the ZyWALL. |

**Table 270** Feature and Performance Specifications

| FEATURE | ZYWALL 70 | ZYWALL 35 | ZYWALL 5 |
|---|---|---|---|
| Local User Database Entries | 32 | 32 | 32 |
| Static DHCP Table Entries | 128 | 128 | 128 |
| Static Routes | 50 | 50 | 30 |
| Policy Routes | 48 | 48 | N/A |
| Port Forwarding Rules | 100 | 50 | 30 |
| Concurrent Sessions (NAT sessions) | 10,000 | 10,000 | 6,000 (without the ZyWALL Turbo Card)<br>4,000 (with the ZyWALL Turbo Card) |
| Address Mapping Rules | 100 | 50 | 30 |
| Configurable IPSec VPN Network Policies (including network policies in the recycle bin) | 120 | 40 | 10 |
| Simultaneous IPSec VPN Connections | 100 | 35 | 10 |
| Bandwidth Management Classes | 100 | 50 | 20 |
| Bandwidth Management Class Levels | 5 | 3 | 1 |
| DNS Address Record Entries | 30 | 30 | 30 |
| DNS Name Server Record Entries | 16 | 16 | 16 |
| Concurrent E-mail Sessions with Anti-Spam Enabled | 200 | 100 | 20 |

**Table 270** Feature and Performance Specifications (continued)

| FEATURE | ZYWALL 70 | ZYWALL 35 | ZYWALL 5 |
|---|---|---|---|
| Anti-Spam Whitelist and Blacklist Entries | 12,288 Kb Individual entries my vary in size. The total number you can configure is less than 860. | 6,144 Kb Individual entries my vary in size. The total number you can configure is less than 450. | 3,072 Kb Individual entries my vary in size. The total number you can configure is less than 220. |
| Firewall Throughput (with NAT) | 80Mbps | 75Mbps | 60Mbps |
| VPN (3DES) Throughput | 40Mbps | 35Mbps | 30Mbps |
| User Licenses | Unlimited | Unlimited | Unlimited |

# Compatible ZyXEL WLAN Cards

The following table lists the ZyXEL WLAN cards that you can use in the ZyWALL at the time of writing. It also shows the security features that each card supports.

Check the product page on the www.zyxel.com website for updates on ZyXEL WLAN cards that you can use in the ZyWALL.

**Table 271** Compatible ZyXEL WLAN Cards and Security Features

| | B-100 | B-101 | B-120 | G-100 | G-110 |
|---|---|---|---|---|---|
| No Security | Yes | Yes | Yes | Yes | Yes |
| Static WEP | Yes | Yes | Yes | Yes | Yes |
| WPA-PSK | No | No | Yes | Yes | Yes |
| WPA (MD5 is not supported) | No | No | Yes | Yes | Yes |
| 802.1x + Dynamic WEP (MD5 is not supported) | No | No | Yes | Yes | Yes |
| 802.1x + Static WEP | Yes | Yes | Yes | Yes | Yes |
| 802.1x + No WEP | Yes | Yes | Yes | Yes | Yes |
| No Access 802.1x + Static WEP | Yes | Yes | Yes | Yes | Yes |
| No Access 802.1x + No WEP | Yes | Yes | Yes | Yes | Yes |

# 55.1 Compatible 3G Cards

At the time of writing, you can use the following 3G wireless cards in the ZyWALL 5. The table also shows you the 3G features supported by the compatible 3G cards.

**Table 272** 3G Features Supported By Compatible 3G Cards

| 3G CARD / FEATURES | SIERRA WIRELESS AC880/ AC881 | SIERRA WIRELESS AC580 | SIERRA WIRELESS AC595 | SIERRA WIRELESS AC850/860 | SIERRA WIRELESS AC875 |
|---|---|---|---|---|---|
| Radio Technology | HSDPA | 1xEV-DO Rev. 0 | 1xEV-DO Rev. A | HSDPA | HSDPA |
| Maximum Speed (Downstream/Upstream) | 7.2 Mbps / 2.0 Mbps | 2.4 Mbps/ 384 Kbps | 3.1 Mbps/ 1.8 Mbps | 1.8 Mbps / 384 Kbps | 3.6 Mbps / 384 Kbps |
| SIM card authentication via the web configurator | Y | | | Y | Y |
| Enabling of the internal modem on the 3G card | | | Y | | |
| Network type selection via the web configurator | Y | | | Y | Y |
| Manual or automatic service provider selection via the web configurator | Y | | | Y | Y |
| Signal strength update even when data is transmitting | Y | Y | Y | | Y |
| Network type update even when data is transmitting | | | | | Y |
| Roaming status update even when data is transmitting | | | Y | | Y |
| Dormant status update after the connection is established | | | Y | | |
| Budget Control | Y | Y | Y | Y | Y |
| Bandwidth Management | Y | Y | Y | Y | Y |

**Table 273** 3G Features Supported By Additional Compatible 3G Cards

| 3G CARD / FEATURES | HUAWEI E612 | HUAWEI E620 | HUAWEI E630 | HUAWEI EC321 | HUAWEI EC360 |
|---|---|---|---|---|---|
| Radio Technology | UMTS | HSDPA | HSDPA | 1xRTT | 1xEV-DO Rev. A |
| Maximum Speed (Downstream/Upstream) | 384 Kbps | 1.8 Mbps / 384 Kbps | 3.6Mbps / 384Kbps | 153.6Kbps/ 153.6Kbps | 3.1Mbps/ 1.8Mbps |
| SIM card authentication via the web configurator | Y | Y | Y | | |
| Enabling of the internal modem on the 3G card | | | | | |
| Network type selection via the web configurator | | | | | |

**Table 273** 3G Features Supported By Additional Compatible 3G Cards

| 3G CARD<br>FEATURES | HUAWEI E612 | HUAWEI E620 | HUAWEI E630 | HUAWEI EC321 | HUAWEI EC360 |
|---|---|---|---|---|---|
| Manual or automatic service provider selection via the web configurator | Y | Y | Y | | |
| Signal strength update even when data is transmitting | Y | Y | Y | | |
| Network type update even when data is transmitting | | | | | |
| Roaming status update even when data is transmitting | | | | | |
| Dormant status update after the connection is established | | | | | |
| Budget Control | Y | Y | Y | Y | Y |
| Bandwidth Management | Y | Y | Y | Y | Y |

**Table 274** 3G Features Supported By Additional Compatible 3G Cards

| 3G CARD<br>FEATURES | HUAWEI EC500 | HUAWEI E220 | OPTION GLOBETROTTER HSDPA 7.2 READY | NOVATEL MERLIN EX720 | NOVATEL MERLIN PC720 |
|---|---|---|---|---|---|
| Radio Technology | 1xEV-DO Rev. 0 | HSDPA | HSDPA | 1xEV-DO Rev. A | 1xEV-DO Rev. A |
| Maximum Speed (Downstream/Upstream) | 2.4 Mbps/ 384 Kbps | 3.6Mbps / 384Kbps | 7.2Mbps / 384Kbps | 1.4 Mbps/ 500Kbps | 3.1Mbps/ 1.8Mbps |
| SIM card authentication via the web configurator | | Y | Y | | |
| Enabling of the internal modem on the 3G card | | | | | |
| Network type selection via the web configurator | | | | | |
| Manual or automatic service provider selection via the web configurator | | Y | Y | | |
| Signal strength update even when data is transmitting | | Y | Y | | |
| Network type update even when data is transmitting | | | | | |
| Roaming status update even when data is transmitting | | | | | |
| Dormant status update after the connection is established | | | | | |

**Table 274** 3G Features Supported By Additional Compatible 3G Cards

| 3G CARD<br>FEATURES | HUAWEI EC500 | HUAWEI E220 | OPTION GLOBETROTTER HSDPA 7.2 READY | NOVATEL MERLIN EX720 | NOVATEL MERLIN PC720 |
|---|---|---|---|---|---|
| Budget Control | Y | Y | Y | Y | Y |
| Bandwidth Management | Y | Y | Y | Y | Y |

## 55.2 Power Adaptor Specifications

**Table 275** North American Plug Standards

| | |
|---|---|
| AC POWER ADAPTOR MODEL | PSA18R-120P (ZA)-R |
| INPUT POWER | 100-240VAC, 50/60HZ, 0.5A |
| OUTPUT POWER | 12VDC, 1.5A |
| POWER CONSUMPTION | 18 W MAX. |
| SAFETY STANDARDS | UL, CUL (UL 60950-1 FIRST EDITIONCSA C22.2 NO. 60950-1-03 1ST.) |

**Table 276** European Plug Standards

| | |
|---|---|
| AC POWER ADAPTOR MODEL | PSA18R-120P (ZE)-R |
| INPUT POWER | 100-240VAC, 50/60HZ, 0.5A |
| OUTPUT POWER | 12VDC, 1.5A |
| POWER CONSUMPTION | 18 W MAX. |
| SAFETY STANDARDS | TUV, CE (EN 60950-1) |

**Table 277** United Kingdom Plug Standards

| | |
|---|---|
| AC POWER ADAPTOR MODEL | PSA18R-120P (ZK)-R |
| INPUT POWER | 100-240VAC, 50/60HZ, 0.5A |
| OUTPUT POWER | 12VDC, 1.5A |
| POWER CONSUMPTION | 18 W MAX. |
| SAFETY STANDARDS | TUV (BS EN 60950-1) |

**Table 278** 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, 1.5A |
| POWER CONSUMPTION | 18 W MAX. |
| SAFETY STANDARDS | AS/NZ60950 |

**Table 279** Japan Plug Standards

| | |
|---|---|
| AC POWER ADAPTOR MODEL | PSA18R-120P (ZA)-R |
| INPUT POWER | 100-240VAC, 50/60HZ, 0.5A |

**Table 279** Japan Plug Standards

| | |
|---|---|
| OUTPUT POWER | 12VDC, 1.5A |
| POWER CONSUMPTION | 18 W MAX. |
| SAFETY STANDARDS | JET |

**Table 280** China Plug Standards

| | |
|---|---|
| AC POWER ADAPTOR MODEL | PSA18R-120P (ZA)-R |
| INPUT POWER | 100-240VAC, 50/60HZ, 0.5A |
| OUTPUT POWER | 12VDC, 1.5A |
| POWER CONSUMPTION | 18 W MAX. |
| SAFETY STANDARDS | CCC |

# Cable Pin Assignments

In a serial communications connection, generally a computer is DTE (Data Terminal Equipment) and a modem is DCE (Data Circuit-terminating Equipment). The ZyWALL is DCE when you connect a computer to the console port. The ZyWALL is DTE when you connect a modem to the dial backup port.[4]

**Figure 498** Console/Dial Backup Port Pin Layout

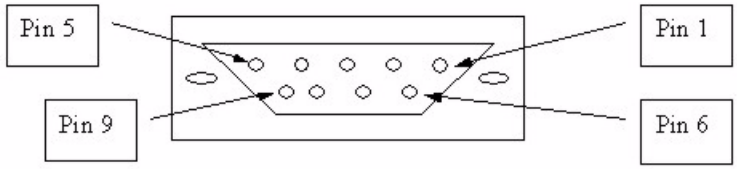



**Table 281** Console/Dial Backup Port Pin Assignments

| CONSOLE Port RS – 232 (Female) DB-9F | DIAL BACKUP RS – 232 (Male) DB-9M (Not on all models) |
|---|---|
| Pin 1 = NON<br>Pin 2 = DCE-TXD<br>Pin 3 = DCE –RXD<br>Pin 4 = DCE –DSR<br>Pin 5 = GND<br>Pin 6 = DCE –DTR<br>Pin 7 = DCE –CTS<br>Pin 8 = DCE –RTS<br>PIN 9 = NON | Pin 1 = NON<br>Pin 2 = DTE-RXD<br>Pin 3 = DTE-TXD<br>Pin 4 = DTE-DTR<br>Pin 5 = GND<br>Pin 6 = DTE-DSR<br>Pin 7 = DTE-RTS<br>Pin 8 = DTE-CTS<br>PIN 9 = NON. |
| The CON/AUX port also has these pin assignments. The CON/AUX switch changes the setting in the firmware only and does not change the CON/AUX port's pin assignments. | ZyWALLs with a CON/AUX port also have a 9-pin adaptor for the console cable with these pin assignments on the male end. |

4. Pins 2,3 and 5 are used.

**Table 282** Ethernet Cable Pin Assignments

| WAN / LAN ETHERNET CABLE PIN LAYOUT | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Straight-through** | | | | **Crossover** | | | |
| (Switch) | | | (Adapter) | (Switch) | | | (Switch) |
| 1 | IRD + | | 1 OTD + | 1 | IRD + | | 1 IRD + |
| 2 | IRD - | | 2 OTD - | 2 | IRD - | | 2 IRD - |
| 3 | OTD + | | 3 IRD + | 3 | OTD + | | 3 OTD + |
| 6 | OTD - | | 6 IRD - | 6 | OTD - | | 6 OTD - |

# PART VIII
# Appendices and Index

# A

# Removing and Installing a Fuse

This appendix shows you how to remove and install fuses for the ZyWALL.

If you need to install a new fuse, follow the procedure below.

If you use a fuse other than the included fuses, make sure it matches the fuse specifications in the product specifications chapter.

## Removing a Fuse

Disconnect all power from the ZyWALL before you begin this procedure.

1. Place the rear panel of the ZyWALL in front of you.
2. Remove the power cord from the back of the unit.
3. The fuse housing is located between the power switch and the power port. Use a small flat-head screwdriver to carefully pry out the fuse housing.
4. A burnt-out fuse is blackened, darkened or cloudy inside its glass casing. A working fuse has a completely clear glass casing. Pull gently, but firmly, to remove the burnt out fuse from the fuse housing. Dispose of the burnt-out fuse.

## Installing a Fuse

1. The ZyWALL is shipped from the factory with one spare fuse included in a box-like section of the fuse housing. Push the middle part of the box-like section to access the spare fuse. Put another spare fuse in its place in order to always have one on hand.
2. Push the replacement fuse into the fuse housing until you hear a click.
3. Firmly, but gently, push the fuse housing back into the ZyWALL until you hear a click.
4. Plug the power cord back into the unit.

# 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 283** 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 (e.g. www.zyxel.com) to IP numbers. |
| 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. |

**Table 283** Commonly Used Services (continued)

| NAME | PROTOCOL | PORT(S) | DESCRIPTION |
|---|---|---|---|
| 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). |
| 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. |

**Table 283** Commonly Used Services (continued)

| NAME | PROTOCOL | PORT(S) | DESCRIPTION |
|---|---|---|---|
| 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. |
| 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

# Wireless LANs

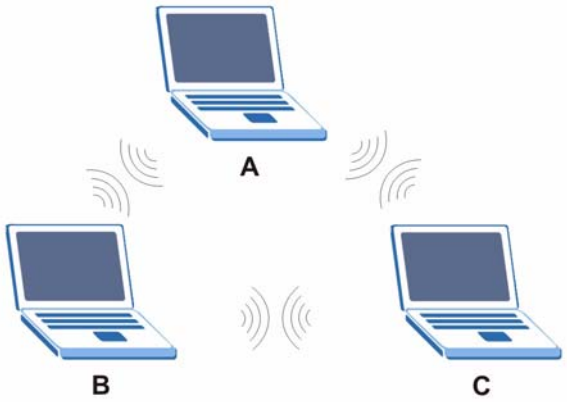
## Wireless LAN Topologies

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 499** Peer-to-Peer Communication in an Ad-hoc Network

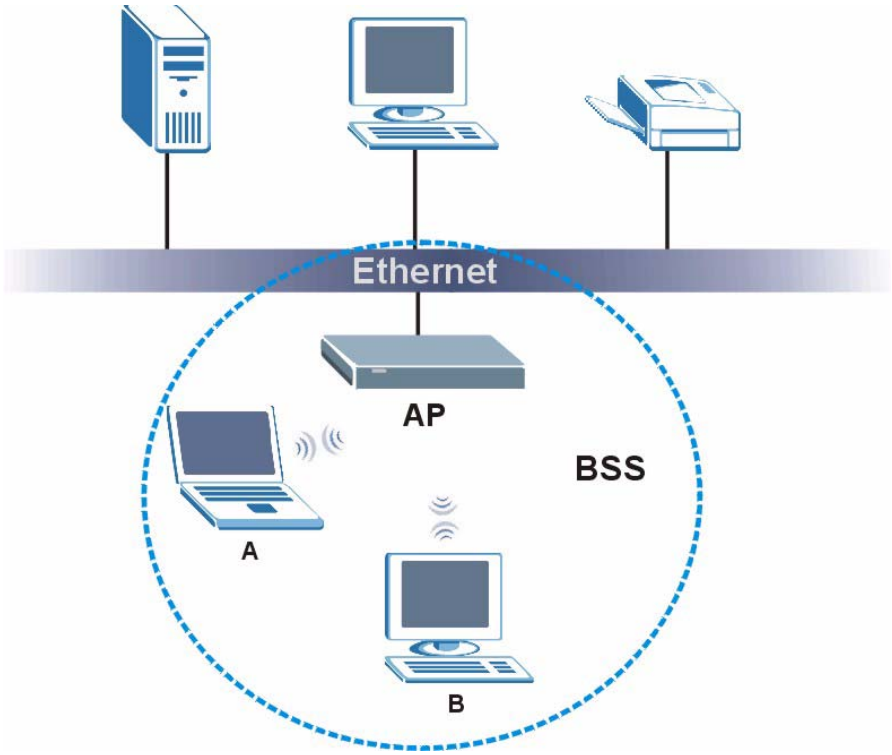



### BSS

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 500** Basic Service Set



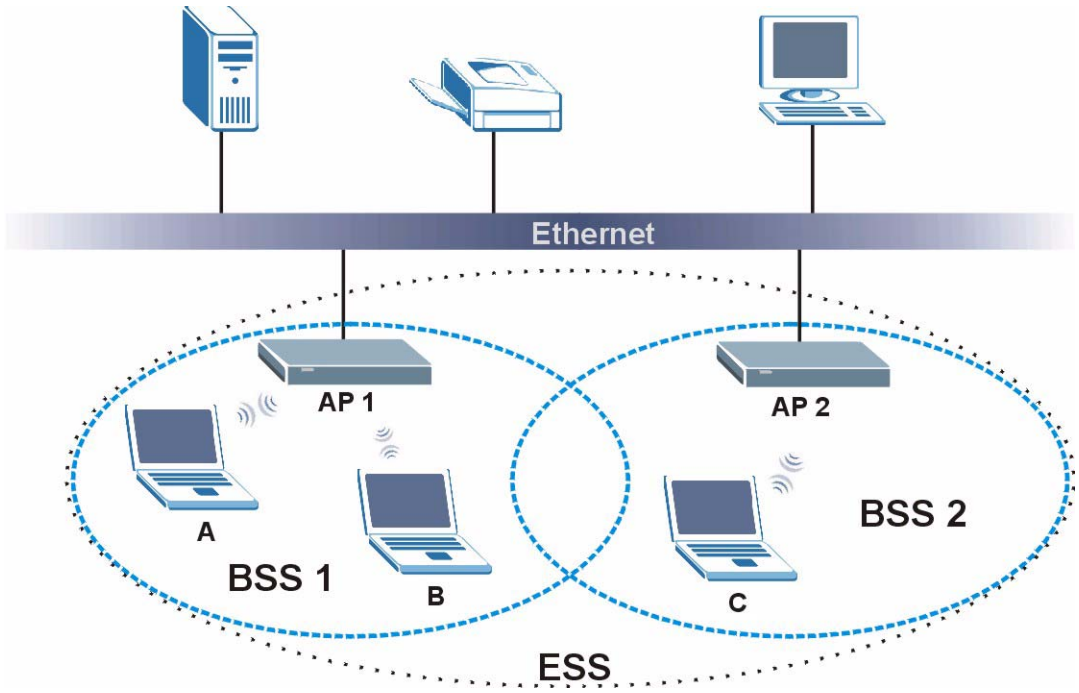

## ESS

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 501** Infrastructure WLAN




## Channel

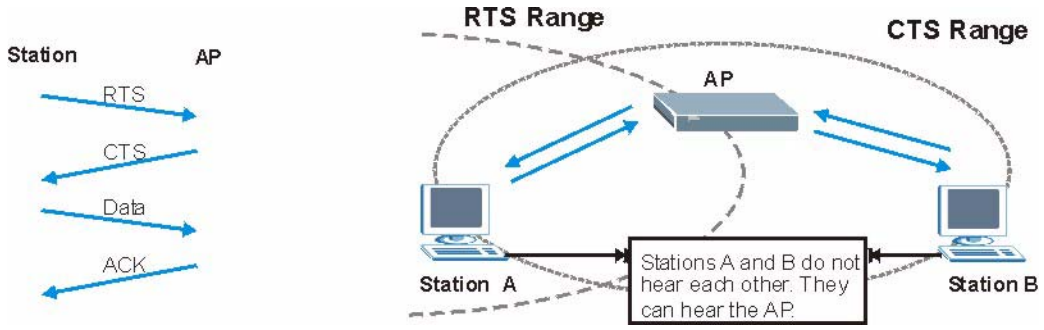
A channel is the radio frequency(ies) used by wireless devices to transmit and receive data. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a channel different from an adjacent AP (access point) to reduce interference. Interference 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 502** 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.

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.

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 284** 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 285** 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 |

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.

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 286** 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.

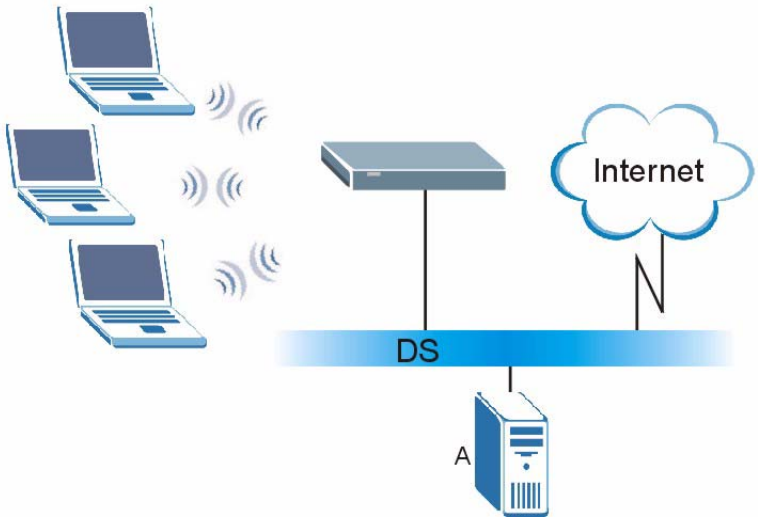
The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

## 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 503** WPA(2) with RADIUS Application Example




## WPA(2)-PSK Application Example

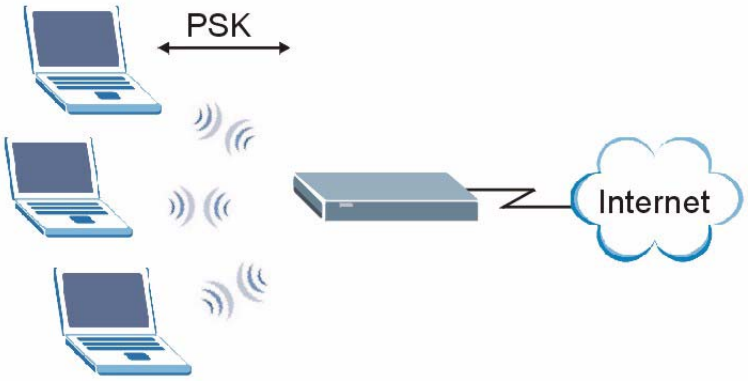
A WPA(2)-PSK application looks as follows.

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 504** 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 287** 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.

# D

# Windows 98 SE/Me Requirements for Anti-Virus Message Display

With the anti-virus packet scan, when a virus is detected, an alert message is displayed on Miscrosoft Windows-based  computers.

For Windows 98 SE/Me, you must open the **WinPopup** window in order to view real-time alert messages. For Windows 2000 and later versions, a message window automatically displays when an alert is received.

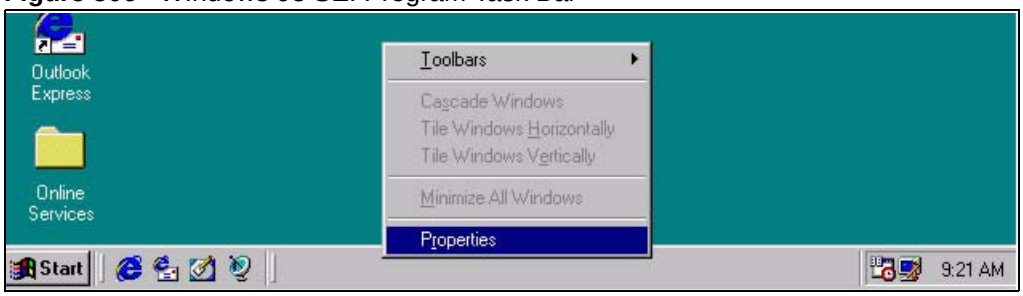
Click **Start**, **Run** and enter “winpopup” in the field provided and click **OK**. The **WinPopup** window displays as shown.

**Figure 505** 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 506** WIndows 98 SE: Program Task Bar



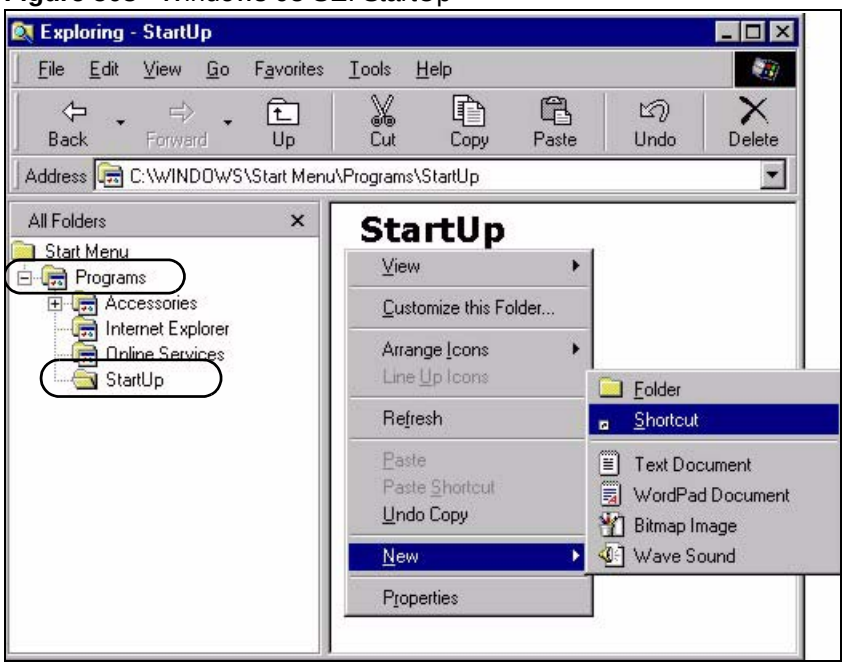

**2** Click the **Start Menu Programs** tab and click **Advanced ...**.

**Figure 507** Windows 98 SE: Task Bar Properties


**3** Double-click **Programs** and click **StartUp**.

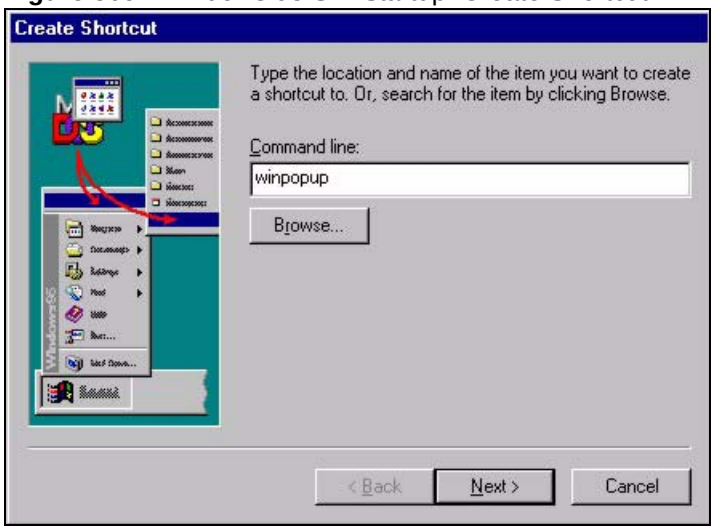
**4** Right-click in the **StartUp** pane and click **New**, **Shortcut**.

**Figure 508** Windows 98 SE: StartUp



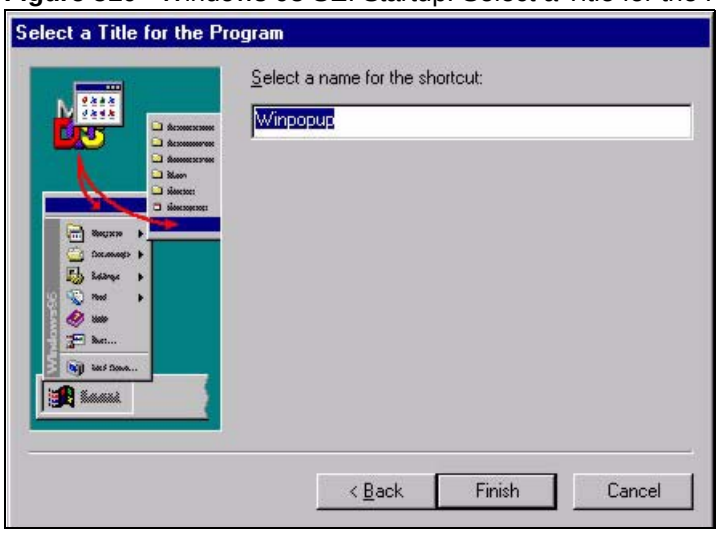

**5** A **Create Shortcut** window displays. Enter "winpopup" in the **Command line** field and click **Next**.

**Figure 509** Windows 98 SE: Startup: Create Shortcut



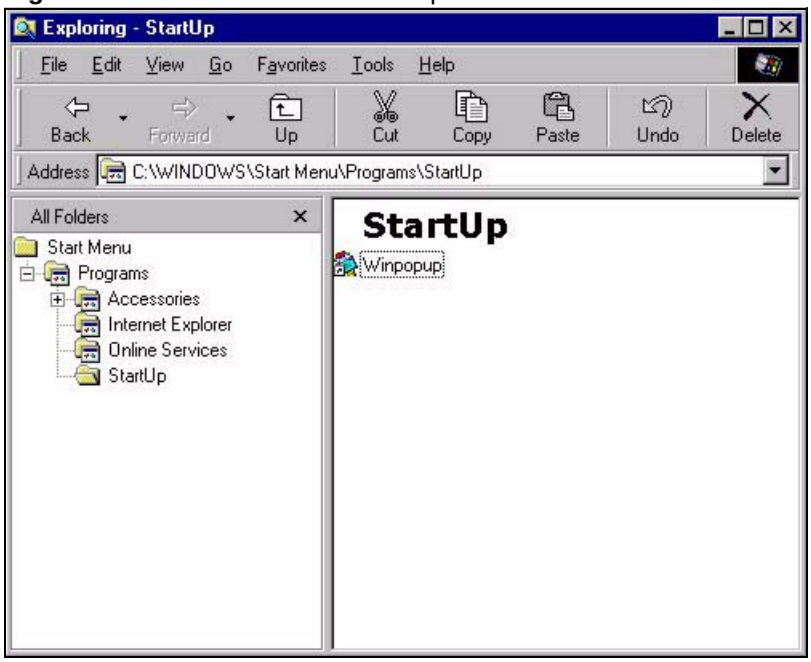

**6** Specify a name for the shortcut or accept the default and click **Finish**.

**Figure 510** 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 511** Windows 98 SE: Startup: Shortcut




The WinPopup window displays after the computer finishes the startup process (see Figure 505 on page 801).

# E

# 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.

Your use of the ZyWALL is subject to the terms and conditions of your service provider.

### 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

### 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.
- IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.
- To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

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 device has been designed for the WLAN 2.4 GHz network throughout the EC region and Switzerland, with restrictions in France.

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 for global products, or at www.us.zyxel.com for North American products.

F

# Customer Support

In the event of problems that cannot be solved by using this manual, 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. Regional offices are listed below (see also http://www.zyxel.com/web/contact_us.php). Please have the following information ready when you contact an office.

### Required Information

- 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.

"+" is the (prefix) number you dial to make an international telephone call.

### Corporate Headquarters (Worldwide)

- Support E-mail: support@zyxel.com.tw
- Sales E-mail: sales@zyxel.com.tw
- Telephone: +886-3-578-3942
- Fax: +886-3-578-2439
- Web: www.zyxel.com
- Regular Mail: ZyXEL Communications Corp., 6 Innovation Road II, Science Park, Hsinchu 300, Taiwan

### China - ZyXEL Communications (Beijing) Corp.

- Support E-mail: cso.zycn@zyxel.cn
- Sales E-mail: sales@zyxel.cn
- Telephone: +86-010-82800646
- Fax: +86-010-82800587
- Address: 902, Unit B, Horizon Building, No.6, Zhichun Str, Haidian District, Beijing
- Web: http://www.zyxel.cn

### China - ZyXEL Communications (Shanghai) Corp.

- Support E-mail: cso.zycn@zyxel.cn
- Sales E-mail: sales@zyxel.cn
- Telephone: +86-021-61199055
- Fax: +86-021-52069033

- Address: 1005F, ShengGao International Tower, No.137 XianXia Rd., Shanghai
- Web: http://www.zyxel.cn

### Costa Rica

- Support E-mail: soporte@zyxel.co.cr
- Sales E-mail: sales@zyxel.co.cr
- Telephone: +506-2017878
- Fax: +506-2015098
- Web: www.zyxel.co.cr
- Regular Mail: ZyXEL Costa Rica, Plaza Roble Escazú, Etapa El Patio, Tercer Piso, San José, Costa Rica

### Czech Republic

- E-mail: info@cz.zyxel.com
- Telephone: +420-241-091-350
- Fax: +420-241-091-359
- Web: www.zyxel.cz
- Regular Mail: ZyXEL Communications, Czech s.r.o., Modranská 621, 143 01 Praha 4 - Modrany, Ceská Republika

### Denmark

- Support E-mail: support@zyxel.dk
- Sales E-mail: sales@zyxel.dk
- Telephone: +45-39-55-07-00
- Fax: +45-39-55-07-07
- Web: www.zyxel.dk
- Regular Mail: ZyXEL Communications A/S, Columbusvej, 2860 Soeborg, Denmark

### Finland

- Support E-mail: support@zyxel.fi
- Sales E-mail: sales@zyxel.fi
- Telephone: +358-9-4780-8411
- Fax: +358-9-4780-8448
- Web: www.zyxel.fi
- Regular Mail: ZyXEL Communications Oy, Malminkaari 10, 00700 Helsinki, Finland

### France

- E-mail: info@zyxel.fr
- Telephone: +33-4-72-52-97-97
- Fax: +33-4-72-52-19-20
- Web: www.zyxel.fr
- Regular Mail: ZyXEL France, 1 rue des Vergers, Bat. 1 / C, 69760 Limonest, France

### Germany

- Support E-mail: support@zyxel.de
- Sales E-mail: sales@zyxel.de
- Telephone: +49-2405-6909-69
- Fax: +49-2405-6909-99
- Web: www.zyxel.de
- Regular Mail: ZyXEL Deutschland GmbH., Adenauerstr. 20/A2 D-52146, Wuerselen, Germany

### Hungary

- Support E-mail: support@zyxel.hu
- Sales E-mail: info@zyxel.hu
- Telephone: +36-1-3361649
- Fax: +36-1-3259100
- Web: www.zyxel.hu
- Regular Mail: ZyXEL Hungary, 48, Zoldlomb Str., H-1025, Budapest, Hungary

### India

- Support E-mail: support@zyxel.in
- Sales E-mail: sales@zyxel.in
- Telephone: +91-11-30888144 to +91-11-30888153
- Fax: +91-11-30888149, +91-11-26810715
- Web: http://www.zyxel.in
- Regular Mail: India - ZyXEL Technology India Pvt Ltd., II-Floor, F2/9 Okhla Phase -1, New Delhi 110020, India

### Japan

- Support E-mail: support@zyxel.co.jp
- Sales E-mail: zyp@zyxel.co.jp
- Telephone: +81-3-6847-3700
- Fax: +81-3-6847-3705
- Web: www.zyxel.co.jp
- Regular Mail: ZyXEL Japan, 3F, Office T&U, 1-10-10 Higashi-Gotanda, Shinagawa-ku, Tokyo 141-0022, Japan

### Kazakhstan

- Support: http://zyxel.kz/support
- Sales E-mail: sales@zyxel.kz
- Telephone: +7-3272-590-698
- Fax: +7-3272-590-689
- Web: www.zyxel.kz
- Regular Mail: ZyXEL Kazakhstan, 43 Dostyk Ave., Office 414, Dostyk Business Centre, 050010 Almaty, Republic of Kazakhstan

### Malaysia

- Support E-mail: support@zyxel.com.my
- Sales E-mail: sales@zyxel.com.my
- Telephone: +603-8076-9933
- Fax: +603-8076-9833
- Web: http://www.zyxel.com.my
- Regular Mail: ZyXEL Malaysia Sdn Bhd., 1-02 & 1-03, Jalan Kenari 17F, Bandar Puchong Jaya, 47100 Puchong, Selangor Darul Ehsan, Malaysia

### North America

- Support E-mail: support@zyxel.com
- Support Telephone: +1-800-978-7222
- Sales E-mail: sales@zyxel.com
- Sales Telephone: +1-714-632-0882
- Fax: +1-714-632-0858
- Web: www.zyxel.com
- Regular Mail: ZyXEL Communications Inc., 1130 N. Miller St., Anaheim, CA 92806-2001, U.S.A.

### Norway

- Support E-mail: support@zyxel.no
- Sales E-mail: sales@zyxel.no
- Telephone: +47-22-80-61-80
- Fax: +47-22-80-61-81
- Web: www.zyxel.no
- Regular Mail: ZyXEL Communications A/S, Nils Hansens vei 13, 0667 Oslo, Norway

### Poland

- E-mail: info@pl.zyxel.com
- Telephone: +48-22-333 8250
- Fax: +48-22-333 8251
- Web: www.pl.zyxel.com
- Regular Mail: ZyXEL Communications, ul. Okrzei 1A, 03-715 Warszawa, Poland

### Russia

- Support: http://zyxel.ru/support
- Sales E-mail: sales@zyxel.ru
- Telephone: +7-095-542-89-29
- Fax: +7-095-542-89-25
- Web: www.zyxel.ru
- Regular Mail: ZyXEL Russia, Ostrovityanova 37a Str., Moscow 117279, Russia

### Singapore

- Support E-mail: support@zyxel.com.sg
- Sales E-mail: sales@zyxel.com.sg
- Telephone: +65-6899-6678
- Fax: +65-6899-8887
- Web: http://www.zyxel.com.sg
- Regular Mail: ZyXEL Singapore Pte Ltd., No. 2 International Business Park, The Strategy #03-28, Singapore 609930

### Spain

- Support E-mail: support@zyxel.es
- Sales E-mail: sales@zyxel.es
- Telephone: +34-902-195-420
- Fax: +34-913-005-345
- Web: www.zyxel.es
- Regular Mail: ZyXEL Communications, Arte, 21 5ª planta, 28033 Madrid, Spain

### Sweden

- Support E-mail: support@zyxel.se
- Sales E-mail: sales@zyxel.se
- Telephone: +46-31-744-7700
- Fax: +46-31-744-7701
- Web: www.zyxel.se
- Regular Mail: ZyXEL Communications A/S, Sjöporten 4, 41764 Göteborg, Sweden

### Taiwan

- Support E-mail: support@zyxel.com.tw
- Sales E-mail: sales@zyxel.com.tw
- Telephone: +886-2-27399889
- Fax: +886-2-27353220
- Web: http://www.zyxel.com.tw
- Address: Room B, 21F., No.333, Sec. 2, Dunhua S. Rd., Da-an District, Taipei

### Thailand

- Support E-mail: support@zyxel.co.th
- Sales E-mail: sales@zyxel.co.th
- Telephone: +662-831-5315
- Fax: +662-831-5395
- Web: http://www.zyxel.co.th
- Regular Mail: ZyXEL Thailand Co., Ltd., 1/1 Moo 2, Ratchaphruk Road, Bangrak-Noi, Muang, Nonthaburi 11000, Thailand.

### Turkey

- Support E-mail: cso@zyxel.com.tr
- Telephone: +90 212 222 55 22
- Fax: +90-212-220-2526
- Web: http:www.zyxel.com.tr
- Address: Kaptanpasa Mahallesi Piyalepasa Bulvari Ortadogu Plaza N:14/13 K:6 Okmeydani/Sisli Istanbul/Turkey

### Ukraine

- Support E-mail: support@ua.zyxel.com
- Sales E-mail: sales@ua.zyxel.com
- Telephone: +380-44-247-69-78
- Fax: +380-44-494-49-32
- Web: www.ua.zyxel.com
- Regular Mail: ZyXEL Ukraine, 13, Pimonenko Str., Kiev 04050, Ukraine

### United Kingdom

- Support E-mail: support@zyxel.co.uk
- Sales E-mail: sales@zyxel.co.uk
- Telephone: +44-1344-303044, 0845 122 0301 (UK only)
- Fax: +44-1344-303034
- Web: www.zyxel.co.uk
- Regular Mail: ZyXEL Communications UK Ltd., 11 The Courtyard, Eastern Road, Bracknell, Berkshire RG12 2XB, United Kingdom (UK)

# Index

## Numerics



## A



## B

## C



## D

## E



## F

## G



## H



## I

## L



## M

## N



## O



## P

## Q



## R



## S

## T

## U



## V



## W

## X



## Z