ZyWALL P1

Internet Security Appliance

User's Guide

Version 3.64
8/2005

ZyXEL

Copyright

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Federal Communications Commission (FCC) Interference Statement

This 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 equipment 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 commercial environment. This equipment 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.

If this equipment does cause harmful interference to radio/television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Notice 1

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Certifications

1. Go to www.zyxel.com
2. Select your product from the drop-down list box on the ZyXEL home page to go to that product's page.
3. Select the certification you wish to view from this page

Safety Warnings

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

- To reduce the risk of fire, use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.
- 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 can service the device. Please contact your vendor for further information.
- Use ONLY the dedicated power supply for your device. Connect the power cord or power adaptor to the right supply voltage (110V AC in North America or 230V AC in Europe).
- Do NOT use the device if the power supply is damaged as it might cause electrocution.
- If the power supply is damaged, remove it from the power outlet.
- Do NOT attempt to repair the power supply. Contact your local vendor to order a new power supply.
- Place connecting cables carefully so that no one will step on them or stumble over them. Do NOT allow anything to rest on the power cord and do NOT locate the product where anyone can walk on the power cord.
- If you wall mount your device, make sure that no electrical, gas or water pipes will be damaged.
- Do NOT install nor use your device during a thunderstorm. There may be a remote risk of electric shock from lightning.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Make sure to connect the cables to the correct ports.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Do NOT store things on the device.
- Connect ONLY suitable accessories to the device.

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 value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product is 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 of character to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Safety Warnings

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

- To reduce the risk of fire, use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.
- 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 can service the device. Please contact your vendor for further information.
- Use ONLY the dedicated power supply for your device. Connect the power cord or power adaptor to the right supply voltage (110V AC in North America or 230V AC in Europe).
- Do NOT use the device if the power supply is damaged as it might cause electrocution.
- If the power supply is damaged, remove it from the power outlet.
- Do NOT attempt to repair the power supply. Contact your local vendor to order a new power supply.

- Place connecting cables carefully so that no one will step on them or stumble over them. Do NOT allow anything to rest on the power cord and do NOT locate the product where anyone can walk on the power cord.
- If you wall mount your device, make sure that no electrical, gas or water pipes will be damaged.
- Do NOT install nor use your device during a thunderstorm. There may be a remote risk of electric shock from lightning.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Make sure to connect the cables to the correct ports.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Do NOT store things on the device.
- Connect ONLY suitable accessories to the device.

Customer Support

Please have the following information ready when you contact customer support.

- 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. .

METHOD / LOCATION	SUPPORT E-MAIL / SALES E-MAIL	TELEPHONE[A] / FAX	WEB SITE / FTP SITE	REGULAR MAIL
CORPORATE HEADQUARTERS (WORLDWIDE)	support@zyxel.com.tw	+886-3-578-3942	www.zyxel.com www.europe.zyxel.com	ZyXEL Communications Corp. 6 Innovation Road II Science Park Hsinchu 300 Taiwan
	sales@zyxel.com.tw	+886-3-578-2439	ftp.zyxel.com ftp.europe.zyxel.com	
CZECH REPUBLIC	info@cz.zyxel.com	+420 241 091 350	www.zyxel.cz	ZyXEL Communications Czech s.r.o. Modranská 621 143 01 Praha 4 - Modrany Ceská Republika
	info@cz.zyxel.com	+420 241 091 359		
DENMARK	support@zyxel.dk	+45 39 55 07 00	www.zyxel.dk	ZyXEL Communications A/S Columbusvej 5 2860 Soeborg Denmark
	sales@zyxel.dk	+45 39 55 07 07		
FINLAND	support@zyxel.fi	+358-9-4780-8411	www.zyxel.fi	ZyXEL Communications Oy Malminkaari 10 00700 Helsinki Finland
	sales@zyxel.fi	+358-9-4780 8448		
FRANCE	info@zyxel.fr	+33 (0)4 72 52 97 97	www.zyxel.fr	ZyXEL France 1 rue des Vergers Bat. 1 / C 69760 Limonest France
		+33 (0)4 72 52 19 20		
GERMANY	support@zyxel.de	+49-2405-6909-0	www.zyxel.de	ZyXEL Deutschland GmbH. Adenauerstr. 20/A2 D-52146 Wuerselen Germany
	sales@zyxel.de	+49-2405-6909-99		
NORTH AMERICA	support@zyxel.com	+1-800-255-4101 +1-714-632-0882	www.us.zyxel.com	ZyXEL Communications Inc. 1130 N. Miller St. Anaheim CA 92806-2001 U.S.A.
	sales@zyxel.com	+1-714-632-0858	ftp.us.zyxel.com	
NORWAY	support@zyxel.no	+47 22 80 61 80	www.zyxel.no	ZyXEL Communications A/S Nils Hansens vei 13 0667 Oslo Norway
	sales@zyxel.no	+47 22 80 61 81		
SPAIN	support@zyxel.es	+34 902 195 420	www.zyxel.es	ZyXEL Communications Alejandro Villegas 33 1º, 28043 Madrid Spain
	sales@zyxel.es	+34 913 005 345		
SWEDEN	support@zyxel.se	+46 31 744 7700	www.zyxel.se	ZyXEL Communications A/S Sjöporten 4, 41764 Göteborg Sweden
	sales@zyxel.se	+46 31 744 7701		

METHOD LOCATION	SUPPORT E-MAIL SALES E-MAIL	TELEPHONE[A] FAX	WEB SITE FTP SITE	REGULAR MAIL
UNITED KINGDOM	support@zyxel.co.uk	+44 (0) 1344 303044 08707 555779 (UK only)	www.zyxel.co.uk	ZyXEL Communications UK Ltd.,11 The Courtyard, Eastern Road, Bracknell, Berkshire, RG12 2XB, United Kingdom (UK)
	sales@zyxel.co.uk	+44 (0) 1344 303034	ftp.zyxel.co.uk	

a. "+" is the (prefix) number you enter to make an international telephone call.

Table of Contents

List of Figures

List of Tables

Preface

Congratulations on your purchase of the ZyWALL.

Note: 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.

Your ZyWALL is easy to install and configure.

About This User's Guide

This manual is designed to guide you through the configuration of your ZyWALL for its various applications.

Note: Use the web configurator or command interpreter interface (CLI) to configure your ZyWALL. Not all features can be configured through all interfaces.

Related Documentation

- Supporting Disk

  Refer to the included CD for support documents.

- Quick Start Guide

  The Quick Start Guide is designed to help you get up and running right away. It contains a detailed easy-to-follow connection diagram, default settings, handy checklists and 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.

- ZyXEL Glossary and Web Site

  Please refer to www.zyxel.com for an online glossary of networking terms and additional support documentation.

User Guide Feedback

Help us help you. E-mail all User Guide-related comments, questions or suggestions for improvement to techwriters@zyxel.com.tw or send regular mail to The Technical Writing Team, ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 300, Taiwan. Thank you!

Syntax Conventions

- "Enter" means for you to type one or more characters. "Select" or "Choose" means for you to use one predefined choices.

- Mouse action sequences are denoted using a comma. For example, "click the Apple icon, **Control Panels** and then **Modem**" means first click the Apple icon, then point your mouse pointer to **Control Panels** and then click **Modem**.
- For brevity's sake, we will use "e.g.," as a shorthand for "for instance", and "i.e.," for "that is" or "in other words" throughout this manual.
- The ZyWALL P1 Internet Security Appliance will be referred to as the ZyWALL in this U*ser's Guide*.

Graphics Icons Key

ZyWALL 	Computer 	Notebook computer 
Server 	DSLAM 	Firewall 
Telephone 	Switch 	Router 
VPN Tunnel		

CHAPTER 1
Getting to Know Your ZyWALL

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

1.1 Overview

The ZyWALL can be pre-configured by a network administrator makes an ideal plug-and-play security device for telecommuters who are always on the move and need a secure connection to the company network through the Internet

By integrating NAT, firewall, certificates and VPN capability, ZyXEL's ZyWALL is a complete security solution that protects your computer. In addition, the embedded web configurator is easy to operate.

1.2 ZyWALL Features

The following sections describe ZyWALL features.

Table 1 Feature Specifications

FEATURE	SPECIFICATION
Number of Static Routes	12
Number of NAT Sessions	2048
Number of IPSec VPN Tunnels/Security Associations	1

1.2.1 Physical Features

10/100 Mbps Ethernet LAN and WAN

The Ethernet ports are auto-negotiating and auto-crossover.

An auto-negotiating port can detect and adjust to the optimum Ethernet speed (10/100Mpbs) and duplex mode (full duplex or half duplex) of the connected device.

An auto-crossover (auto-MDI/MDI-X) port automatically works with a straight-through or crossover Ethernet cable.

Time and Date

The ZyWALL allows you to get the current time and date from an external server when you turn on your ZyWALL. You can also set the time manually. The Real Time Chip (RTC) keeps track of the time and date.

Reset Button

Use the reset button to restore the factory default password to 1234; IP address to 192.168.167.1, subnet mask to 255.255.255.0 and DHCP server enabled with a pool of 1 with 192.168.167.33 as the client IP address.

1.2.2 Non-Physical Features

IPSec VPN Capability

Establish a Virtual Private Network (VPN) to connect with business partners and branch offices using data encryption and the Internet to provide secure communications 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.

X-Auth (Extended Authentication)

X-Auth provides added security for VPN by requiring a VPN client to use a username and password.

Certificates

The ZyWALL can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. Certificates provide a way to exchange public keys for use in authentication.

SSH

The ZyWALL uses the SSH (Secure Shell) secure communication protocol to provide secure encrypted communication between two hosts over an unsecured network.

HTTPS

HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL is a web protocol that encrypts and decrypts web sessions. Use HTTPS for secure web configurator access to the ZyWALL

Firewall

The ZyWALL is a stateful inspection firewall with DoS (Denial of Service) protection. By default, when the firewall is activated, all incoming traffic from the WAN to the LAN is blocked unless it is initiated from the LAN. The ZyWALL firewall supports TCP/UDP inspection, DoS detection and prevention, real time alerts, reports and logs.

Universal Plug and Play (UPnP)

Using the standard TCP/IP protocol, the ZyWALL and other UPnP-enabled devices can dynamically join a network, obtain an IP address and convey its capabilities to other devices on the network.

PPPoE

PPPoE facilitates the interaction of a host with an Internet modem to achieve access to high-speed data networks via a familiar "dial-up networking" user interface.

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 a TCP/IP-based network.

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.

Dynamic DNS Support

With Dynamic DNS (Domain Name System) support, you can have a static hostname alias for a dynamic IP address, allowing the host to be more easily accessible from various locations on the Internet. You must register for this service with a Dynamic DNS service provider.

IP Multicast

Deliver IP packets to a specific group of hosts using IP multicast. IGMP (Internet Group Management Protocol) is the protocol used to support multicast groups. The latest version is version 2 (see RFC 2236); the ZyWALL supports both versions 1 and 2.

Static Route

Static routes tell the ZyWALL routing information that it cannot learn automatically through other means. This can arise in cases where RIP is disabled on the LAN or a remote network is beyond the one that is directly connected to a remote node.

Central Network Management

Central Network Management (CNM) allows an enterprise or service provider network administrator to manage your ZyWALL. The enterprise or service provider network administrator can configure your ZyWALL, perform firmware upgrades and do troubleshooting for you.

SNMP

SNMP (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).

Network Address Translation (NAT)

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).

Port Forwarding

Use this feature to forward incoming service requests to a server on your local network. 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.

DHCP (Dynamic Host Configuration Protocol)

DHCP (Dynamic Host Configuration Protocol) allows the individual client computers to obtain the TCP/IP configuration at start-up from a centralized DHCP server. The ZyWALL has built-in DHCP server capability, enabled by default, which means it can assign IP addresses, an IP default gateway and DNS servers to all systems that support the DHCP client.

Full Network Management

The embedded web configurator is an all-platform web-based utility that allows you to easily access the ZyWALL's management settings and configure the firewall.

RoadRunner Support

In addition to standard cable modem services, the ZyWALL supports Time Warner's RoadRunner Service.

Logging and Tracing

- Built-in message logging and packet tracing.
- Unix syslog facility support.

- Firewall logs.

Upgrade ZyWALL Firmware via LAN

The firmware of the ZyWALL can be upgraded via the LAN.

Embedded FTP and TFTP Servers

The ZyWALL's embedded FTP and TFTP servers enable fast firmware upgrades as well as configuration file backups and restoration.

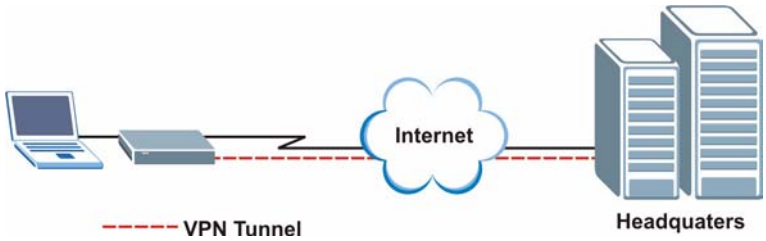
1.3 Applications

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

1.3.1 Secure Network Access for Telecommuters

The following figure shows a VPN network example. A telecommunter can simply connect the pre-configured ZyWALL and enter the VPN account information to establish a VPN connection through the Internet to headquaters.

Figure 1 Application: Telecommuters

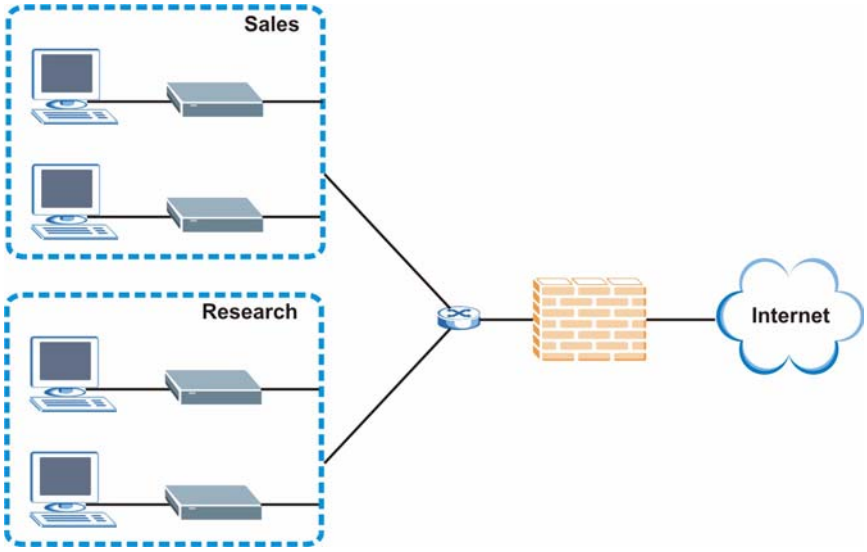


1.3.2 LAN Network Protection

In most cases, firewalls are deployed to protect the local network (LAN) from attacks originating from the WAN (such as the Internet). However, security outbreaks are possible on the LAN via other means (such as file shareing with removable storage devices). You can use the ZyWALL to provide network security on the LAN.

In the following example, computers in the Sales and Research departments are protected from each other by the ZyWALLs on the LAN.

Figure 2 Application: LAN Network Protection



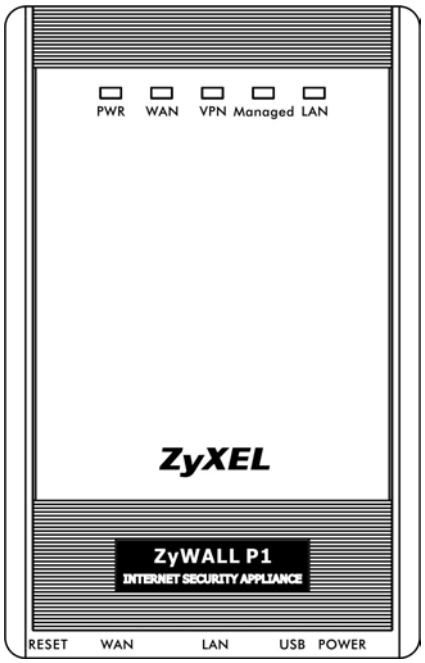
1.4 ZyWALL Hardware Connection

Refer to the Quick Start Guide for information on hardware connection and basic setup.

1.5 Front Panel LED

The LED and port labels are on the front panel.

Figure 3 Front Panel: LEDs



The following table describes the LEDs.

Table 2 Front Panel LEDs

LED	COLOR	STATUS	DESCRIPTION
PWR		Off	The ZyWALL is turned off.
	Green	On	The ZyWALL is turned on.
		Blinking	The ZyWALL is starting.
WAN		Off	The WAN connection is not ready, or has failed.
	Green	On	The ZyWALL has a successful 10Mbps WAN connection.
		Blinking	The 10M WAN is sending or receiving packets.
	Amber	On	The ZyWALL has a successful 100Mbps WAN connection.
		Blinking	The 100M WAN is sending or receiving packets.
VPN		Off	The ZyWALL does not have a VON connection.
	Green	On	The ZyWALL has a successful VPN connection.
		Blinking	The ZyWALL is receiving or sending data through the VPN connection.
Managed		Off	The ZyWALL does not have a CNM connection.
	Green	On	The ZyWALL has a successful CNM connection.
		Blinking	The ZyWALL is receiving or sending data using CNM.
LAN		Off	The LAN is not connected.
	Green	On	The ZyWALL has a successful 10Mbps LAN connection.
		Blinking	The 10M LAN is sending or receiving packets.
	Amber	On	The ZyWALL has a successful 100Mbps LAN connection.
		Blinking	The 100M LAN is sending or receiving packets.

CHAPTER 2
Introducing the Web Configurator

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

2.1 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).

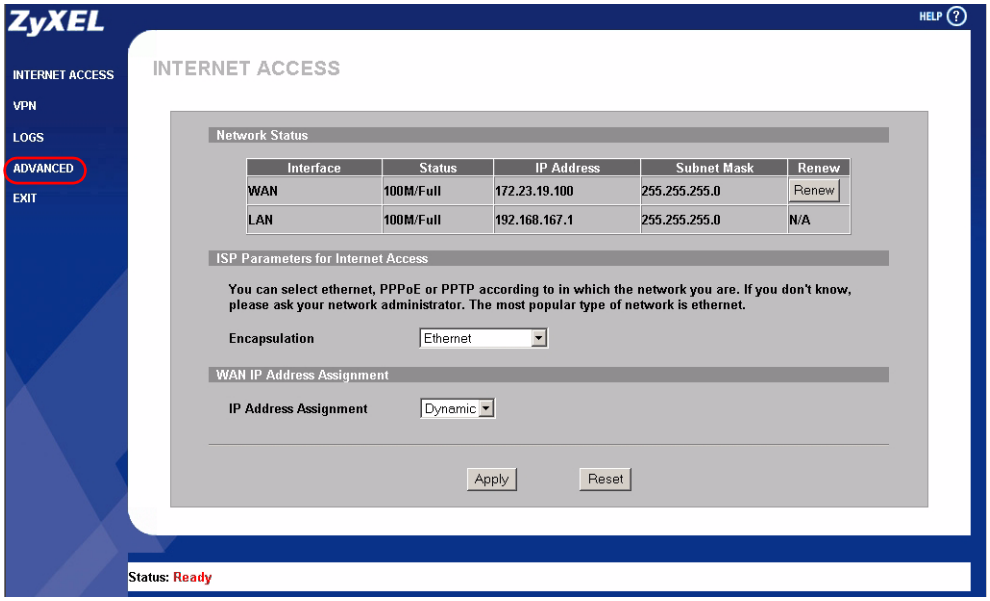
See the Troubleshooting chapter to see how to make sure these functions are allowed in Internet Explorer.

2.2 Accessing the Web Configurator

Follow the steps below to access the advanced web configurator screens.

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 "192.168.167.1" as the URL.
4. The initial screen displays. Refer to the Quick Start Guide for more information.
5. To log into the ZyWALL, click **ADVANCED** in the navigation panel.

Figure 4 Web Configurator: Initial Screen



6 A login screen displays. Type "1234" (default) as the password and click **Login**. In some versions, the default password appears automatically - if this is the case, click **Login**.

Figure 5 Web Configurator: Login Screen

7 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**.

Note: If you do not change the password, the following screen appears every time you log in.

Figure 6 Change Password Screen

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

Note: 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 7 Replace Certificate Screen

9 You should now see the **HOME** screen (see Figure 8 on page 43)

Note: 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.

2.3 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 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 password will be reset to 1234, also.

2.3.1 Procedure to Use the Reset Button

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

1. Press the **RESET** button in for about 10 seconds and release it. When the **PWR** LED starts 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 **PWR** LED will begin to blink. This indicates that the defaults have been restored. Release the **RESET** button.
5. Wait for the ZyWALL to finish restarting before accessing again.

2.4 Navigating the Web Configurator

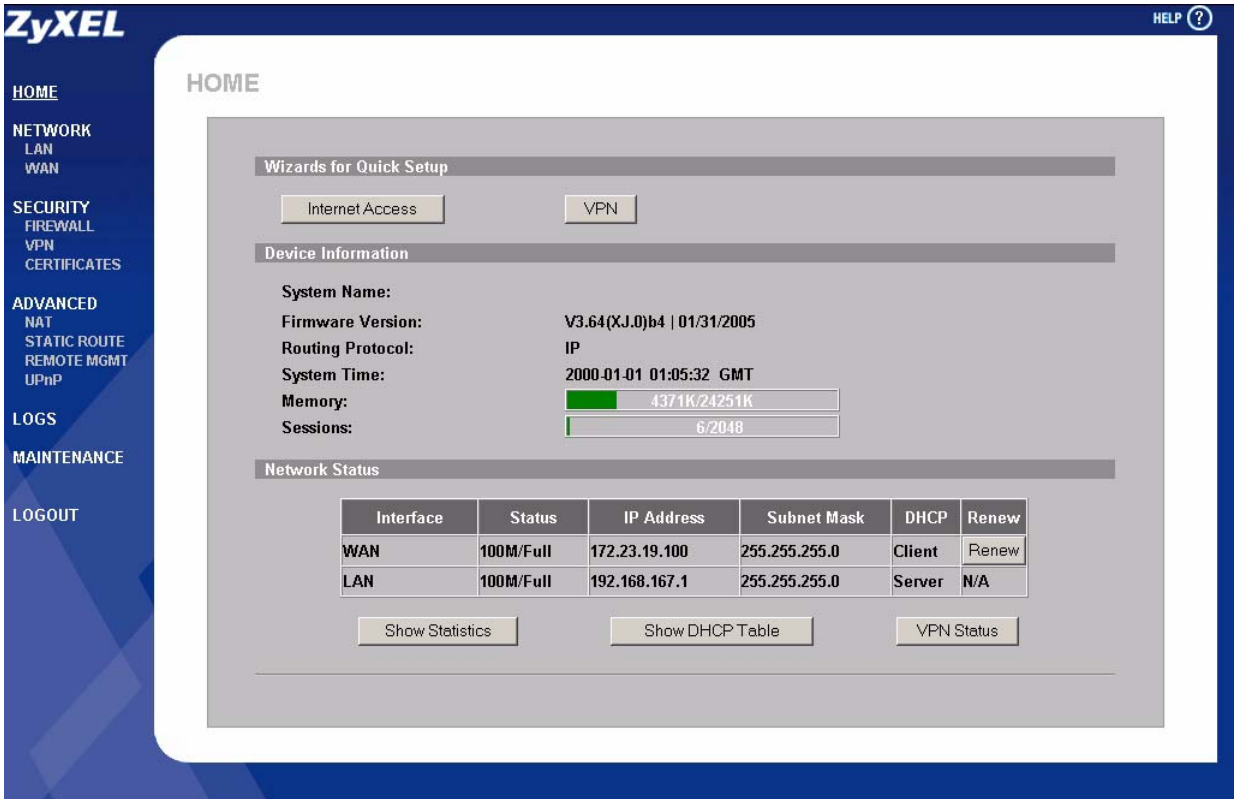
The following summarizes how to navigate the web configurator from the **HOME** screen.

Note: Follow the instructions you see in the **HOME** screen or click the HELP icon (located in the top right corner of most screens) to view online help.

2.4.1 The HOME Screen

The following screen shows the **HOME** screen.

Figure 8 Web Configurator: HOME



- Use the submenus to configure ZyWALL features.
- Click **LOGOUT** at any time to exit the web configurator.
- Click **MAINTENANCE** to view information about your ZyWALL or upgrade configuration/firmware files. Maintenance includes **General**, **Password**, **Time and Date**, **F/W** (firmware) **Upload**, **Configuration** (Backup, Restore, Default), and **Restart**.

The following table describes the labels in this screen.

Table 3 Web Configurator: HOME

LABEL	DESCRIPTION
Wizards for Quick Setup	
Internet Access	Click **Internet Access** to use the initial configuration wizard. .
VPN Wizard	Click **VPN Wizard** to create VPN policies.
Device Information	
System Name	This is the **System Name** you enter in the **MAINTENANCE General** screen. It is for identification purposes.
Firmware Version	This is the ZyNOS firmware version and the date created. ZyNOS is ZyXEL's proprietary Network Operating System (NOS) design.
Routing Protocol	This shows the routing protocol - **IP** for which the ZyWALL is configured. This field is not configurable.
System Time	This field displays your ZyWALL's present date and time.

Table 3 Web Configurator: HOME (continued)

LABEL	DESCRIPTION
Memory	The first number shows how many kilobytes 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. The second number shows the ZyWALL's total heap memory (in kilobytes). 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 • Initiated from the ZyWALL The second number is the maximum number of sessions that can be open at one time. 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.
Network Status	
Interface	This is the port type. Port types are: WAN and LAN.
Status	For the LAN port, this displays the port speed and duplex setting. For the WAN port, it displays the port speed and duplex setting if you're using Ethernet encapsulation and **Down** (line is down or not connected), **Idle** (line (ppp) idle), or **Drop** (dropping a call) if you're using PPPoE encapsulation.
IP Address	This shows the port's IP address.
Subnet Mask	This shows the port's subnet mask.
DHCP	This shows the WAN port's DHCP role - **Client** or **None**. This shows the LAN port's DHCP role - **Server** or **None**.
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 or PPPoE connection.
Show Statistics	Click **Show Statistics** to see performance statistics such as the number of packets sent and number of packets received for each port, including WAN and LAN.
Show DHCP Table	Click **Show DHCP Table** to show current DHCP client information.
VPN Status	Click **VPN Status** to display the active VPN connections.

2.4.2 Navigation Panel

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

Table 4 Navigation Panel: Menu 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.
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.
WAN	Route	This screen allows you to configure route priority and traffic redirect properties.
	WAN	Use this screen to configure ZyWALL WAN port for internet access.
	DDNS	Use this screen to configure dynamic DNS settings.
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.
VPN	VPN Rules (IKE)	Use this screen to configure VPN connections using IKE and view the rule summary.
	SA Monitor	Use this screen to display and manage active VPN connections.
	Global Setting	Use this screen to set the VPN traffic and gateway domain name update timers
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.
NAT	NAT Overview	Use this screen to enable NAT.
	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.

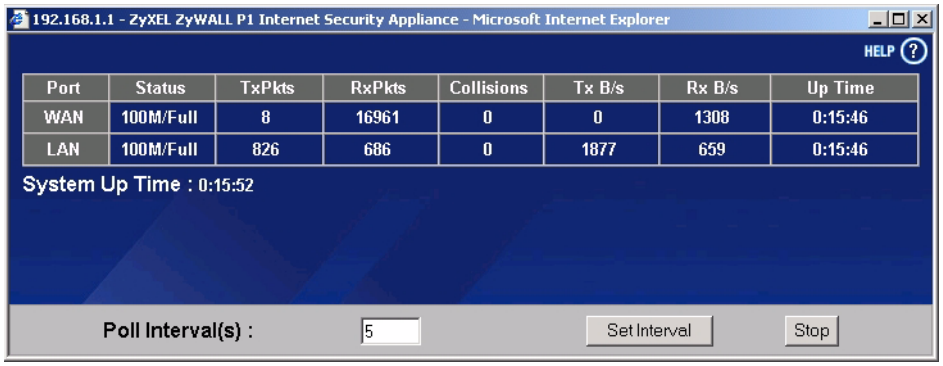
Table 4 Navigation Panel: Menu Summary (continued)

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 your ZyWALL's CNM (Central Network Management) settings to allow management from a remote 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.
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.
	Reports	Use this screen to have the ZyWALL record and display the network usage reports.
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.
	F/W Upload	Use this screen to upload firmware to your ZyWALL
	Configuration	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.
LOGOUT		Click this label to exit the web configurator.

2.4.3 System Statistics

Click **Show Statistics** in the **HOME** screen. Read-only information here includes port status and packet specific statistics. Also provided is "Up Time" and "poll interval(s)". The **Poll Interval(s)** field is configurable.

Figure 9 Home : Show Statistics



The following table describes the labels in this screen.

Table 5 Home: Show Statistics

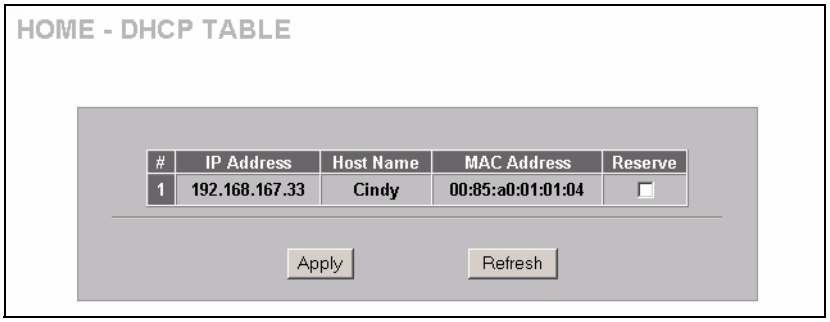
LABEL	DESCRIPTION
Port	This is the WAN or LAN port.
Status	This displays the port speed and duplex setting if you're using Ethernet encapsulation and **Down** (line is down), **Idle** (line (ppp) idle), **Dial** (starting to trigger a call) or **Drop** (dropping a call) if you're using PPPoE encapsulation.
TxPkts	This is the number of transmitted packets on this port.
RxPkts	This is the number of received packets on this port.
Collisions	This is the number of collisions 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.
Poll Interval(s)	Enter the time interval for refreshing statistics in this field.
Set Interval	Click this button to apply the new poll interval you entered in the **Poll Interval(s)** field.
Stop	Click **Stop** to stop refreshing statistics.

2.4.4 DHCP Table Screen

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 DHCP client. 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. 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 the network client using the ZyWALL's DHCP server.

Figure 10 Home: DHCP Table



The following table describes the labels in this screen.

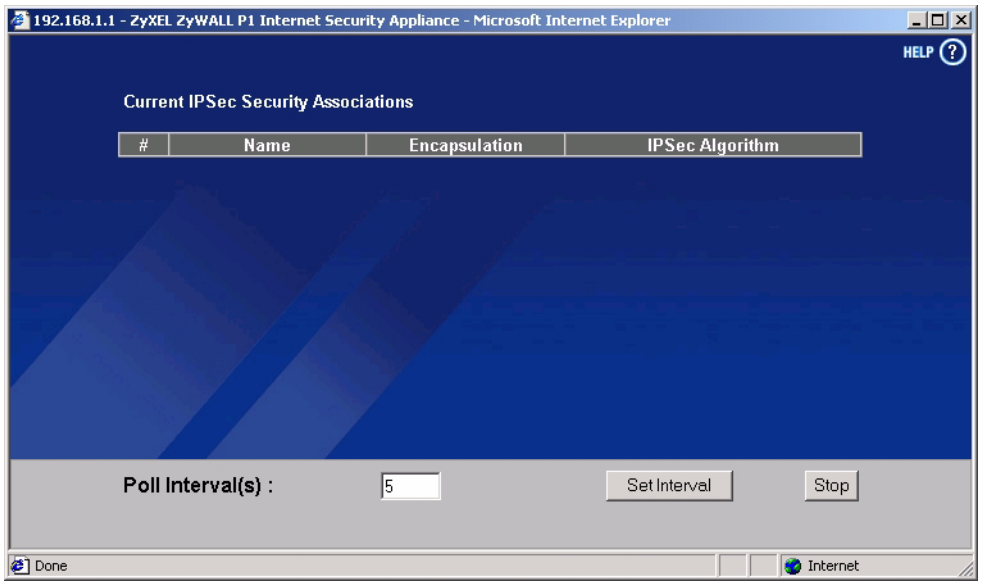
Table 6 Home: DHCP Table

LABEL	DESCRIPTION
#	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.
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). 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 this check box to have the ZyWALL always assign this IP address to this MAC address (and host name). You can select up to 8 entries in this table. After you click **Apply**, the MAC address and IP address also display in the **LAN Static DHCP** screen (where you can edit them).
Refresh	Click **Refresh** to reload the DHCP table.

2.4.5 VPN Status

Click **VPN Status** in the **HOME** screen when the ZyWALL. Read-only information here includes encapsulation mode and security protocol. The **Poll Interval(s)** field is configurable.

Figure 11 Home : VPN Status



The following table describes the labels in this screen.

Table 7 Home: VPN Status

LABEL	DESCRIPTION
#	This is the security association index number.
Name	This field displays the identification name for this VPN policy.
Encapsulation	This field displays **Tunnel** or **Transport** mode.
IPSec Algorithm	This field displays the security protocols used for an SA. Both AH and ESP increase ZyWALL processing requirements and communications latency (delay).
Poll Interval(s)	Enter the time interval for refreshing statistics in this field.
Set Interval	Click this button to apply the new poll interval you entered in the **Poll Interval(s)** field.
Stop	Click **Stop** to stop refreshing statistics.

CHAPTER 3
Wizard Setup

This chapter provides information on the Wizard Setup screens in the advanced web configurator.

3.1 Overview

The web configurator's setup wizards help you configure the WAN port on the ZyWALL to access the Internet and edit VPN policies and configure IKE settings to establish a VPN tunnel.

3.2 Internet Access Wizard Setup

The first Internet access wizard screen has three variations depending on what encapsulation type you use. Refer to your ISP checklist in the *Quick Start Guide* to know what to enter in each field. Leave a field blank if you don't have that information.

3.2.1 ISP Parameters

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

3.2.2 WAN and DNS

The second wizard screen allows you to configure WAN IP address assignment, DNS server address assignment and the WAN MAC address.

3.2.2.1 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 8 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.

Note: 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.

3.2.2.2 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. Let's say you select 192.168.1.0 as the network number; which 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, 192.168.167.1, 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.

3.2.2.3 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.

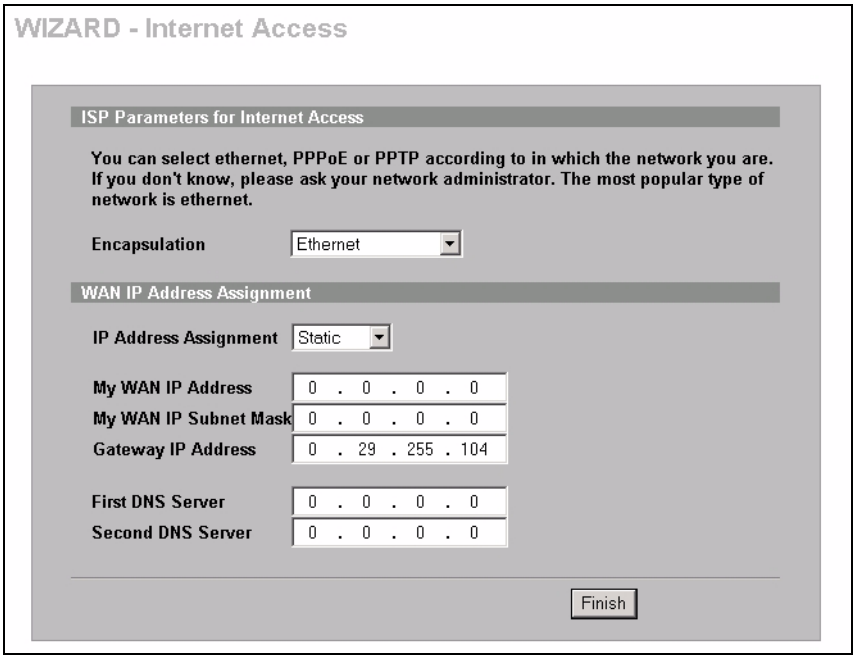
1. The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, manually enter them in the DNS server fields.
2. If your ISP dynamically assigns the DNS server IP addresses (along with the ZyWALL's WAN IP address), 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.

3.2.2.4 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 12 Internet Access Wizard: Ethernet Encapsulation



The following table describes the labels in this screen

.

Table 9 Internet Access Wizard: 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. **Note:** You can select a service type in the advanced WAN screen (refer to Section 5.3 on page 80).
WAN IP Address Assignment	Select **Dynamic** If your ISP did not assign you a fixed IP address. This is the default selection. Select **Static** If your ISP assigned a fixed IP address. The set the following fields.
My WAN IP Address	Enter your WAN IP address in this field if you select **Static** in the **WAN IP Address Assignment** field.
My WAN IP Subnet Mask	Enter the IP subnet mask in this field if you select **Static** in the **WAN IP Address Assignment** field.
Gateway IP Address	Enter the gateway IP address in this field if you select **Static** in the **WAN IP Address Assignment** field.
First/Second DNS Server	DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa, e.g., 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. Enter the IP address(es) of the DNS server(s) provided by your ISP.
Finish	Click **Finish** to save the settings.

3.2.2.5 PPPoE Encapsulation

Point-to-Point Protocol over Ethernet (PPPoE) functions as a dial-up connection. PPPoE is an IETF (Internet Engineering Task Force) draft standard specifying how a host personal computer interacts with a broadband modem (for example xDSL, cable, wireless, etc.) to achieve access to high-speed data networks. It preserves the existing Microsoft Dial-Up Networking experience and requires no new learning or procedures.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for instance, Radius). For the user, PPPoE provides a login and authentication method that the existing Microsoft Dial-Up Networking software can activate, and therefore requires no new learning or procedures for Windows users.

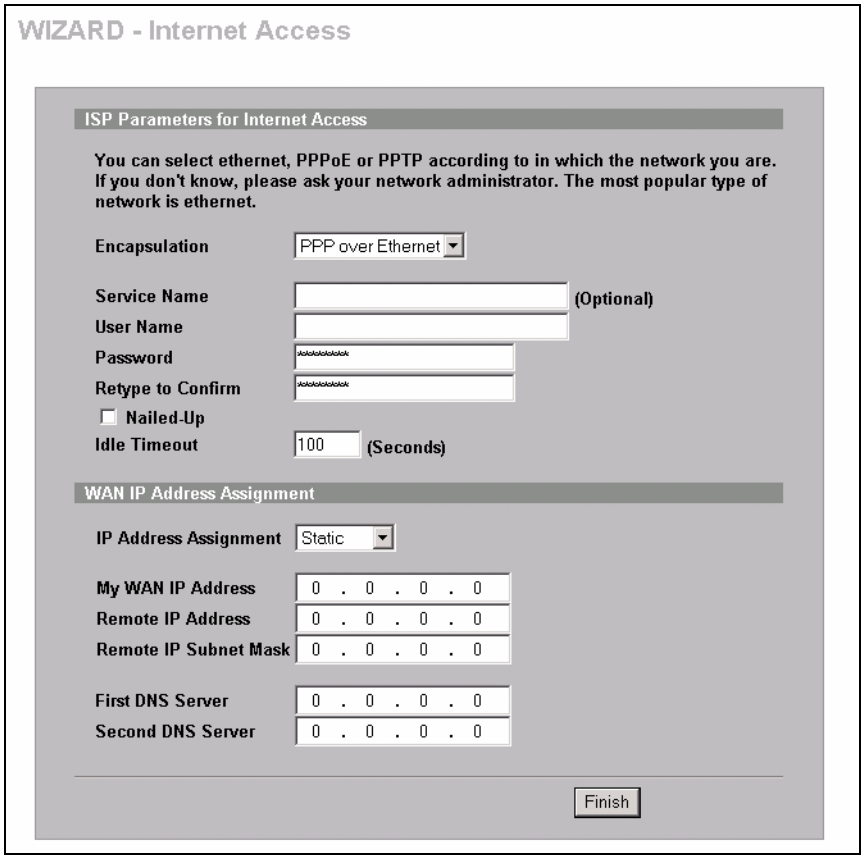
One of the benefits of PPPoE is the ability to let end users access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for specific users.

Operationally, PPPoE saves significant effort for both the subscriber and the ISP/carrier, as it requires no specific configuration of the broadband modem at the subscriber's 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 LAN's computers will have Internet access.

Refer to Appendix C on page 289 for more information on PPPoE.

Figure 13 Internet Access Wizard: PPPoE Encapsulation



The following table describes the related labels in this screen.

Table 10 Internet Access Wizard: 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 Password	Type your password again for confirmation.

Table 10 Internet Access Wizard: PPPoE Encapsulation (continued)

LABEL	DESCRIPTION
Nailed-Up Connection	Select **Nailed-Up Connection** 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.

Refer to Table 9 on page 54 for other label descriptions.

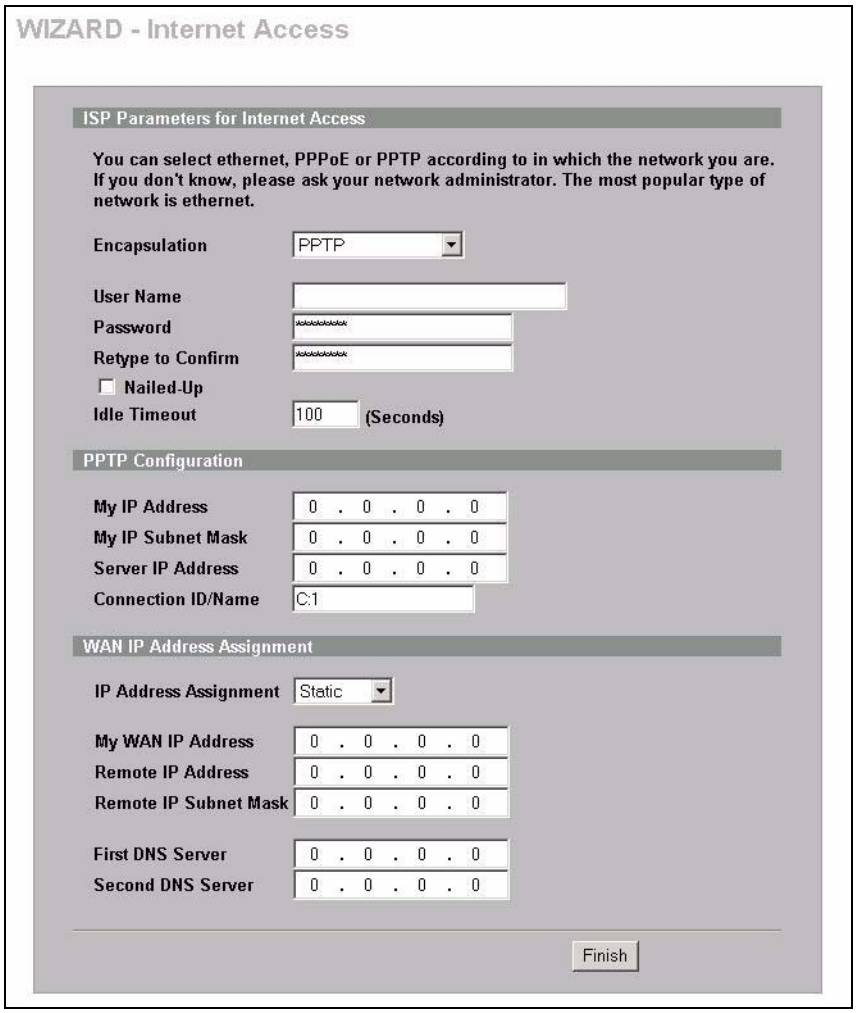
3.2.2.6 PPTP Encapsulation

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.

Note: Refer to Appendix D on page 291 for more information on PPTP. . The ZyWALL supports one PPTP server connection at any given time.

Figure 14 Internet Access Wizard: PPTP Encapsulation



The following table describes the related labels in this screen.

Table 11 Internet Access Wizard: PPTP Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	Select **PPTP** from the drop-down list box.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the User Name above.
Retype Password	Type your password again for confirmation.
Nailed-Up Connection	Select **Nailed-Up Connection** 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.

Table 11 Internet Access Wizard: PPTP Encapsulation (continued)

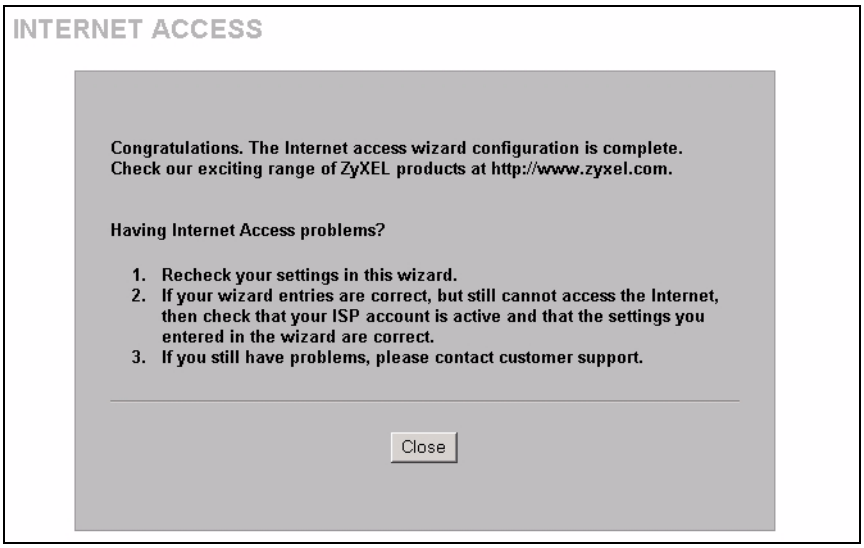
LABEL	DESCRIPTION
My IP Subnet Mask	Type the subnet mask assigned to you by your ISP (if given).
Server IP Address	Type the IP address of the PPTP server.
Connection ID/ Name	Enter the connection ID or connection name in this field. It must follow the "c:id" and "n:name" format. For example, C:12 or N:My ISP. This field is optional and depends on the requirements of your DSL modem.

Refer to Table 9 on page 54 for other label descriptions.

3.2.3 Internet Access Wizard Setup Complete

Well done! You have successfully set up your ZyWALL to operate on your network and access the Internet.

Figure 15 Internet Access Wizard: Complete



3.3 VPN Wizard Setup

A VPN (Virtual Private Network) 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 technologies/services used to transport traffic over the Internet or any insecure network that uses the TCP/IP protocol suite for communication.

Use the VPN wizard screens to configure a VPN rule that use a pre-shared key. If you want to set the rule to use a certificate, please go to the advanced VPN screens for configuration.

3.3.1 IPSec

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.

3.3.2 Security Association

A Security Association (SA) is a contract between two parties indicating what security parameters, such as keys and algorithms they will use.

3.3.3 My IP Address

My IP Address identifies the WAN IP address of the ZyWALL. You can enter the ZyWALL's static WAN IP address (if it has one) or leave the field set to **0.0.0.0**. The ZyWALL has to rebuild the VPN tunnel if the **My IP Address** changes after setup.

3.3.4 Secure Gateway Address

Secure Gateway Address is the WAN IP address or domain name of the remote IPSec router (secure gateway).

If the remote secure gateway has a static WAN IP address, enter it in the **Secure Gateway Address** field. You may alternatively enter the remote secure gateway's domain name (if it has one) in the **Secure Gateway Address** field.

You can also enter a remote secure gateway's domain name in the **Secure Gateway Address** field if the remote secure gateway has a dynamic WAN IP address and is using DDNS. The ZyWALL has to rebuild the VPN tunnel each time the remote secure gateway's WAN IP address changes (there may be a delay until the DDNS servers are updated with the remote gateway's new WAN IP address).

3.3.4.1 Dynamic Secure Gateway Address

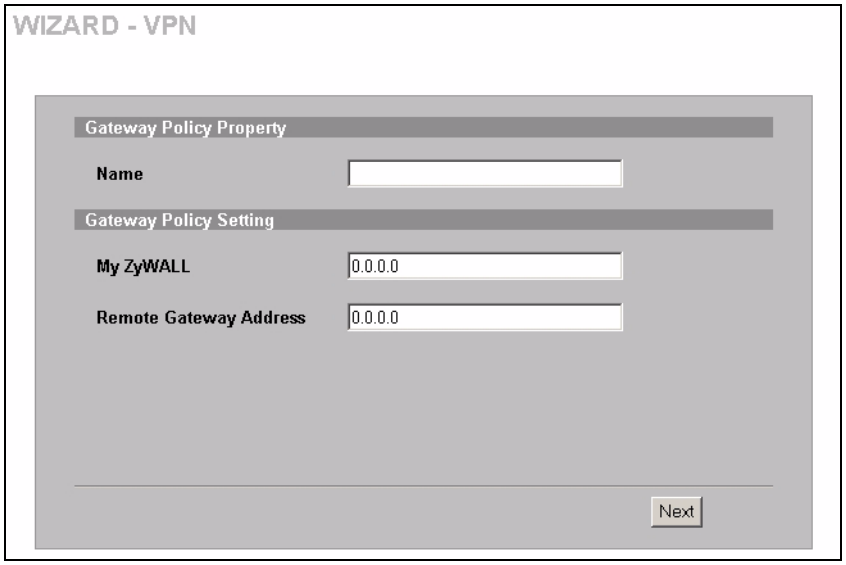
If the remote secure gateway has a dynamic WAN IP address and does not use DDNS, enter 0.0.0.0 as the secure gateway's address. In this case only the remote secure gateway can initiate SAs. This may be useful for telecommuters initiating a VPN tunnel to the company network.

3.3.5 VPN Wizard: Gateway Policy Setting

Click **VPN Wizard** in the **HOME** screen to open the screen as shown and have the quick and initial VPN configuration.

Configure the first VPN wizard screen to configure the settings between the ZyWALL and the remote VPN router.

Figure 16 VPN Wizard: Gateway Policy Setting



The following table describes the labels in this screen.

Table 12 VPN Wizard: Gateway Policy Setting

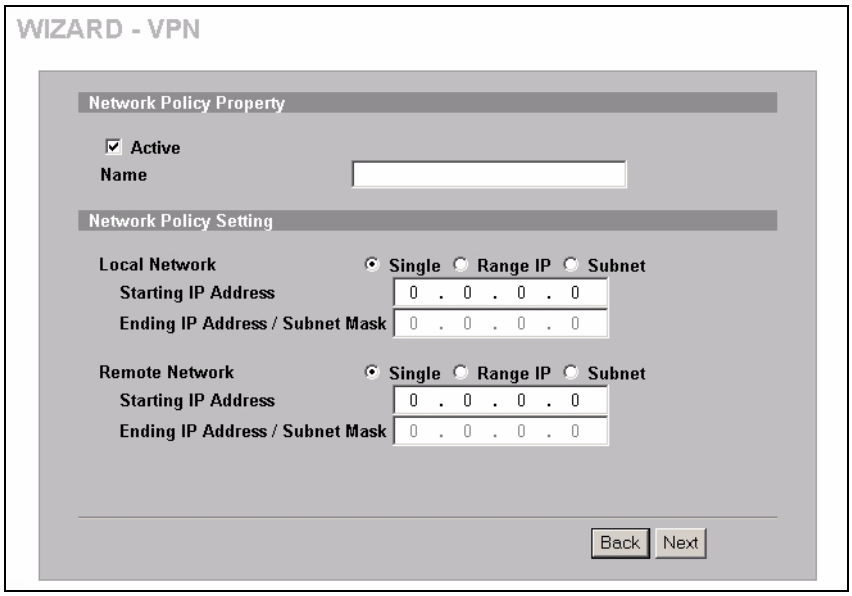
LABEL	DESCRIPTION
Gateway Policy Property	
Name	Type up to 32 characters to identify this VPN gateway policy. You may use any character, including spaces, but the ZyWALL drops trailing spaces.
Gateway Policy Setting	
My ZyWALL	Enter the WAN IP address or the domain name of your ZyWALL. The ZyWALL uses its current WAN IP address (static or dynamic) in setting up the VPN tunnel if you leave this field as **0.0.0.0**. The ZyWALL has to rebuild the VPN tunnel if the IP address changes after setup.
Remote Gateway	Enter the WAN IP address or the domain name 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.
Next	Click **Next** to continue.

3.3.6 VPN Wizard: Network Setting

Use the second VPN wizard screen to configure the settings for each LAN network behind the ZyWALL and the remote VPN router.

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 17 VPN Wizard: Network Setting



The following table describes the labels in this screen.

Table 13 VPN Wizard: Network Setting

LABEL	DESCRIPTION
Network Policy Property	
Active	Select this checkbox to enable this VPN rule.
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. 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. 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.

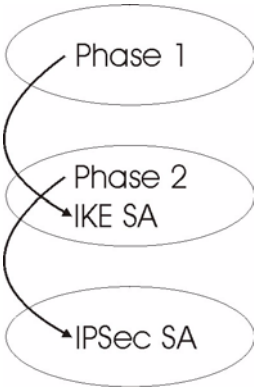
Table 13 VPN Wizard: Network Setting (continued)

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 not applicable. 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.

3.3.7 IKE Phases

There are two phases to every IKE (Internet Key Exchange) negotiation – phase 1 (Authentication) and phase 2 (Key Exchange). A phase 1 exchange establishes an IKE SA and the second one uses that SA to negotiate SAs for IPSec.

Figure 18 Two Phases to Set Up the IPSec SA



In phase 1 you must:

- Choose a negotiation mode.
- Authenticate the connection by entering a pre-shared key.
- Choose an encryption algorithm.
- Choose an authentication algorithm.
- Choose a Diffie-Hellman public-key cryptography key group (**DH1** or **DH2**).
- Set the IKE SA lifetime. This field allows you to determine how long an IKE SA should stay up before it times out. An IKE SA times out when the IKE SA lifetime period expires. If an IKE SA times out when an IPSec SA is already established, the IPSec SA stays connected.

In phase 2 you must:

- Choose which protocol to use (**ESP** or **AH**) for the IKE key exchange.
- Choose an encryption algorithm.
- Choose an authentication algorithm
- Choose whether to enable Perfect Forward Secrecy (PFS) using Diffie-Hellman public-key cryptography (see Section 3.3.7 on page 62). Select **None** (the default) to disable PFS.
- Choose **Tunnel** mode or **Transport** mode.
- Set the IPSec SA lifetime. This field allows you to determine how long the IPSec SA should stay up before it times out. The ZyWALL automatically renegotiates the IPSec SA if there is traffic when the IPSec SA lifetime period expires. The ZyWALL also automatically renegotiates the IPSec SA if both IPSec routers have keep alive enabled, even if there is no traffic. If an IPSec SA times out, then the IPSec router must renegotiate the SA the next time someone attempts to send traffic.

3.3.7.1 Negotiation Mode

The phase 1 **Negotiation Mode** you select determines how the Security Association (SA) will be established for each connection through IKE negotiations.

- **Main Mode** ensures the highest level of security when the communicating parties are negotiating authentication (phase 1). It uses 6 messages in three round trips: SA negotiation, Diffie-Hellman exchange and an exchange of nonces (a nonce is a random number). This mode features identity protection (your identity is not revealed in the negotiation).
- **Aggressive Mode** is quicker than **Main Mode** because it eliminates several steps when the communicating parties are negotiating authentication (phase 1). However the trade-off is that faster speed limits its negotiating power and it also does not provide identity protection. It is useful in remote access situations where the address of the initiator is not know by the responder and both parties want to use pre-shared key authentication.

3.3.7.2 Pre-Shared Key

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.

3.3.7.3 Diffie-Hellman (DH) Key Groups

Diffie-Hellman (DH) is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communications channel. Diffie-Hellman is used within IKE SA setup to establish session keys. 768-bit (Group 1 - **DH1**) and 1024-bit (Group 2 – **DH2**) Diffie-Hellman groups are supported. Upon completion of the Diffie-Hellman exchange, the two peers have a shared secret, but the IKE SA is not authenticated. For authentication, use pre-shared keys.

3.3.7.4 Perfect Forward Secrecy (PFS)

Enabling PFS means that the key is transient. The key is thrown away and replaced by a brand new key using a new Diffie-Hellman exchange for each new IPSec SA setup. With PFS enabled, if one key is compromised, previous and subsequent keys are not compromised, because subsequent keys are not derived from previous keys. The (time-consuming) Diffie-Hellman exchange is the trade-off for this extra security.

This may be unnecessary for data that does not require such security, so PFS is disabled (**None**) by default in the ZyWALL. Disabling PFS means new authentication and encryption keys are derived from the same root secret (which may have security implications in the long run) but allows faster SA setup (by bypassing the Diffie-Hellman key exchange).

3.4 IPSec Algorithms

The **ESP** and **AH** protocols are necessary to create a Security Association (SA), the foundation of an IPSec VPN. An SA is built from the authentication provided by the **AH** and **ESP** protocols. The primary function of key management is to establish and maintain the SA between systems. Once the SA is established, the transport of data may commence.

3.4.1 AH (Authentication Header) Protocol

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.

In applications where confidentiality is not required or not sanctioned by government encryption restrictions, an **AH** can be employed to ensure integrity. This type of implementation does not protect the information from dissemination but will allow for verification of the integrity of the information and authentication of the originator.

3.4.2 ESP (Encapsulating Security Payload) Protocol

The **ESP** protocol (RFC 2406) provides encryption as well as some of the services offered by **AH**. **ESP** authenticating properties are limited compared to the **AH** due to the non-inclusion of the IP header information during the authentication process. However, **ESP** is sufficient if only the upper layer protocols need to be authenticated.

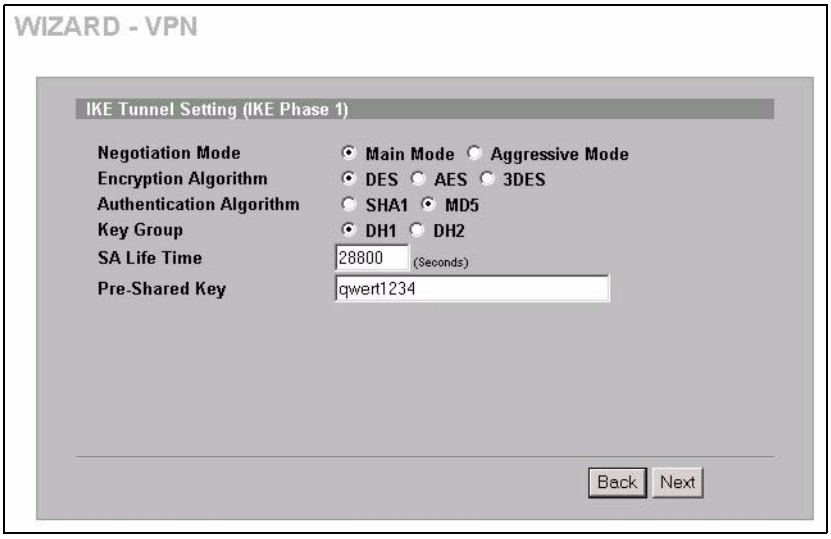
An added feature of the **ESP** is payload padding, which further protects communications by concealing the size of the packet being transmitted.

Table 14 ESP and AH

	ESP	AH
Encryption	**DES** (default) Data Encryption Standard (DES) is a widely used method of data encryption using a secret key. DES applies a 56-bit key to each 64-bit block of data.	
	3DES Triple DES (3DES) is a variant of DES, which iterates three times with three separate keys (3 x 56 = 168 bits), effectively doubling the strength of DES.	
	AES Advanced Encryption Standard is a newer method of data encryption that also uses a secret key. This implementation of AES applies a 128-bit key to 128-bit blocks of data. AES is faster than 3DES.	
	Select **NULL** to set up a phase 2 tunnel without encryption.	
Authentication	**MD5** (default) MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.	**MD5** (default) MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.
	SHA1 SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.	**SHA1** SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.
	Select **MD5** for minimal security and **SHA-1** for maximum security.	

3.4.3 IKE Tunnel Setting (IKE Phase 1)

Figure 19 VPN Wizard: IKE Tunnel Setting



The following table describes the labels in this screen.

Table 15 VPN Wizard: IKE Tunnel Setting

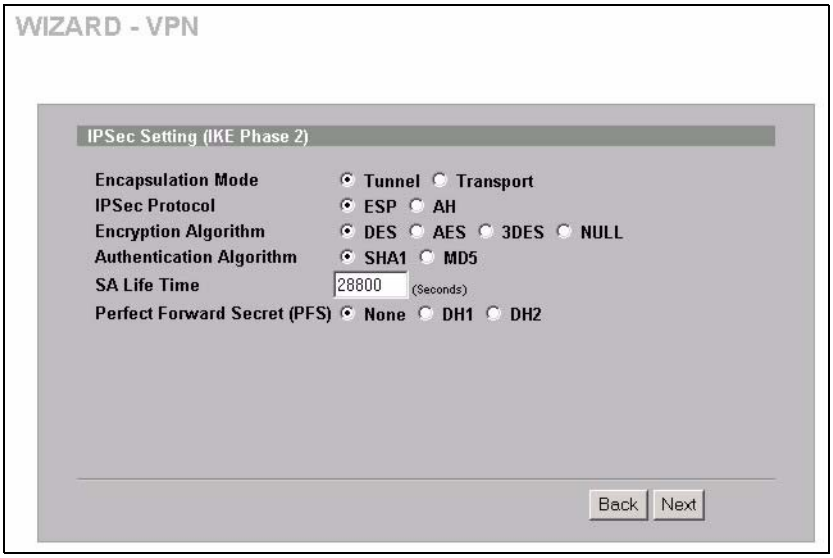
LABEL	DESCRIPTION
Negotiation Mode	Use the radio buttons to select **Main Mode** or **Aggressive Mode**. Multiple SAs connecting through a secure gateway must have the same negotiation mode.
Encryption Algorithm	When **DES** is used for data communications, both sender and receiver must know the same 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 (1Kb) 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. 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 15 VPN Wizard: IKE Tunnel Setting (continued)

LABEL	DESCRIPTION
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. 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. 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.

3.4.4 IPSec Setting (IKE Phase 2)

Figure 20 VPN Wizard: IPSec Setting



The following table describes the labels in this screen.

Table 16 VPN Wizard: IPSec Setting

LABEL	DESCRIPTION
Encapsulation Mode	Select **Tunnel** mode or **Transport** mode.
IPSec Protocol	Select the security protocols used for an SA. Both **AH** and **ESP** increase ZyWALL processing requirements and communications latency (delay).

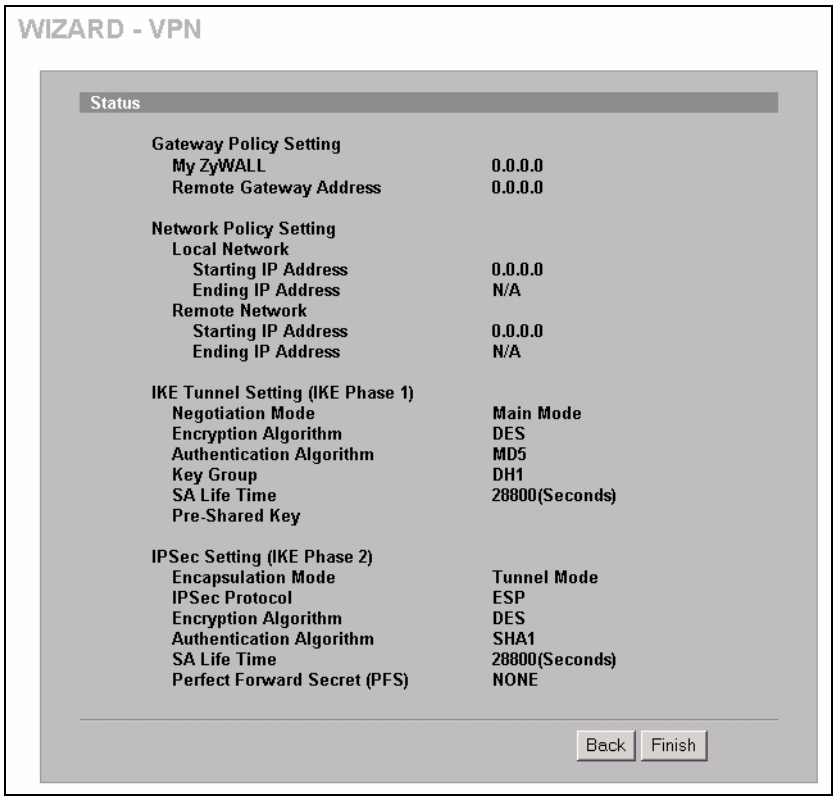
Table 16 VPN Wizard: IPSec Setting (continued)

LABEL	DESCRIPTION
Encryption Algorithm	When **DES** is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on DES that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. 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. A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Perfect Forward Secret (PFS)	Perfect Forward Secret (PFS) is disabled (**None**) by default in phase 2 IPSec SA setup. This allows faster IPSec setup, but is not so secure. Select **DH1** or **DH2** 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).
Back	Click **Back** to return to the previous screen.
Next	Click **Next** to continue.

3.4.5 VPN 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 21 VPN Wizard: VPN Status



The following table describes the labels in this screen.

Table 17 VPN Wizard: VPN Status

LABEL	DESCRIPTION
Gateway Setting	
My ZyWALL	This is the WAN IP address or domain name of your ZyWALL.
Remote Gateway Address	This is the IP address or domain name used to identify the remote IPSec router.
Network 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 not applicable. 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 not applicable. 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.

Table 17 VPN Wizard: VPN Status (continued)

LABEL	DESCRIPTION
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.
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** or **DH2** are selected to enable PFS.
Back	Click **Back** to return to the previous screen.
Finish	Click **Finish** to complete and save the wizard setup.

3.4.6 VPN Wizard Setup Complete

Congratulations! You have successfully set up the VPN rule after any existing rule(s) for your ZyWALL.

Figure 22 VPN Wizard: Complete

CHAPTER 4
LAN Screens

This chapter describes how to configure LAN settings.

4.1 LAN Overview

Local Area Network (LAN) is a shared communication system to which many computers are attached. The LAN screens can help you configure a LAN DHCP server and manage IP addresses.

4.2 DHCP Setup

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 DHCP client. If DHCP service is disabled, you must have another DHCP server on your LAN, or else the computer must be manually configured.

4.2.1 IP Pool Setup

The ZyWALL is pre-configured to provide one IP address of 169.254.1.33 to a DHCP client. This configuration leaves 253 IP addresses (excluding the ZyWALL itself) in the lower range for other server computers, for instance, servers for mail, FTP, TFTP, web, etc., that you may have.

4.2.2 DNS Servers

Use the **DNS** screens to configure the DNS server information that the ZyWALL sends to the DHCP client devices on the LAN.

There are three places where you can configure DNS setup on the ZyWALL.

1. Use the **MAINTENANCE General** screen to configure the ZyWALL to use a DNS server to resolve domain names for ZyWALL system features like VPN, DDNS and the time server.
2. Use the **LAN** screen to configure the DNS server information that the ZyWALL sends to the DHCP client devices on the LAN.

4.3 LAN TCP/IP

The ZyWALL has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

4.3.1 Factory LAN Defaults

The LAN parameters of the ZyWALL are preset in the factory with the following values:

- IP address of 192.168.167.1 with subnet mask of 255.255.255.0.
- DHCP server enabled with one client IP address of 192.168.167.33.

These parameters should work for the majority of installations. If your ISP gives you explicit DNS server address(es), read the embedded web configurator help regarding what fields need to be configured.

4.3.2 IP Address and Subnet Mask

Refer to Section 3.2.2.2 on page 52 for this information.

4.3.3 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**.

4.3.4 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.

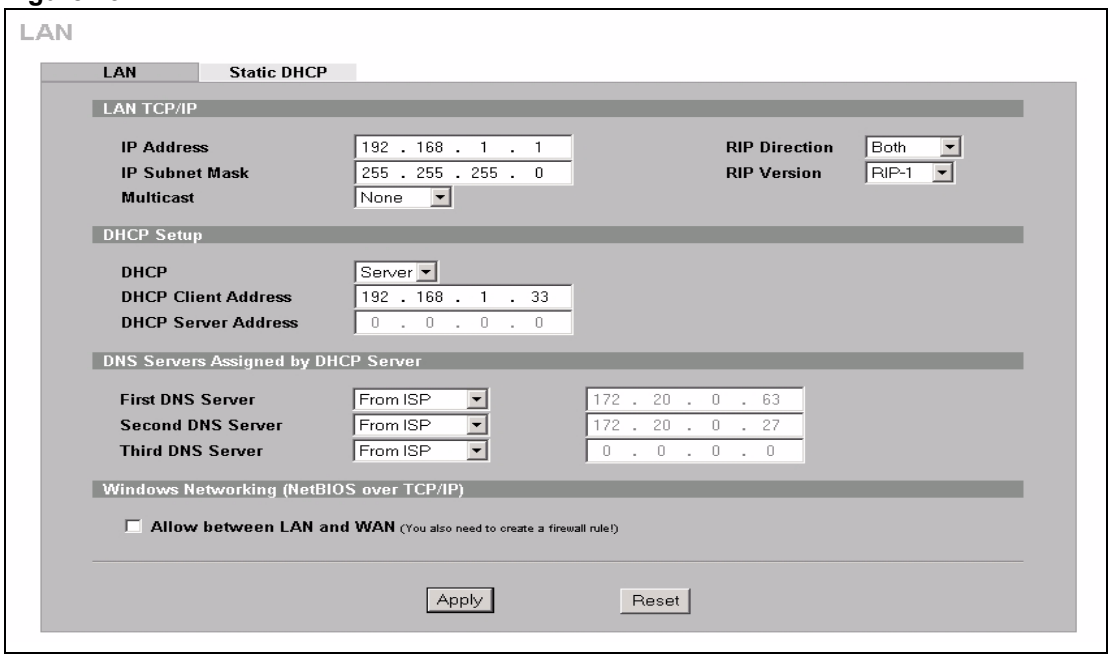
IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed 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.

4.4 Configuring LAN

Click **LAN** to open the **LAN** screen.

Figure 23 LAN: LAN



The following table describes the labels in this screen.

Table 18 LAN: LAN

LABEL	DESCRIPTION
LAN TCP/IP	
IP Address	Type the IP address of your ZyWALL in dotted decimal notation. 192.168.167.1 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 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. **Both** is the default.
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 Multicast 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. Select **Server** to set the ZyWALL to assign network information (IP address, DNS information etc.) to an Ethernet device connected to the **LAN** port. Select **None** to to stop the ZyWALL from acting as a DHCP server. you must have another DHCP server on your LAN, or else the computer must be manually configured. Select **Relay** to set the ZyWALL to forward network configuration requests to a DHCP server on the LAN network
DHCP Client Address	This field is applicable when you select **Server** in the **DHCP** field. Specify the IP address for the DHCP client. Make sure the IP address is in the same range as the ZyWALL's LAN IP address.
DHCP Server Address	This field is applicable when you select **Relay** in the **DHCP** field. Enter the IP address (in dotted decimal notation) of a DHCP server on the LAN.

Table 18 LAN: LAN (continued)

LABEL	DESCRIPTION
DNS Servers Assigned by DHCP Server	The ZyWALL passes a DNS (Domain Name System) server IP address (in the order you specify here) to the DHCP client. The ZyWALL only passes this information to the LAN DHCP client when you select the **DHCP Server** check box. When you clear the **DHCP Server** check box, DHCP service is disabled and you must have another DHCP sever on your LAN, or else the computers must have their DNS server addresses manually configured.
First DNS Server Second DNS Server Third DNS Server	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. 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**. Select **DNS Relay** to have the ZyWALL act as a DNS proxy. The ZyWALL's LAN IP address displays in the field to the right (read-only). The ZyWALL tells the DHCP client on the LAN that the ZyWALL itself is the DNS server. When a computer on the LAN 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**. Select **None** 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 computer in order to access it.
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 WAN	Select this check box to forward NetBIOS packets from the LAN to the WAN and from the WAN to the LAN. If your firewall is enabled with the default policy set to block WAN to LAN traffic, you also need to enable the default WAN to LAN firewall rule that forwards NetBIOS traffic. Clear this check box to block all NetBIOS packets going from the LAN to the WAN and from the WAN to the LAN.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

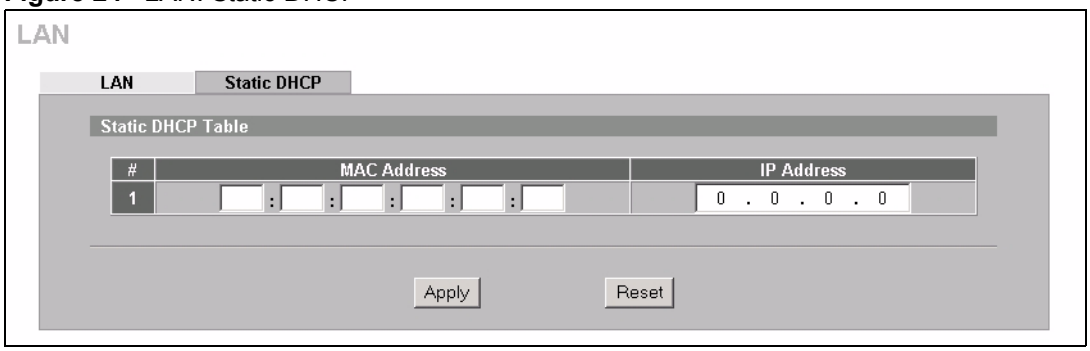
4.5 Configuring Static DHCP

This table allows you to assign one IP address on the LAN to a specific computer based on the 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.

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

Figure 24 LAN: Static DHCP



The following table describes the labels in this screen.

Table 19 LAN: Static DHCP

LABEL	DESCRIPTION
#	This is the index number of the Static IP table entry (row).
MAC Address	Type the MAC address (with colons) 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.

CHAPTER 5
WAN Screens

This chapter describes how to configure WAN settings.

5.1 WAN Overview

See Chapter 3 on page 51 for more information on the fields in the WAN screens.

5.1.1 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".

The metric sets the priority for the ZyWALL's routes to the Internet. Each route must have a unique metric.

5.1.2 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.

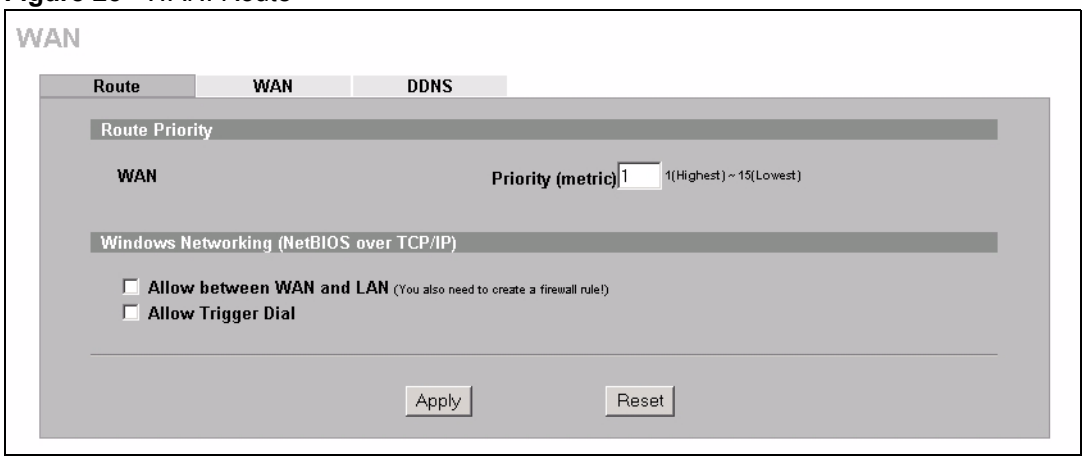
Table 20 Example of Network Properties for LAN Servers with Fixed IP Addresses

Choose an IP address	192.168.167.2 ~ 192.168.167.32; 192.168.167.34 ~ 192.168.167.254.
Subnet mask	255.255.255.0
Gateway (or default route)	192.168.167.1(ZyWALL LAN IP)

5.2 WAN Route Setup

Click **WAN** to open the **Route** screen.

Figure 25 WAN: Route



The following table describes the labels in this screen.

Table 21 WAN: Route

LABEL	DESCRIPTION
Route Priority	
WAN	The default WAN connection is "1" as your broadband connection via the WAN port should always be your preferred method of accessing the WAN.
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 WAN and LAN	Select this check box to forward NetBIOS packets from the LAN to the WAN and from the WAN to the LAN. If your firewall is enabled with the default policy set to block WAN to LAN traffic, you also need to enable the default WAN to LAN firewall rule that forwards NetBIOS traffic. Clear this check box to block all NetBIOS packets going from the LAN to the WAN and from the WAN to the LAN.
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.

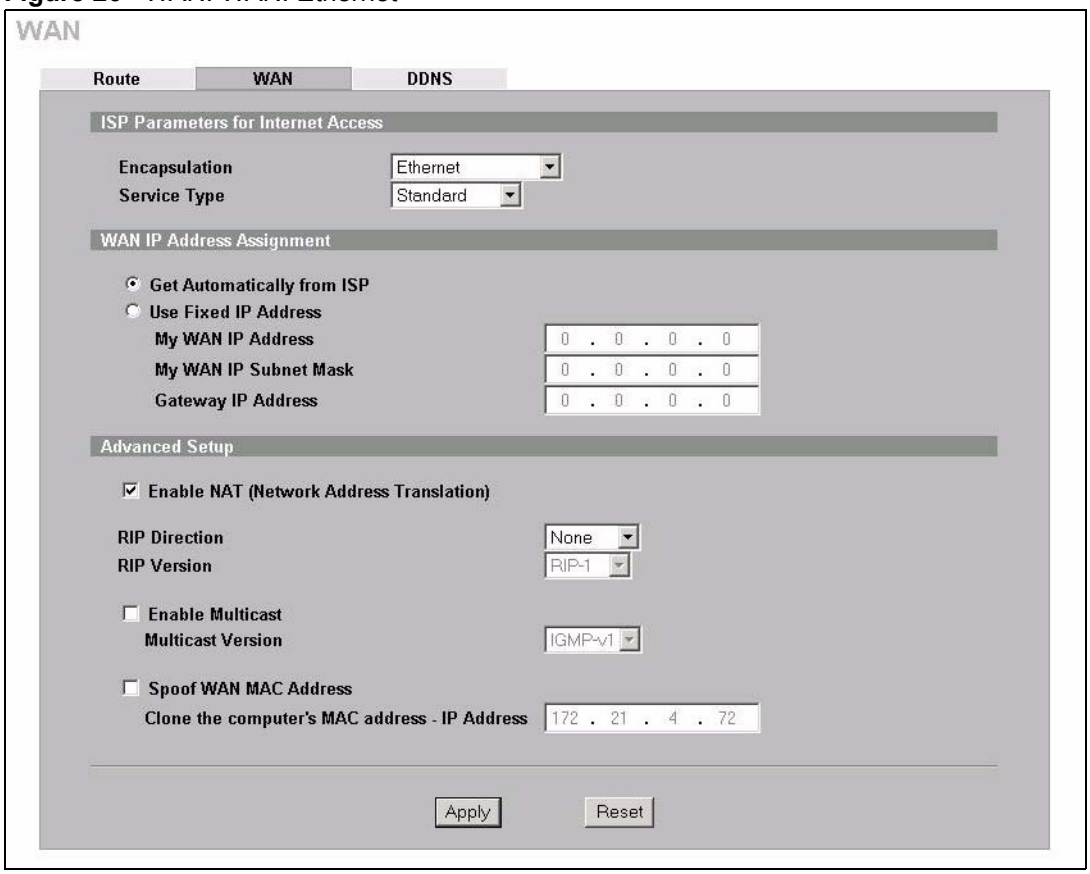
5.3 Configuring WAN Setup

To change your ZyWALL's WAN ISP, IP and MAC settings, click **WAN**, then the **WAN** tab. The screen differs by the encapsulation.

5.3.1 Ethernet Encapsulation

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

Figure 26 WAN: WAN: Ethernet



The following table describes the labels in this screen.

Table 22 WAN: WAN: Ethernet

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**. 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.
Login Server IP Address	Type the authentication server IP address here if your ISP gave you one. 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.

Table 22 WAN: WAN: Ethernet (continued)

LABEL	DESCRIPTION
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). Select this checkbox to enable NAT. For more information about NAT see Chapter 11 on page 177.
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. Choose **Both**, **None**, **In Only** or **Out Only**. When set to **Both** or **Out Only**, the ZyWALL will broadcast its routing table periodically. When set to **Both** or **In Only**, the ZyWALL will incorporate RIP information that it receives. When set to **None**, the ZyWALL will not send any RIP packets and will ignore any RIP packets received. 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). Choose **RIP-1**, **RIP-2B** or **RIP-2M**. **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 Multicast Protocol). IGMP is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data.

Table 22 WAN: WAN: Ethernet (continued)

LABEL	DESCRIPTION
Multicast Version	Choose **None** (default), **IGMP-V1** or **IGMP-V2**. IGMP (Internet Group Multicast 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 interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236.
Spoof WAN MAC Address	You can use the factory assigned default MAC Address or cloning the MAC address from a computer on your LAN. Otherwise, select the check box next to **Spoof WAN MAC Address** 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. 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.

5.3.2 PPPoE Encapsulation

The ZyWALL supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF Draft standard (RFC 2516) specifying how a computer 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). PPPoE provides a login and authentication method that the existing Microsoft Dial-Up Networking software can activate, and therefore requires no new learning or procedures for Windows users.

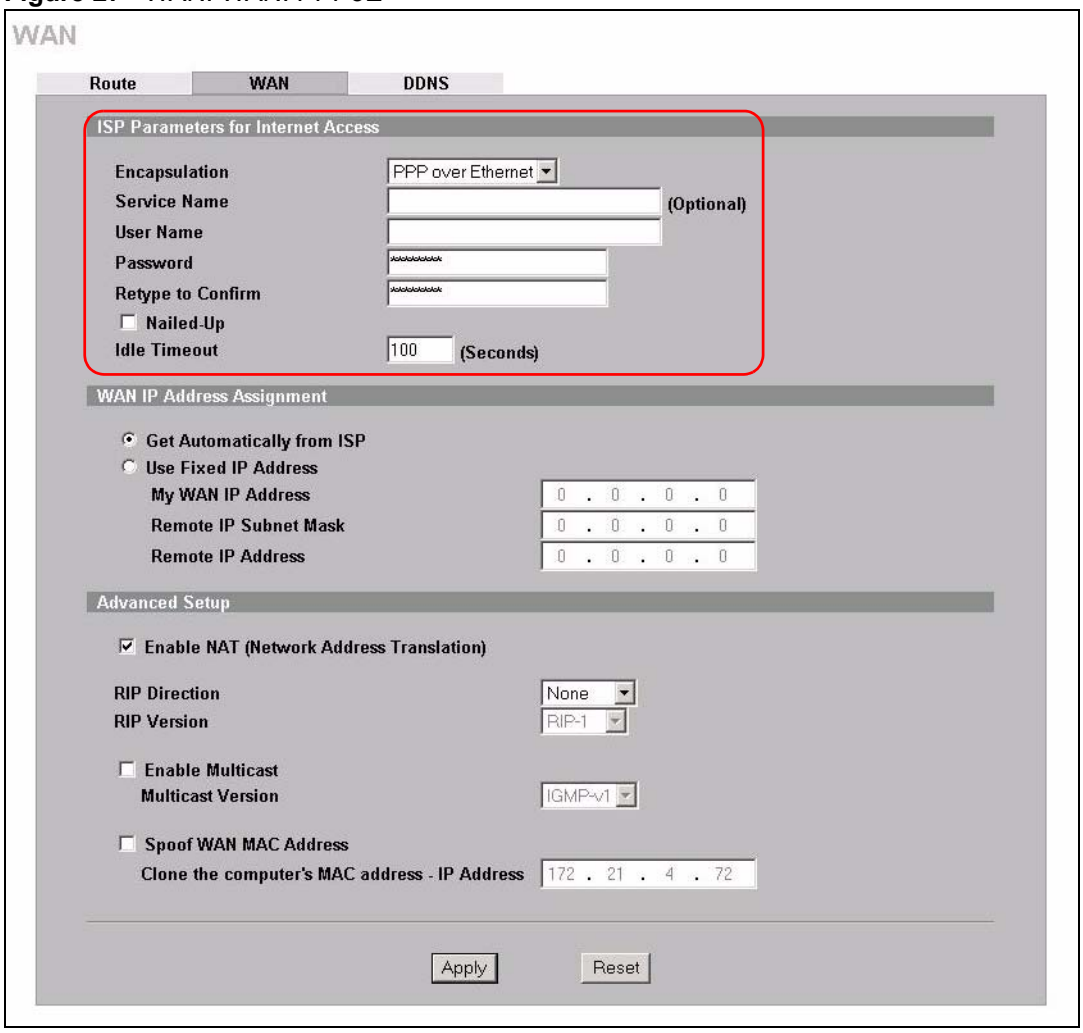
One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

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 27 WAN: WAN: PPPoE



The following table describes the labels not previously discussed.

Table 23 WAN: WAN: PPPoE

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	The PPPoE choice is for a dial-up connection using PPPoE. The router supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF Draft standard (RFC 2516) specifying how a computer interacts with a broadband modem (i.e. DSL, cable, wireless, etc.) connection. Operationally, PPPoE saves significant effort for both the end user and ISP/carrier, as it requires no specific configuration of the broadband modem at the customer site. By implementing PPPoE directly on the router rather than individual computers, the computers on the LAN do not need PPPoE software installed, since the router does that part of the task. Further, with NAT, all of the LAN's computers will have access.
Service Name	Type the PPPoE service name provided to you. PPPoE uses a service name to identify and reach the PPPoE server.

Table 23 WAN: WAN: PPPoE (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.

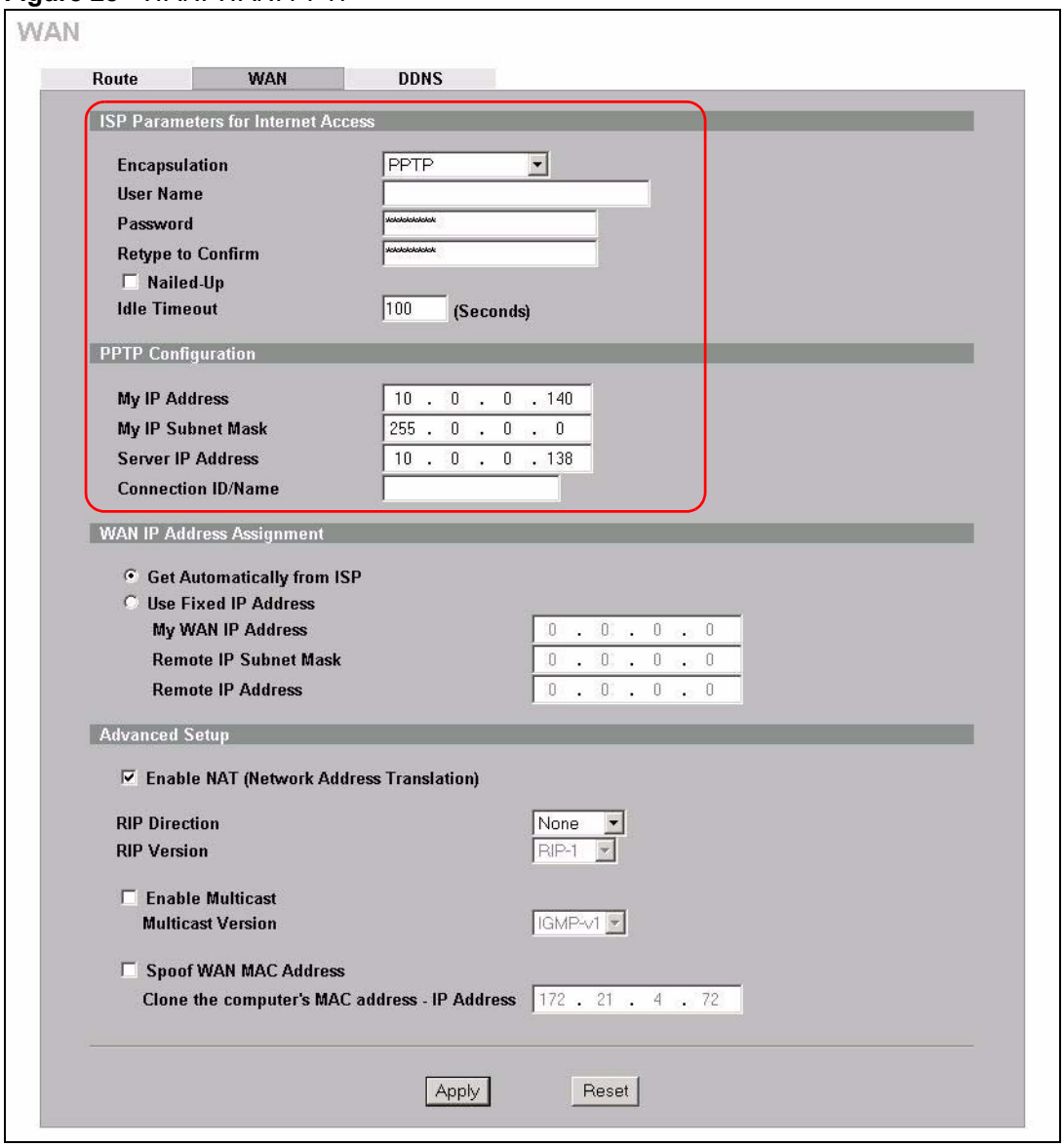
Refer to Table 22 on page 81 for other field descriptions.

5.3.3 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 28 WAN: WAN: PPTP



The following table describes the labels not previously discussed.

Table 24 WAN: WAN: PPTP

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
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 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.

Table 24 WAN: WAN: PPTP (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 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.

Refer to Table 22 on page 81 for other field descriptions.

5.4 Dynamic DNS

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.

First of all, you need to have registered a dynamic DNS account with www.dyndns.org. 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.

Note: 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.

5.4.1 DYNDNS Wildcard

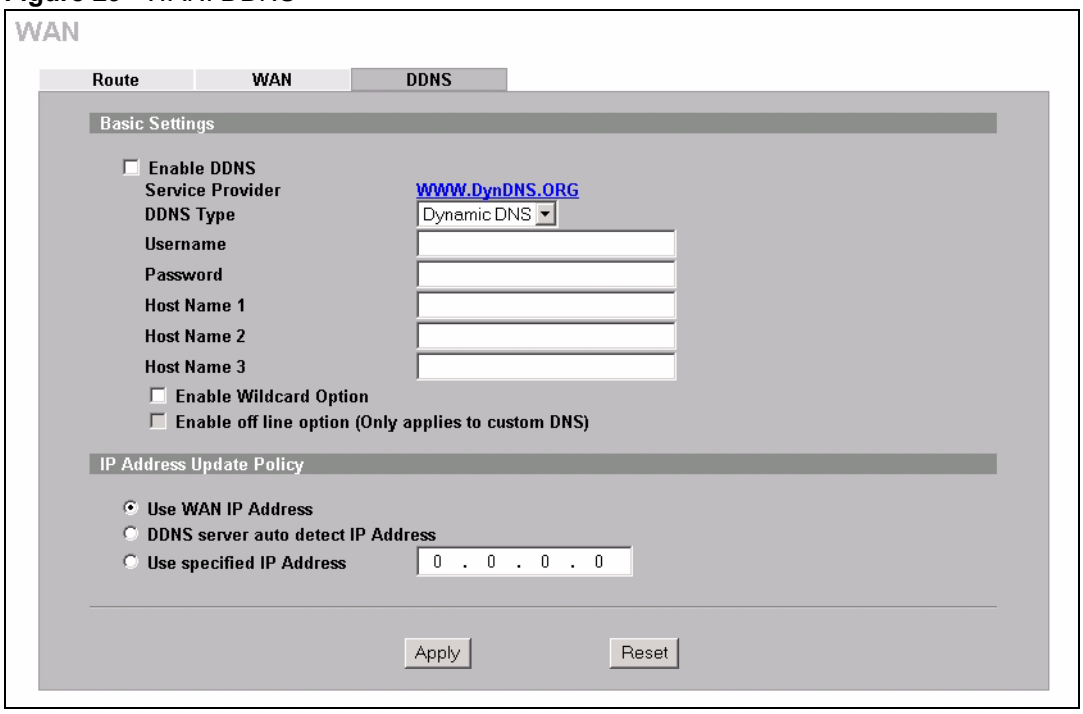
Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

Note: If you have a private WAN IP address, then you cannot use Dynamic DNS.

5.4.2 Configuring Dynamic DNS

To change your ZyWALL's DDNS, click **WAN**, then the **DDNS** tab. The screen appears as shown.

Figure 29 WAN: DDNS



The following table describes the labels in this screen.

Table 25 WAN: DDNS

LABEL	DESCRIPTION
Account Setup	
Enable DDNS	Select this check box to use dynamic DNS.
Service Provider	This is the name of your Dynamic DNS service provider.
DDNS Type	Select the type of service that you are registered for from your Dynamic DNS service provider. Select **Dynamic DNS** if you have the Dynamic DNS service. Select **Static DNS** if you have the Static DNS service. Select **Custom DNS** if you have the Custom DNS service.
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.
Domain Name 1~3	Enter the host names in these fields.
Enable Wildcard Options	Select the check box to enable DYNDNS Wildcard.

Table 25 WAN: DDNS (continued)

LABEL	DESCRIPTION
Enable off line option (Only applies to custom DNS)	This option is applicable when **Custom DNS** 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.
IP Address Update Policy	Select **Use WAN IP Address** to have the ZyWALL update the domain name with the WAN port's IP address. Select **DDNS server auto detect IP Address** 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. Select **Use specified IP Address** and enter the IP address if you have a static IP address. **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.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

CHAPTER 6
Firewalls

This chapter gives some background information on firewalls and introduces the ZyWALL firewall.

6.1 Firewall Overview

Originally, the term *firewall* referred to a construction technique designed to prevent the spread of fire from one room to another. The networking term firewall is a system or group of systems that enforces an access-control policy between two networks. It may also be defined as a mechanism used to protect a trusted network from an untrusted network. Of course, firewalls cannot solve every security problem. A firewall is *one* of the mechanisms used to establish a network security perimeter in support of a network security policy. It should never be the *only* mechanism or method employed. For a firewall to guard effectively, you must design and deploy it appropriately. This requires integrating the firewall into a broad information-security policy. In addition, specific policies must be implemented within the firewall itself.

6.2 Types of Firewalls

There are three main types of firewalls:

1. Packet Filtering Firewalls
2. Application-level Firewalls
3. Stateful Inspection Firewalls

6.2.1 Packet Filtering Firewalls

Packet filtering firewalls restrict access based on the source/destination computer network address of a packet and the type of application.

6.2.2 Application-level Firewalls

Application-level firewalls restrict access by serving as proxies for external servers. Since they use programs written for specific Internet services, such as HTTP, FTP and telnet, they can evaluate network packets for valid application-specific data. Application-level gateways have a number of general advantages over the default mode of permitting application traffic directly to internal hosts:

1. Information hiding prevents the names of internal systems from being made known via DNS to outside systems, since the application gateway is the only host whose name must be made known to outside systems.
2. Robust authentication and logging pre-authenticates application traffic before it reaches internal hosts and causes it to be logged more effectively than if it were logged with standard host logging. Filtering rules at the packet filtering router can be less complex than they would be if the router needed to filter application traffic and direct it to a number of specific systems. The router need only allow application traffic destined for the application gateway and reject the rest.

6.2.3 Stateful Inspection Firewalls

Stateful inspection firewalls restrict access by screening data packets against defined access rules. They make access control decisions based on IP address and protocol. They also "inspect" the session data to assure the integrity of the connection and to adapt to dynamic protocols. These firewalls generally provide the best speed and transparency; however, they may lack the granular application level access control or caching that some proxies support. See Section 6.5 on page 97 for more information on Stateful Inspection.

Firewalls, of one type or another, have become an integral part of standard security solutions for enterprises.

6.3 Introduction to ZyXEL's Firewall

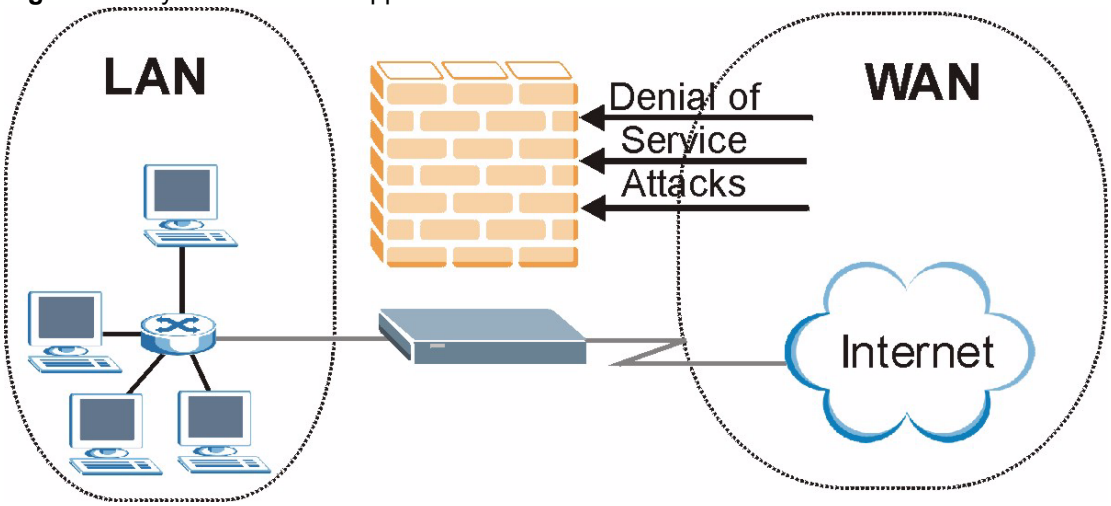
The ZyWALL firewall is a stateful inspection firewall and is designed to protect against Denial of Service attacks when activated. The ZyWALL's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The ZyWALL can be used to prevent theft, destruction and modification of data, as well as log events, which may be important to the security of your network. The ZyWALL also has packet-filtering capabilities.

The ZyWALL is installed between the LAN and a broadband modem connecting to the Internet. This allows it to act as a secure gateway for all data passing between the Internet and the LAN.

The ZyWALL has one Ethernet WAN port and one Ethernet LAN port, which are used to physically separate the network into the following areas.

- The WAN (Wide Area Network) port attaches to the broadband modem (cable or DSL) connecting to the Internet.
- The LAN (Local Area Network) port attaches to a network of computers, which needs security from the outside world. These computers will have access to Internet services such as e-mail, FTP, and the World Wide Web. However, inbound access will not be allowed unless the remote host is authorized to use a specific service.

Figure 30 ZyWALL Firewall Application



6.4 Denial of Service

Denials of Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources. The ZyWALL is pre-configured to automatically detect and thwart all known DoS attacks.

6.4.1 Basics

Computers share information over the Internet using a common language called TCP/IP. TCP/IP, in turn, is a set of application protocols that perform specific functions. An extension number, called the "TCP port" or "UDP port" identifies these protocols, such as HTTP (Web), FTP (File Transfer Protocol), POP3 (E-mail), etc. For example, Web traffic by default uses TCP port 80.

When computers communicate on the Internet, they are using the client/server model, where the server "listens" on a specific TCP/UDP port for information requests from remote client computers on the network. For example, a Web server typically listens on port 80. Please note that while a computer may be intended for use over a single port, such as Web on port 80, other ports are also active. If the person configuring or managing the computer is not careful, a hacker could attack it over an unprotected port.

Some of the most common IP ports are:

Table 26 Common IP Ports

21	FTP	53	DNS
23	Telnet	80	HTTP
25	SMTP	110	POP3

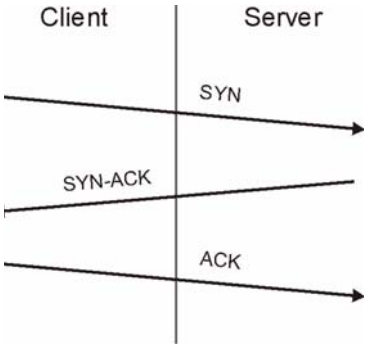
6.4.2 Types of DoS Attacks

There are four types of DoS attacks:

1. Those that exploit bugs in a TCP/IP implementation.
2. Those that exploit weaknesses in the TCP/IP specification.
3. Brute-force attacks that flood a network with useless data.
4. IP Spoofing.

- "**Ping of Death**" and "**Teardrop**" attacks exploit bugs in the TCP/IP implementations of various computer and host systems.
    - **a** Ping of Death uses a "ping" utility to create an IP packet that exceeds the maximum 65,536 bytes of data allowed by the IP specification. The oversize packet is then sent to an unsuspecting system. Systems may crash, hang or reboot.
    - **b** Teardrop attack exploits weaknesses in the reassembly of IP packet fragments. As data is transmitted through a network, IP packets are often broken up into smaller chunks. Each fragment looks like the original IP packet except that it contains an offset field that says, for instance, "This fragment is carrying bytes 200 through 400 of the original (non fragmented) IP packet." The Teardrop program creates a series of IP fragments with overlapping offset fields. When these fragments are reassembled at the destination, some systems will crash, hang, or reboot.
- Weaknesses in the TCP/IP specification leave it open to "**SYN Flood**" and "**LAND**" attacks. These attacks are executed during the handshake that initiates a communication session between two applications.

Figure 31 Three-Way Handshake

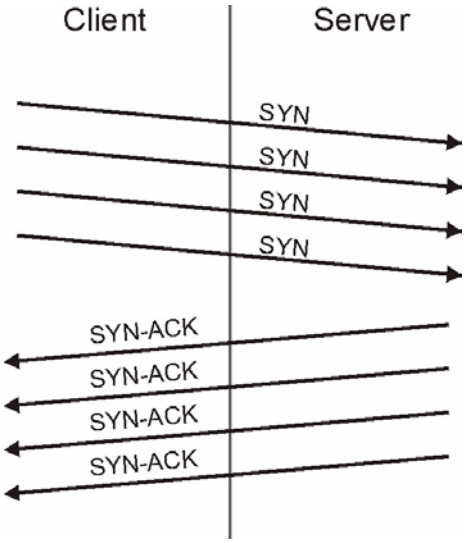


Under normal circumstances, the application that initiates a session sends a SYN (synchronize) packet to the receiving server. The receiver sends back an ACK (acknowledgment) packet and its own SYN, and then the initiator responds with an ACK (acknowledgment). After this handshake, a connection is established.

- **a** **SYN Attack** floods a targeted system with a series of SYN packets. Each packet causes the targeted system to issue a SYN-ACK

response. While the targeted system waits for the ACK that follows the SYN-ACK, it queues up all outstanding SYN-ACK responses on what is known as a backlog queue. SYN-ACKs are moved off the queue only when an ACK comes back or when an internal timer (which is set at relatively long intervals) terminates the three-way handshake. Once the queue is full, the system will ignore all incoming SYN requests, making the system unavailable for legitimate users.

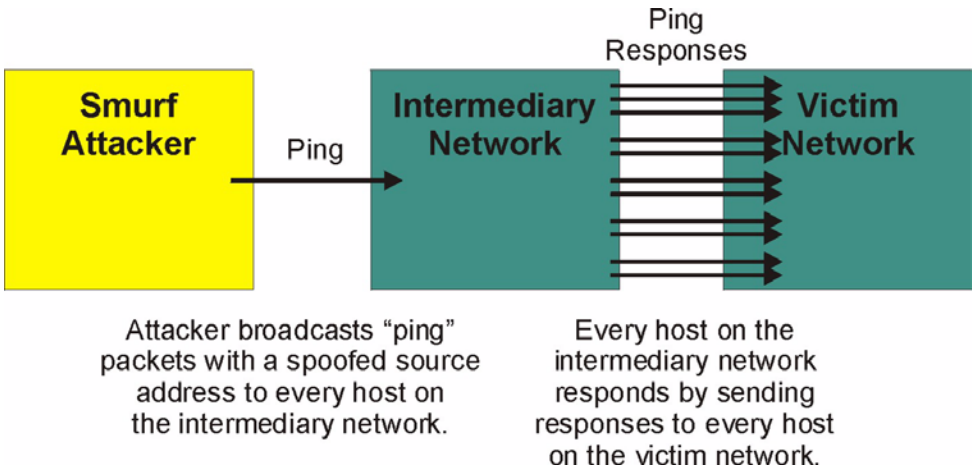
Figure 32 SYN Flood



b In a **LAND Attack**, hackers flood SYN packets into the network with a spoofed source IP address of the targeted system. This makes it appear as if the host computer sent the packets to itself, making the system unavailable while the target system tries to respond to itself.

- A **brute-force** attack, such as a "Smurf" attack, targets a feature in the IP specification known as directed or subnet broadcasting, to quickly flood the target network with useless data. A Smurf hacker floods a router with Internet Control Message Protocol (ICMP) echo request packets (pings). Since the destination IP address of each packet is the broadcast address of the network, the router will broadcast the ICMP echo request packet to all hosts on the network. If there are numerous hosts, this will create a large amount of ICMP echo request and response traffic. If a hacker chooses to spoof the source IP address of the ICMP echo request packet, the resulting ICMP traffic will not only clog up the "intermediary" network, but will also congest the network of the spoofed source IP address, known as the "victim" network. This flood of broadcast traffic consumes all available bandwidth, making communications impossible.

Figure 33 Smurf Attack



6.4.2.1 ICMP Vulnerability

ICMP is an error-reporting protocol that works in concert with IP. The following ICMP types trigger an alert:

Table 27 ICMP Commands That Trigger Alerts

5	REDIRECT
13	TIMESTAMP_REQUEST
14	TIMESTAMP_REPLY
17	ADDRESS_MASK_REQUEST
18	ADDRESS_MASK_REPLY

6.4.2.2 Illegal Commands (NetBIOS and SMTP)

The only legal NetBIOS commands are the following - all others are illegal.

Table 28 Legal NetBIOS Commands

MESSAGE:
REQUEST:
POSITIVE:
NEGATIVE:
RETARGET:
KEEPALIVE:

All SMTP commands are illegal except for those displayed in the following tables.

Table 29 Legal SMTP Commands

AUTH	DATA	EHLO	ETRN	EXPN	HELO	HELP	MAIL	NOOP
QUIT	RCPT	RSET	SAML	SEND	SOML	TURN	VRFY	

6.4.2.3 Traceroute

Traceroute is a utility used to determine the path a packet takes between two endpoints. Sometimes when a packet filter firewall is configured incorrectly an attacker can traceroute the firewall gaining knowledge of the network topology inside the firewall.

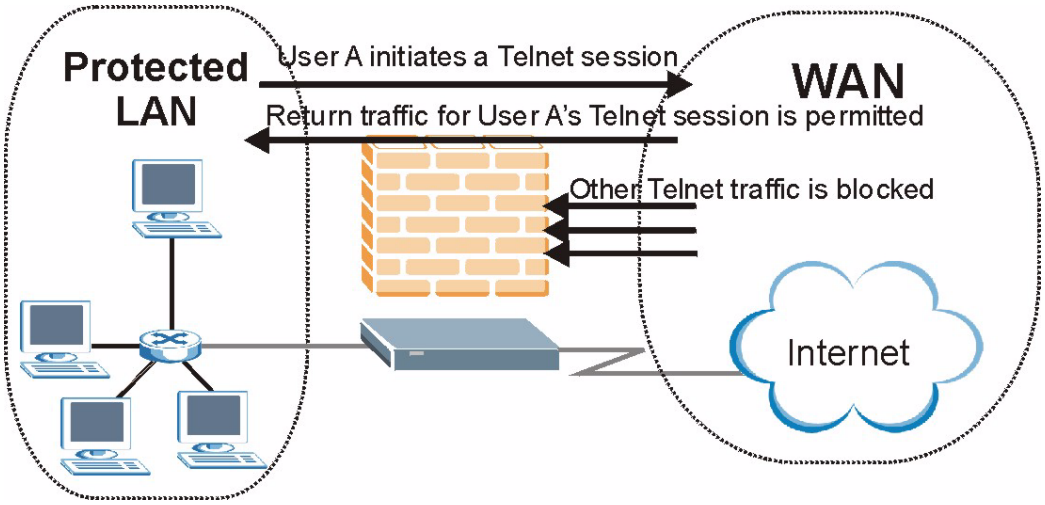
Often, many DoS attacks also employ a technique known as "**IP Spoofing**" as part of their attack. IP Spoofing may be used to break into systems, to hide the hacker's identity, or to magnify the effect of the DoS attack. IP Spoofing is a technique used to gain unauthorized access to computers by tricking a router or firewall into thinking that the communications are coming from within the trusted network. To engage in IP spoofing, a hacker must modify the packet headers so that it appears that the packets originate from a trusted host and should be allowed through the router or firewall. The ZyWALL blocks all IP Spoofing attempts.

6.5 Stateful Inspection

With stateful inspection, fields of the packets are compared to packets that are already known to be trusted. For example, if you access some outside service, the proxy server remembers things about your original request, like the port number and source and destination addresses. This remembering is called *saving the state.* When the outside system responds to your request, the firewall compares the received packets with the saved state to determine if they are allowed in. The ZyWALL uses stateful packet inspection to protect the private LAN from hackers and vandals on the Internet. By default, the ZyWALL's stateful inspection allows all communications to the Internet that originate from the LAN, and blocks all traffic to the LAN that originates from the Internet. In summary, stateful inspection:

- Allows all sessions originating from the LAN (local network) to the WAN (Internet).
- Denies all sessions originating from the WAN to the LAN.

Figure 34 Stateful Inspection



The previous figure shows the ZyWALL's default firewall rules in action as well as demonstrates how stateful inspection works. User A can initiate a Telnet session from within the LAN and responses to this request are allowed. However other Telnet traffic initiated from the WAN is blocked.

6.5.1 Stateful Inspection Process

In this example, the following sequence of events occurs when a TCP packet leaves the LAN network through the firewall's WAN interface. The TCP packet is the first in a session, and the packet's application layer protocol is configured for a firewall rule inspection:

1. The packet travels from the firewall's LAN to the WAN.
2. The packet is evaluated against the interface's existing outbound access list, and the packet is permitted (a denied packet would simply be dropped at this point).
3. The firewall inspects packets to determine and record information about the state of the packet's connection. This information is recorded in a new state table entry created for the new connection. If there is not a firewall rule for this packet and it is not an attack, then the setting in the **Firewall Default Rule** screen determines the action for this packet.
4. Based on the obtained state information, a firewall rule creates a temporary access list entry that is inserted at the beginning of the WAN interface's inbound extended access list. This temporary access list entry is designed to permit inbound packets of the same connection as the outbound packet just inspected.
5. The outbound packet is forwarded out through the interface.
6. Later, an inbound packet reaches the interface. This packet is part of the connection previously established with the outbound packet. The inbound packet is evaluated against the inbound access list, and is permitted because of the temporary access list entry previously created.
7. The packet is inspected by a firewall rule, and the connection's state table entry is updated as necessary. Based on the updated state information, the inbound extended access list

temporary entries might be modified, in order to permit only packets that are valid for the current state of the connection.

8 Any additional inbound or outbound packets that belong to the connection are inspected to update the state table entry and to modify the temporary inbound access list entries as required, and are forwarded through the interface.

9 When the connection terminates or times out, the connection's state table entry is deleted and the connection's temporary inbound access list entries are deleted.

6.5.2 Stateful Inspection and the ZyWALL

Additional rules may be defined to extend or override the default rules. For example, a rule may be created which will:

1 Block all traffic of a certain type, such as IRC (Internet Relay Chat), from the LAN to the Internet.

2 Allow certain types of traffic from the Internet to specific hosts on the LAN.

3 Allow access to a Web server to everyone but competitors.

4 Restrict use of certain protocols, such as Telnet, to authorized users on the LAN.

These custom rules work by evaluating the network traffic's Source IP address, Destination IP address, IP protocol type, and comparing these to rules set by the administrator.

Note: The ability to define firewall rules is a very powerful tool. Using custom rules, it is possible to disable all firewall protection or block all access to the Internet. Use extreme caution when creating or deleting firewall rules. Test changes after creating them to make sure they work correctly.

Below is a brief technical description of how these connections are tracked. Connections may either be defined by the upper protocols (for instance, TCP), or by the ZyWALL itself (as with the "virtual connections" created for UDP and ICMP).

6.5.3 TCP Security

The ZyWALL uses state information embedded in TCP packets. The first packet of any new connection has its SYN flag set and its ACK flag cleared; these are "initiation" packets. All packets that do not have this flag structure are called "subsequent" packets, since they represent data that occurs later in the TCP stream.

If an initiation packet originates on the WAN, this means that someone is trying to make a connection from the Internet into the LAN. Except in a few special cases (see Section 6.5.5 on page 100), these packets are dropped and logged.

If an initiation packet originates on the LAN, this means that someone is trying to make a connection from the LAN to the Internet. Assuming that this is an acceptable part of the security policy (as is the case with the default policy), the connection will be allowed. A cache entry is added which includes connection information such as IP addresses, TCP ports, sequence numbers, etc.

When the ZyWALL receives any subsequent packet (from the Internet or from the LAN), its connection information is extracted and checked against the cache. A packet is only allowed to pass through if it corresponds to a valid connection (that is, if it is a response to a connection which originated on the LAN).

6.5.4 UDP/ICMP Security

UDP and ICMP do not themselves contain any connection information (such as sequence numbers). However, at the very minimum, they contain an IP address pair (source and destination). UDP also contains port pairs, and ICMP has type and code information. All of this data can be analyzed in order to build "virtual connections" in the cache.

For instance, any UDP packet that originates on the LAN will create a cache entry. Its IP address and port pairs will be stored. For a short period of time, UDP packets from the WAN that have matching IP and UDP information will be allowed back in through the firewall.

A similar situation exists for ICMP, except that the ZyWALL is even more restrictive. Specifically, only outgoing echoes will allow incoming echo replies, outgoing address mask requests will allow incoming address mask replies, and outgoing timestamp requests will allow incoming timestamp replies. No other ICMP packets are allowed in through the firewall, simply because they are too dangerous and contain too little tracking information. For instance, ICMP redirect packets are never allowed in, since they could be used to reroute traffic through attacking machines.

6.5.5 Upper Layer Protocols

Some higher layer protocols (such as FTP and RealAudio) utilize multiple network connections simultaneously. In general terms, they usually have a "control connection" which is used for sending commands between endpoints, and then "data connections" which are used for transmitting bulk information.

Consider the FTP protocol. A user on the LAN opens a control connection to a server on the Internet and requests a file. At this point, the remote server will open a data connection from the Internet. For FTP to work properly, this connection must be allowed to pass through even though a connection from the Internet would normally be rejected.

In order to achieve this, the ZyWALL inspects the application-level FTP data. Specifically, it searches for outgoing "PORT" commands, and when it sees these; it adds a cache entry for the anticipated data connection. This can be done safely, since the PORT command contains address and port information, which can be used to uniquely identify the connection.

Any protocol that operates in this way must be supported on a case-by-case basis. You can use the web configurator's **Custom Services** feature to do this (refer to Section 7.6.3 on page 112 for more information).

6.6 Guidelines For Enhancing Security With Your Firewall

1. Change the default password via CLI or web configurator.
2. Think about access control before you connect a console port to the network in any way, including attaching a modem to the port. Be aware that a break on the console port might give unauthorized individuals total control of the firewall, even with access control configured.
3. Limit who can telnet into your router.
4. Don't enable any local service (such as SNMP or NTP) that you don't use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.
5. For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.
6. Protect against IP spoofing by making sure the firewall is active.
7. Keep the firewall in a secured (locked) room.

6.7 Packet Filtering Vs Firewall

Below are some comparisons between the ZyWALL's filtering and firewall functions.

6.7.1 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.

6.7.1.1 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.

6.7.2 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 nonexistent 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.

6.7.2.1 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.

CHAPTER 7
Firewall Screens

This chapter shows you how to configure your ZyWALL firewall.

7.1 Access Methods

The web configurator is, by far, the most comprehensive firewall configuration tool your ZyWALL has to offer. For this reason, it is recommended that you configure your firewall using the web configurator. CLI commands provide limited configuration options and are only recommended for advanced users, please refer to Appendix J on page 331 for firewall CLI commands.

7.2 Firewall Policies Overview

Firewall rules are grouped based on the direction of travel of packets to which they apply:

- LAN to LAN/ZyWALL
- LAN to WAN
- WAN to LAN
- WAN to WAN/ZyWALL

By default, the ZyWALL's stateful packet inspection allows packets traveling in the following directions:

- LAN to LAN/ZyWALL

  This allows computers on the LAN to manage the ZyWALL and communicate between networks or subnets connected to the LAN interface.
- LAN to WAN

By default, the ZyWALL's stateful packet inspection blocks packets traveling in the following directions:

- WAN to LAN
- WAN to WAN/ZyWALL

  This prevents computers on the WAN from using the ZyWALL as a gateway to communicate with other computers on the WAN and/or managing the ZyWALL.

You may define additional rules and sets or modify existing ones but please exercise extreme caution in doing so.

Note: If you configure firewall rules without a good understanding of how they work, you might inadvertently introduce security risks to the firewall and to the protected network. Make sure you test your rules after you configure them.

For example, you may create rules to:

- Block certain types of traffic, such as IRC (Internet Relay Chat), from the LAN to the Internet.
- Allow certain types of traffic, such as Lotus Notes database synchronization, from specific hosts on the Internet to specific hosts on the LAN.
- Allow everyone except your competitors to access a Web server.
- Restrict use of certain protocols, such as Telnet, to authorized users on the LAN.

These custom rules work by comparing the Source IP address, Destination IP address and IP protocol type of network traffic to rules set by the administrator. Your customized rules take precedence and override the ZyWALL's default rules.

7.3 Rule Logic Overview

Note: Study these points carefully before configuring rules.

7.3.1 Rule Checklist

1. State the intent of the rule. For example, This restricts all IRC access from the LAN to the Internet. Or, This allows a remote Lotus Notes server to synchronize over the Internet to an inside Notes server.
2. Is the intent of the rule to forward or block traffic?
3. What direction of traffic does the rule apply to (see Section 6.2 on page 91)?
4. What IP services will be affected?
5. What computers on the LAN are to be affected (if any)?
6. What computers on the Internet will be affected? The more specific, the better. For example, if traffic is being allowed from the Internet to the LAN, it is better to allow only certain machines on the Internet to access the LAN.

7.3.2 Security Ramifications

Once the logic of the rule has been defined, it is critical to consider the security ramifications created by the 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 plugging the information into the correct fields in the web configurator screens.

7.3.3 Key Fields For Configuring Rules

7.3.3.1 Action

Should the action be to **Block** or **Forward**?

Note: "Block" means the firewall silently discards the packet.

7.3.3.2 Service

Select the service from the **Service** scrolling list box. If the service is not listed, it is necessary to first define it. See Section 7.8 on page 116 for more information on predefined services.

7.3.3.3 Source Address

What is the connection's source address; is it on the LAN or WAN? Is it a single IP, a range of IPs or a subnet?

7.3.3.4 Destination Address

What is the connection's destination address; is it on the LAN or WAN? Is it a single IP, a range of IPs or a subnet?

7.4 Connection Direction Examples

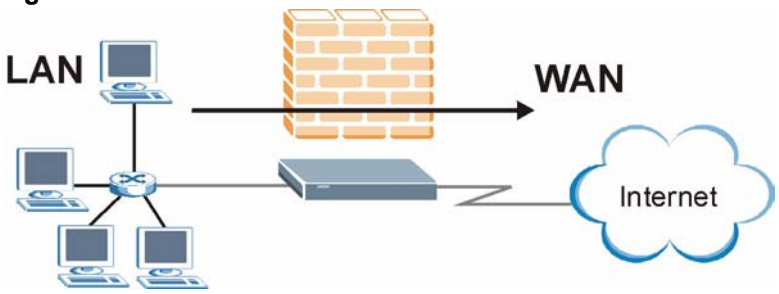
This section describes examples for firewall rules for connections going from LAN to WAN and from WAN to LAN.

LAN to LAN/ZyWALL and WAN to WAN/ZyWALL rules apply to packets coming in on the associated interface (LAN or WAN respectively). LAN to LAN/ZyWALL means policies for LAN-to-ZyWALL (the policies for managing the ZyWALL through the LAN interface) and policies for LAN-to-LAN (the policies that control routing between two subnets on the LAN). Similarly,WAN to WAN/ZyWALL policy applyies in the same way to the WAN ports.

7.4.1 LAN To WAN Rules

The default rule for LAN to WAN traffic is that all users on the LAN are allowed non-restricted access to the WAN. When you configure a LAN to WAN rule, you in essence want to limit some or all users from accessing certain services on the WAN. See the following figure.

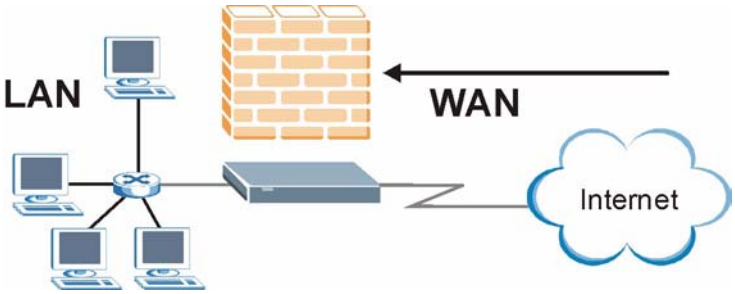
Figure 35 LAN to WAN Traffic



7.4.2 WAN To LAN Rules

The default rule for WAN to LAN traffic blocks all incoming connections (WAN to LAN). If you wish to allow certain WAN users to have access to your LAN, you will need to create custom rules to allow it. See the following figure.

Figure 36 WAN to LAN Traffic



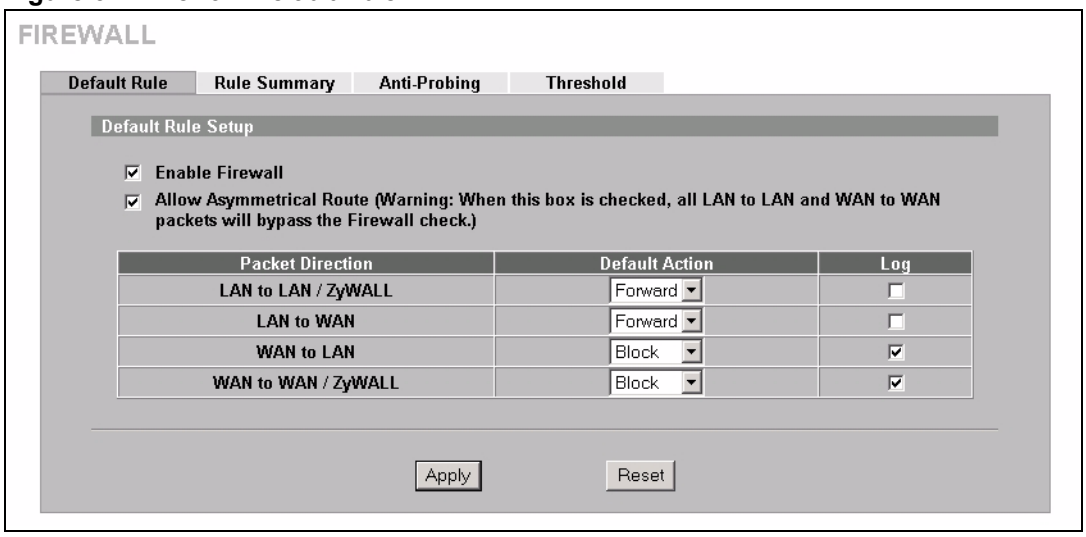
7.5 Alerts

Alerts are reports on events, such as attacks, that you may want to know about right away. You can choose to generate an alert when a rule is matched in the **Edit Rule** screen (see Figure 39 on page 110). Configure the **Log Settings** screen to have the ZyWALL send an immediate e-mail message to you when an event generates an alert. Refer to the chapter on logs for details.

7.6 Configuring Firewall

Click **FIREWALL** to open the **Default Rule** screen. Enable (or activate) the firewall by selecting the **Enable Firewall** check box as seen in the following screen.

Figure 37 Firewall: Default Rule



The following table describes the labels in this screen.

Table 30 Firewall: Default Rule

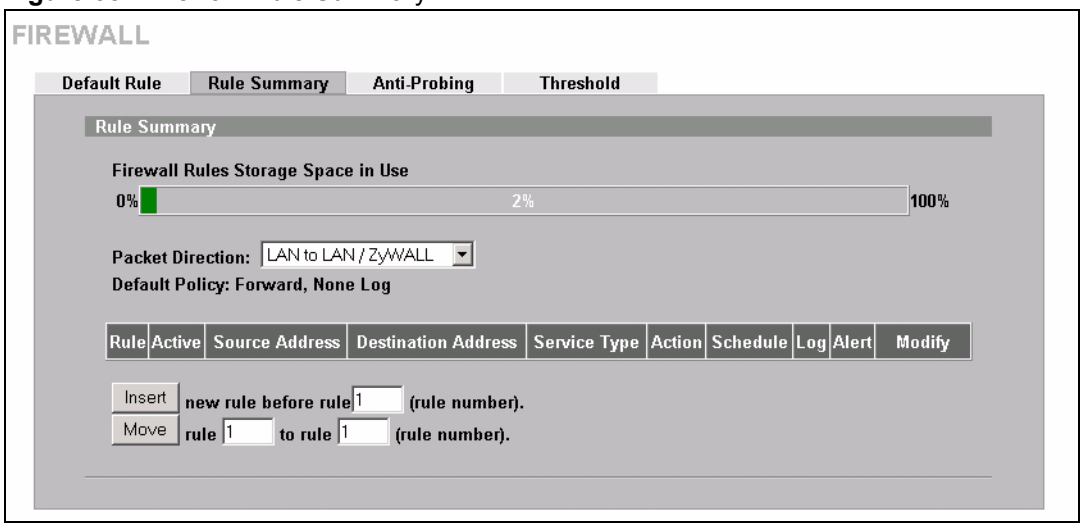
LABEL	DESCRIPTION
Enable Firewall	Select this check box to activate the firewall. The ZyWALL performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Allow Asymmetrical Route	Select this check box to have the ZyWALL firewall permit the use of triangle route topology on the network. See Appendix E on page 295 for more on triangle route topology.
Packet Direction	This is the direction of travel of packets (**LAN to LAN/ZyWALL**, **LAN to WAN**, **WAN to LAN**, **WAN to WAN/ZyWALL**). Firewall rules are grouped based on the direction of travel of packets to which they apply. For example, **LAN to LAN/ZyWALL** means packets traveling from a computer/subnet on the LAN to either another computer/subnet on the LAN interface of the ZyWALL or the ZyWALL itself.
Default Action	Use the drop-down list boxes to select whether to **Block** (silently discard) or **Forward** (allow the passage of) packets that are traveling in the selected direction.
Log	Select the check box to create a log (when the above action is taken) for packets that are traveling in the selected direction and do not match any of the rules below.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to begin configuring this screen afresh.

7.6.1 Rule Summary

Note: The ordering of your rules is very important as rules are applied in turn.

Click **FIREWALL**, then the **Rule Summary** tab to open the screen.

Figure 38 Firewall: Rule Summary



The following table describes the labels in this screen.

Table 31 Firewall: Rule Summary

LABEL	DESCRIPTION
Firewall Rules Storage Space in Use	This read-only bar shows how much of the ZyWALL's memory for recording firewall rules it is currently using. When you are using 80% or less of the storage space, the bar is green. When the amount of space used is over 80%, the bar is red.
Packet Direction	Use the drop-down list box to select a direction of travel of packets for which you want to configure firewall rules.
Default Policy	This field displays the default action and log policy you selected in the **Default Rule** screen for the packet direction shown in the field above.
The following read-only 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.	
Rule	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.
Active	This field displays whether a firewall is turned on (**Y**) or not (**N**).
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. Please note that a blank service type is equivalent to **Any**. See Table 34 on page 116 for more information.
Action	This is the specified action for that rule, either **Block** or **Forward**. Note that **Block** means the firewall silently discards the packet.
Schedule	This field tells you whether a schedule is specified (**Yes**) or not (**No**).

Table 31 Firewall: Rule Summary (continued)

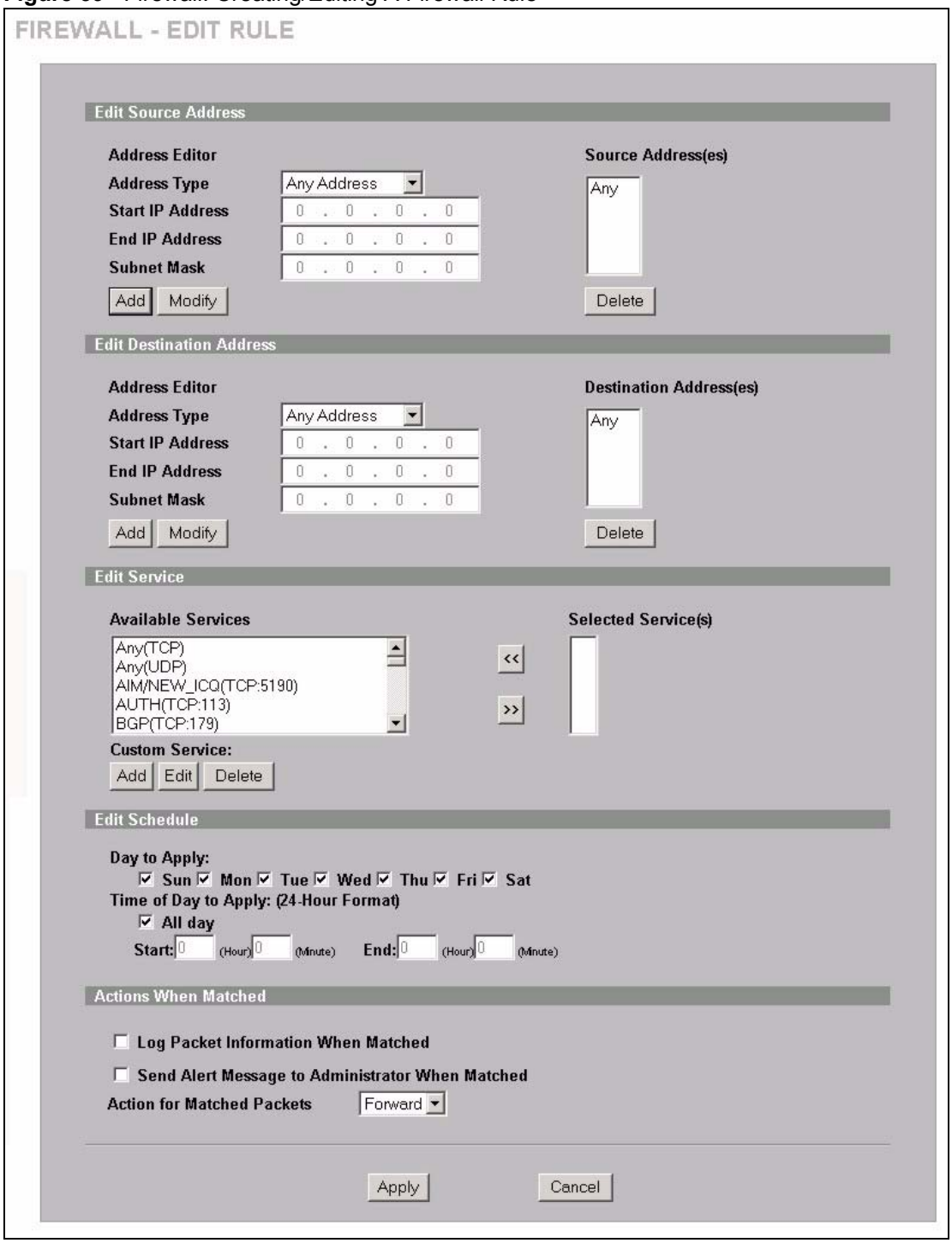
LABEL	DESCRIPTION
Log	This field shows you whether a log is created when packets match this rule (**Enabled**) or not (**Disable**).
Alert	This field tells you whether this rule generates an alert (**Yes**) or not (**No**) when the rule is matched.
Modify	Click the edit icon to go to the screen where you can edit the rule. Click the delete icon to delete an existing firewall rule. A window display 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.
Insert	Type the index number for where you want to put a 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. Click **Insert** to display this screen and refer to the following table for information on the fields.
Move	Type a rule'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. The ordering of your rules is important as they are applied in order of their numbering.

7.6.2 Configuring Firewall Rules

Follow these directions to create a new rule.

1. 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.
2. Click **Insert** to display this screen and refer to the following table for information on the labels.

Figure 39 Firewall: Creating/Editing A Firewall Rule



The following table describes the labels in this screen.

Table 32 Firewall: Creating/Editing A Firewall Rule

LABEL	DESCRIPTION
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 (e.g., 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 above and click **Delete** to remove it.
Edit Service	
Available/ Selected Services	Refer to Table 34 on page 116 for more information on services available. 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 **<<**.
Custom Service	
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.
Edit	Select a custom service (denoted by an *) from the **Available Services** list and click this button to edit the service.
Delete	Select a custom service (denoted by an *) from the **Available Services** list and click this button to remove the service.
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 (**Enable**) or not (**Disable**). 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.
Action for Matched Packets	Use the drop-down list box to select whether to discard (**Block**) or allow the passage of (**Forward**) packets that match this rule.

Table 32 Firewall: Creating/Editing A Firewall Rule (continued)

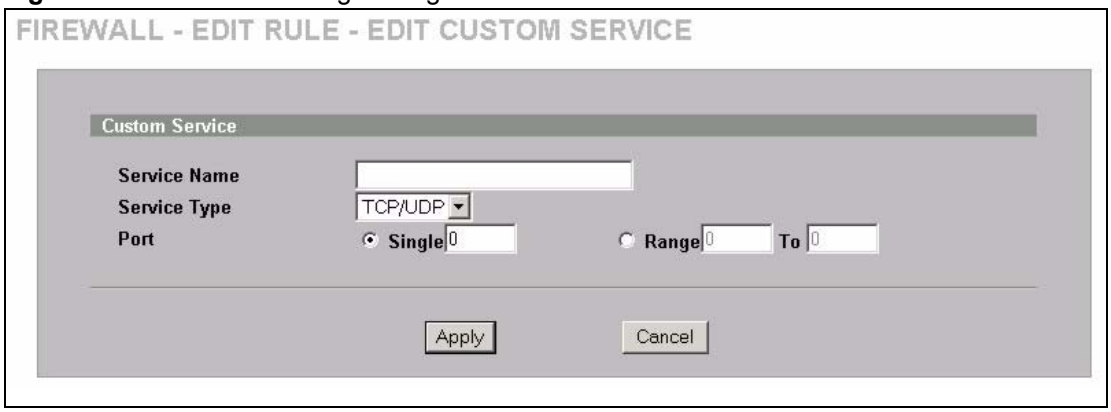
LABEL	DESCRIPTION
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

7.6.3 Configuring Custom Services

Configure customized ports for services not predefined by the ZyWALL (See Section 7.8 on page 116 for a list of predefined services). For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

Click the **Add** button under **Custom Service** while editing a firewall rule to configure a custom service. This displays the following screen.

Figure 40 Firewall: Creating/Editing A Custom Service



The following table describes the labels in this screen.

Table 33 Firewall: Creating/Editing A Custom Service

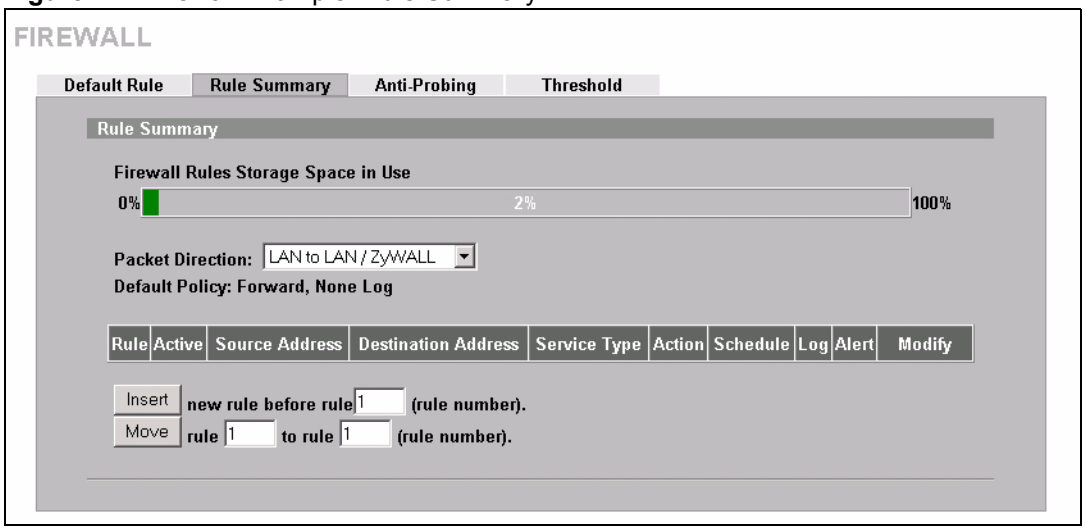
LABEL	DESCRIPTION
Service Name	Enter a unique name for your custom service.
Service Type	Choose the IP port (**TCP**, **UDP** or **Both**) that defines your customized service from the drop down list box.
Port	Select **Single** to specify one port only or **Range** to specify a span of ports that define your customized service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.

7.7 Example Firewall Rule

The following Internet firewall rule example allows a hypothetical My Service connection from the Internet.

1 Click the **FIREWALL** link and then the **Rule Summary** tab. Select **WAN to LAN** from the **Packet Direction** drop-down list box.

Figure 41 Firewall Example: Rule Summary



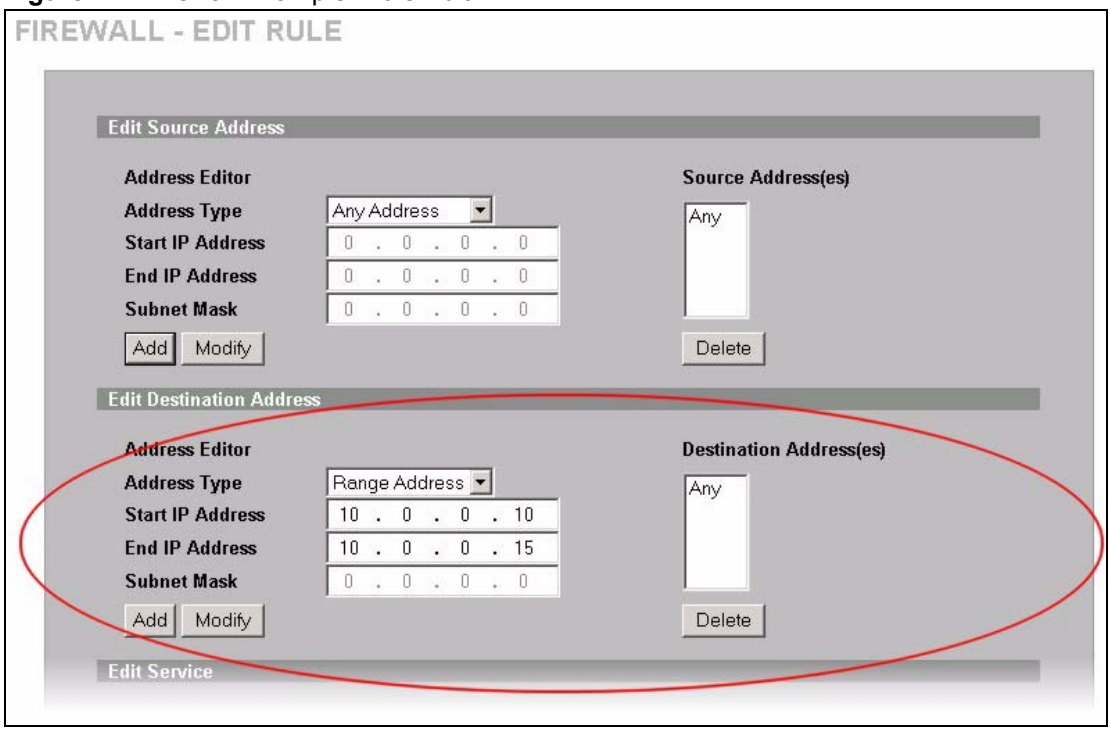
2 In the **Rule Summary** screen, type the index number for where you want to put the rule. For example, if you type 6, your new rule becomes number 6 and the previous rule 6 (if there is one) becomes rule 7.

3 Click **Insert** to display the firewall rule configuration screen.

4 Select **Any** in the **Destination Address** box and then click **Delete**.

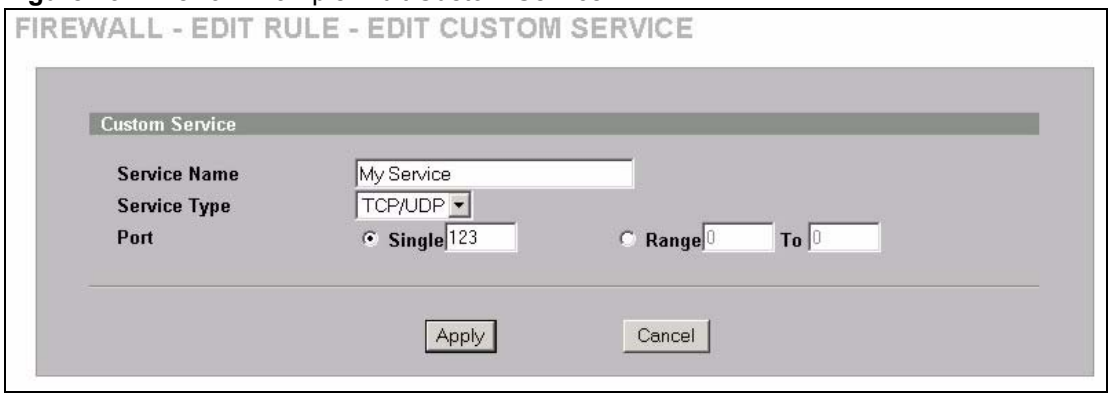
5 Configure the destination address screen as follows and click **Add**.

Figure 42 Firewall Example: Rule Edit



6 In the **Edit Rule** screen, click **Add** under **Custom Service** to open the **Edit Custom Service** screen. Configure it as follows and click **Apply**.

Figure 43 Firewall Example: Edit Custom Service



7 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.

Note: Custom services show up with an * before their names in the **Services** list box and the **Rule Summary** list box. Click **Apply** after you've created your custom service.

Figure 44 Firewall Example: My Service Rule Configuration

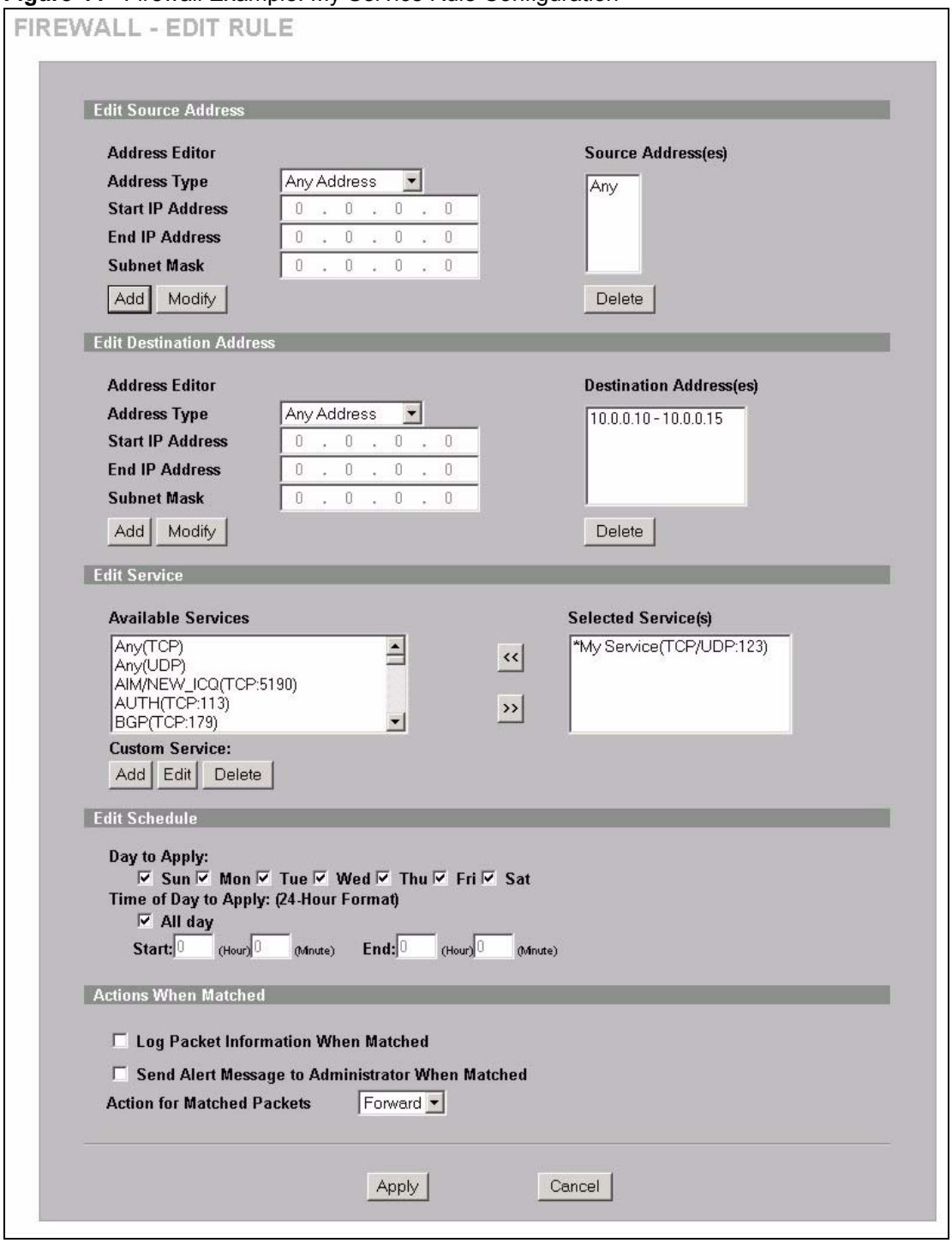
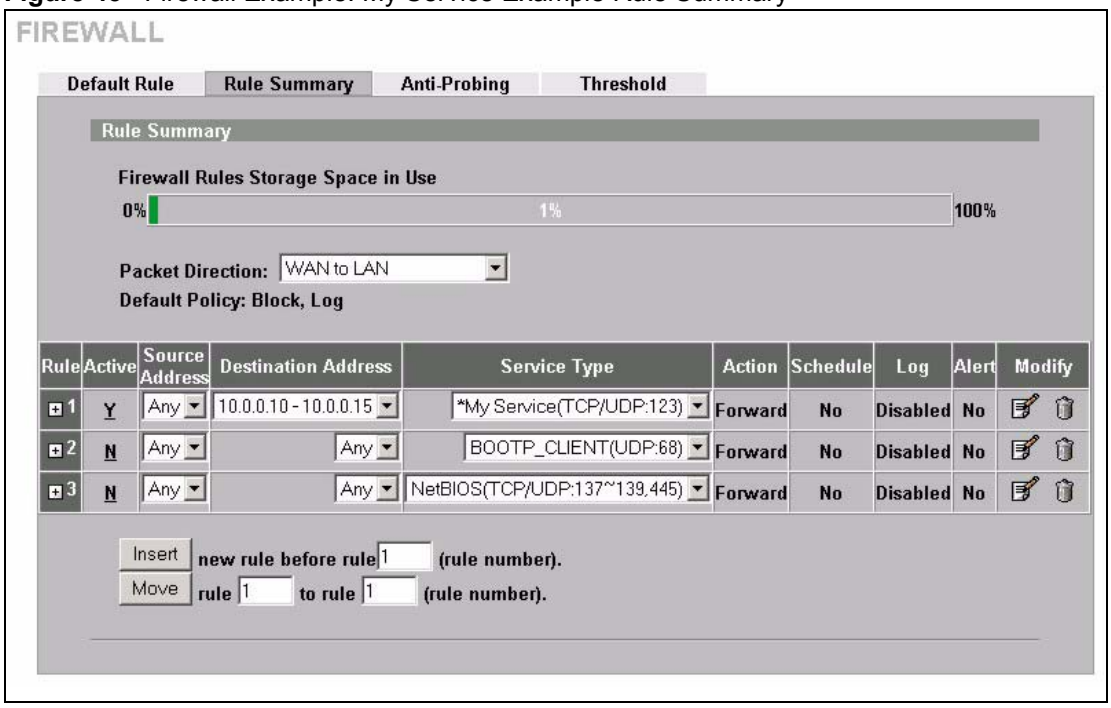


Figure 45 Firewall Example: My Service Example Rule Summary



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.

7.8 Predefined Services

The **Available Services** list box in the **Edit Rule** screen (see Figure 39 on page 110) displays all predefined services that the ZyWALL already supports. Next to the name of the 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 default configuration labeled (**DNS**). **(UDP/TCP:53)** means UDP port 53 and TCP port 53. Custom services may also be configured using the **Custom Services** function discussed previously.

Table 34 Predefined Services

SERVICE	DESCRIPTION
AIM/New-ICQ(TCP:5190)	AOL's Internet Messenger service, 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/UDP:7648, 24032)	A popular videoconferencing solution from White Pines Software.
DNS(UDP/TCP:53)	Domain Name Server, a service that matches web names (e.g. www.zyxel.com) to IP numbers.

Table 34 Predefined Services (continued)

SERVICE	DESCRIPTION
FINGER(TCP:79)	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP(TCP:20.21)	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.
ICQ(UDP:4000)	This is a popular Internet chat program.
IKE(UDP:500)	The Internet Key Exchange algorithm is used for key distribution and management.
IPSEC_ TRANSPORT / TUNNEL(AH:0)	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
IPSEC_TUNNEL(ESP:0)	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
IRC(TCP/UDP:6667)	This is another popular Internet chat program.
MSN Messenger (TCP:1863)	Microsoft Networks' messenger service uses this protocol.
MULTICAST(IGMP:0)	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
NetBIOS(TCP/UDP:137~139, 45)	NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to connect to and communicate with a LAN.
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(ICMP:0)	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:0)	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.
ROADRUNNER(TCP/ UDP:1026)	This is Time Warner's cable modem session management protocol. It handles authentication and dynamic addressing.
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.

Table 34 Predefined Services (continued)

SERVICE	DESCRIPTION
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.
SSDP(UDP:1900)	Simple Service Discovery Protocol (SSDP) is a discovery service searching for Universal Plug and Play devices on your home network or upstream Internet gateways using UDP port 1900.
SSH(TCP/UDP:22)	Secure Shell Remote Login Program.
STRMWORKS(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.

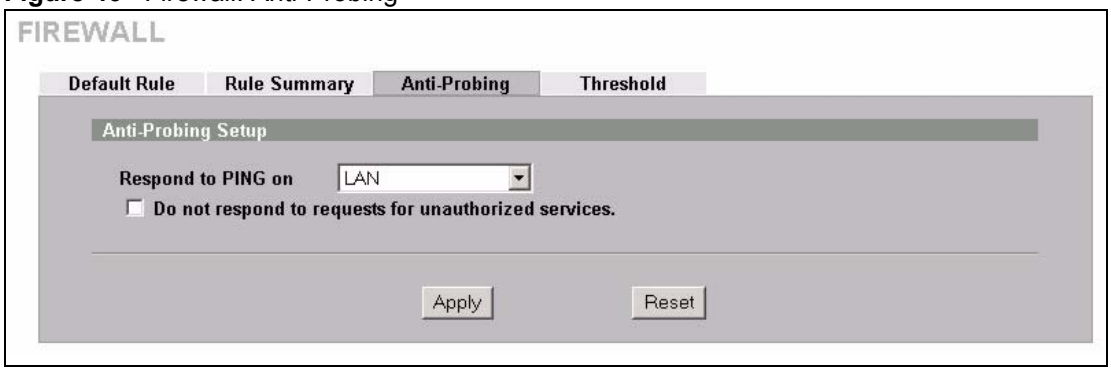
7.9 Anti-Probing

If an outside user attempts to probe an unsupported port on your ZyWALL, an ICMP response packet is automatically returned. This allows the outside user to know the ZyWALL exists. The ZyWALL supports anti-probing, which prevents ZyWALL ICMP response packet from being sent. This keeps outsiders from discovering your ZyWALL when unsupported ports are probed.

Internet Control Message Protocol (ICMP) is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.

Click **FIREWALL**, then the **Anti-Probing** tab to open the screen.

Figure 46 Firewall: Anti-Probing



The following table describes the labels in this screen.

Table 35 Firewall: Anti-Probing

LABEL	DESCRIPTION
Respond to PING on	The ZyWALL does not respond to any incoming Ping requests when **Disable** is selected. Select **LAN** to reply to incoming LAN Ping requests. Select **WAN** to reply to incoming WAN Ping requests. Select **LAN & WAN** to reply to incoming Ping requests on the LAN and WAN.
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. By default this option is not selected and 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. Note that the probing packets must first traverse the ZyWALL's firewall mechanism before reaching this anti-probing mechanism. Therefore if the firewall mechanism blocks a probing packet, the ZyWALL reacts based on the firewall policy, which by default, is to send a TCP reset packet for a blocked TCP packet. You can use the command "sys firewall tcprst rst [on|off]" to change this policy. When the firewall mechanism blocks a UDP packet, it drops the packet 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.

7.10 Configuring Attack Alert

Attack alerts are the first defense against DoS attacks. In the **Threshold** screen, shown later, you may choose to generate an alert whenever an attack is detected. For DoS attacks, the ZyWALL uses thresholds to determine when to drop sessions that do not become fully established. These thresholds apply globally to all sessions.

You can use the default threshold values, or you can change them to values more suitable to your security requirements.

7.10.1 Threshold Values

Tune these parameters when something is not working and after you have checked the firewall counters. These default values should work fine for normal small offices with ADSL bandwidth. 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.

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), then the default values should be reduced.

You should make any changes to the threshold values before you continue configuring firewall rules.

7.10.2 Half-Open Sessions

For TCP, half-open means that the session has not reached the established state-the TCP three-way handshake has not yet been completed (see Figure 31 on page 94). For UDP, half-open means that the firewall has detected no return traffic. An unusually high number of half-open sessions (either an absolute number or measured as the arrival rate) could indicate that a Denial of Service attack is occurring.

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.

When the number of existing half-open sessions rises above a threshold (**max-incomplete high**), the ZyWALL starts deleting half-open sessions as required to accommodate new connection requests. The ZyWALL continues to delete half-open requests as necessary, until the number of existing half-open sessions drops below another threshold (**max-incomplete low**).

When the rate of new connection attempts rises above a threshold (**one-minute high**), the ZyWALL starts deleting half-open sessions as required to accommodate new connection requests. The ZyWALL continues to delete half-open sessions as necessary, until the rate of new connection attempts drops below another threshold (**one-minute low**). The rate is the number of new attempts detected in the last one-minute sample period.

7.10.2.1 TCP Maximum Incomplete and Blocking Time

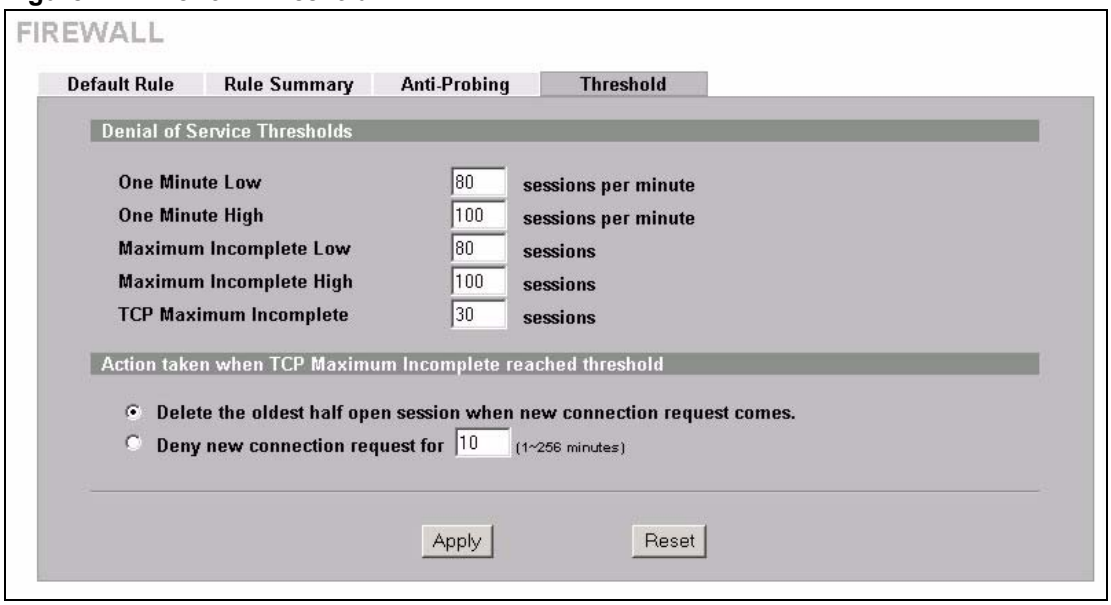
An unusually high number of half-open sessions with the same destination host address could indicate that a Denial of Service attack is being launched against the host.

Whenever the number of half-open sessions with the same destination host address rises above a threshold (**TCP Maximum Incomplete**), the ZyWALL starts deleting half-open sessions according to one of the following methods:

1. If the **Blocking Time** timeout is 0 (the default), then the ZyWALL deletes the oldest existing half-open session for the host for every new connection request to the host. This ensures that the number of half-open sessions to a given host will never exceed the threshold.
2. If the **Blocking Time** timeout is greater than 0, then the ZyWALL blocks all new connection requests to the host giving the server time to handle the present connections. The ZyWALL continues to block all new connection requests until the **Blocking Time** expires.

The ZyWALL also sends alerts whenever **TCP Maximum Incomplete** is exceeded. The global values specified for the threshold and timeout apply to all TCP connections. Click the **FIREWALL** link and then the **Threshold** tab to bring up the next screen.

Figure 47 Firewall: Threshold



The following table describes the labels in this screen.

Table 36 Firewall: Threshold

LABEL	DESCRIPTION
Denial of Service Thresholds	
One Minute Low	This is the rate of new half-open sessions 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.

Table 36 Firewall: Threshold (continued)

LABEL	DESCRIPTION
One Minute High	This is the rate of new half-open sessions 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. The numbers, say 80 in the **One Minute Low** field and 100 in this field, cause the ZyWALL to start deleting half-open sessions when more than 100 session establishment attempts have been detected in the last minute, and to stop deleting half-open sessions when fewer than 80 session establishment attempts have been detected in the last minute.
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. The above values, say 80 in the **Maximum Incomplete Low** field and 100 in this field, cause the ZyWALL to start deleting half-open sessions when the number of existing half-open sessions rises above 100, and to stop deleting half-open sessions with the number of existing half-open sessions drops below 80.
TCP Maximum Incomplete	This is 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.
Action taken when the TCP Maximum Incomplete threshold is reached.	
Delete the oldest half open session when new connection request comes	Select this radio button to clear the oldest half open session when a new connection request comes.
Deny new connection request for	Select this radio button and specify for how long the ZyWALL should block new connection requests when **TCP Maximum Incomplete** is reached. Enter the length of blocking time in minutes (between 1 and 256).
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

CHAPTER 8
Introduction to IPSec

This chapter introduces the basics of IPSec VPNs.

8.1 VPN Overview

A VPN (Virtual Private Network) 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 technologies/services used to transport traffic over the Internet or any insecure network that uses the TCP/IP protocol suite for communication.

8.1.1 IPSec

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.

8.1.2 Security Association

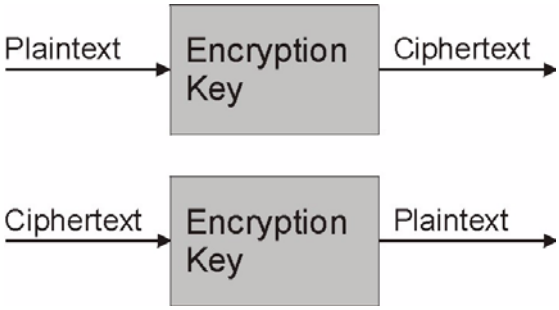
A Security Association (SA) is a contract between two parties indicating what security parameters, such as keys and algorithms they will use.

8.1.3 Other Terminology

8.1.3.1 Encryption

Encryption is a mathematical operation that transforms data from "plaintext" (readable) to "ciphertext" (scrambled text) using a "key". The key and clear text are processed by the encryption operation, which leads to the data scrambling that makes encryption secure. Decryption is the opposite of encryption: it is a mathematical operation that transforms ciphertext to plaintext. Decryption also requires a key.

Figure 48 Encryption and Decryption



8.1.3.2 Data Confidentiality

The IPSec sender can encrypt packets before transmitting them across a network.

8.1.3.3 Data Integrity

The IPSec receiver can validate packets sent by the IPSec sender to ensure that the data has not been altered during transmission.

8.1.3.4 Data Origin Authentication

The IPSec receiver can verify the source of IPSec packets. This service depends on the data integrity service.

8.1.4 VPN Applications

The ZyWALL supports the following VPN applications.

8.1.4.1 Linking Two or More Private Networks Together

Connect branch offices and business partners over the Internet with significant cost savings and improved performance when compared to leased lines between sites.

8.1.4.2 Accessing Network Resources When NAT Is Enabled

When NAT is enabled, remote users are not able to access hosts on the LAN unless the host is designated a public LAN server for that specific protocol. Since the VPN tunnel terminates inside the LAN, remote users will be able to access all computers that use private IP addresses on the LAN.

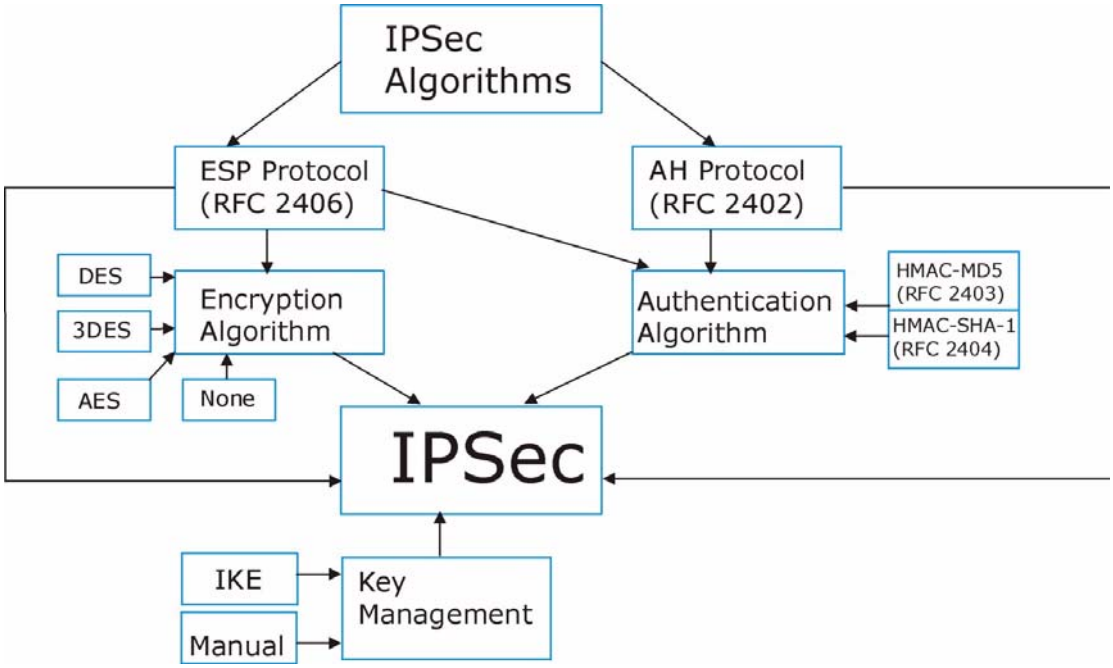
8.1.4.3 Unsupported IP Applications

A VPN tunnel may be created to add support for unsupported emerging IP applications. See Chapter 1 on page 31 for an example of a VPN application.

8.2 IPSec Architecture

The overall IPSec architecture is shown as follows.

Figure 49 IPSec Architecture



8.2.1 IPSec Algorithms

The **ESP** (Encapsulating Security Payload) Protocol (RFC 2406) and **AH** (Authentication Header) protocol (RFC 2402) describe the packet formats and the default standards for packet structure (including implementation algorithms).

The Encryption Algorithm describes the use of encryption techniques such as DES (Data Encryption Standard), AES (Advanced Encryption Standard) and Triple DES algorithms.

The Authentication Algorithms, HMAC-MD5 (RFC 2403) and HMAC-SHA-1 (RFC 2404, provide an authentication mechanism for the **AH** and **ESP** protocols. Refer to Section 9.2 on page 129 for more information.

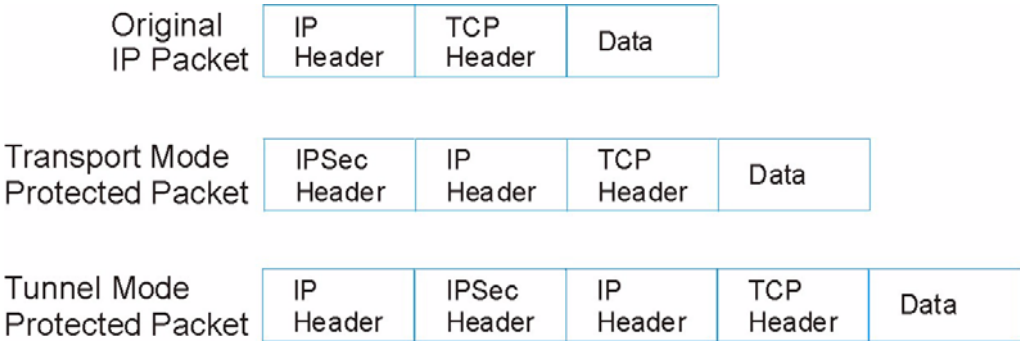
8.2.2 Key Management

Key management allows you to determine whether to use IKE (ISAKMP) or manual key configuration in order to set up a VPN.

8.3 Encapsulation

The two modes of operation for IPSec VPNs are **Transport** mode and **Tunnel** mode.

Figure 50 Transport and Tunnel Mode IPSec Encapsulation



8.3.1 Transport Mode

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).

With **ESP,** protection is applied only to the upper layer protocols contained in the packet. The IP header information and options are not used in the authentication process. Therefore, the originating IP address cannot be verified for integrity against the data.

With the use of **AH** as the security protocol, protection is extended forward into the IP header to verify the integrity of the entire packet by use of portions of the original IP header in the hashing process.

8.3.2 Tunnel Mode

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. This is the most common mode of operation. **Tunnel** mode is required for gateway to gateway and host to gateway communications. **Tunnel** mode communications have two sets of IP headers:

- **Outside header**: The outside IP header contains the destination IP address of the VPN gateway.
- **Inside header**: The inside IP header contains the destination IP address of the final system behind the VPN gateway. The security protocol appears after the outer IP header and before the inside IP header.

8.4 IPSec and NAT

Read this section if you are running IPSec on a host computer behind the ZyWALL.

NAT is incompatible with the **AH** protocol in both **Transport** and **Tunnel** mode. An IPSec VPN using the **AH** protocol digitally signs the outbound packet, both data payload and headers, with a hash value appended to the packet. When using **AH** protocol, packet contents (the data payload) are not encrypted.

A NAT device in between the IPSec endpoints will rewrite either the source or destination address with one of its own choosing. The VPN device at the receiving end will verify the integrity of the incoming packet by computing its own hash value, and complain that the hash value appended to the received packet doesn't match. The VPN device at the receiving end doesn't know about the NAT in the middle, so it assumes that the data has been maliciously altered.

IPSec using **ESP** in **Tunnel** mode encapsulates the entire original packet (including headers) in a new IP packet. The new IP packet's source address is the outbound address of the sending VPN gateway, and its destination address is the inbound address of the VPN device at the receiving end. When using **ESP** protocol with authentication, the packet contents (in this case, the entire original packet) are encrypted. The encrypted contents, but not the new headers, are signed with a hash value appended to the packet.

Tunnel mode **ESP** with authentication is compatible with NAT because integrity checks are performed over the combination of the "original header plus original payload," which is unchanged by a NAT device. **Transport** mode **ESP** with authentication is not compatible with NAT, although NAT traversal provides a way to use **Transport** mode **ESP** when there is a NAT router between the IPSec endpoints (See Section 9.5 on page 131 for details).

Table 37 VPN and NAT

SECURITY PROTOCOL	MODE	NAT
AH	Transport	N
AH	Tunnel	N
ESP	Transport	N
ESP	Tunnel	Y

CHAPTER 9
VPN Screens

This chapter introduces the VPN Web Configurator. See Chapter 15 on page 225 for information on viewing logs and Appendix N on page 347 for IPSec log descriptions.

9.1 VPN/IPSec Overview

Use the screens documented in this chapter to configure rules for VPN connections and manage VPN connections.

9.2 IPSec Algorithms

The **ESP** and **AH** protocols are necessary to create a Security Association (SA), the foundation of an IPSec VPN. An SA is built from the authentication provided by the **AH** and **ESP** protocols. The primary function of key management is to establish and maintain the SA between systems. Once the SA is established, the transport of data may commence.

9.2.1 AH (Authentication Header) Protocol

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.

In applications where confidentiality is not required or not sanctioned by government encryption restrictions, an **AH** can be employed to ensure integrity. This type of implementation does not protect the information from dissemination but will allow for verification of the integrity of the information and authentication of the originator.

9.2.2 ESP (Encapsulating Security Payload) Protocol

The **ESP** protocol (RFC 2406) provides encryption as well as the services offered by **AH**. **ESP** authenticating properties are limited compared to the **AH** due to the non-inclusion of the IP header information during the authentication process. However, **ESP** is sufficient if only the upper layer protocols need to be authenticated.

An added feature of the **ESP** is payload padding, which further protects communications by concealing the size of the packet being transmitted.

Table 38 ESP and AH

	ESP	AH
Encryption	**DES** (default) Data Encryption Standard (DES) is a widely used method of data encryption using a secret key. DES applies a 56-bit key to each 64-bit block of data.	
	3DES Triple DES (3DES) is a variant of DES, which iterates three times with three separate keys (3 x 56 = 168 bits), effectively doubling the strength of DES.	
	AES Advanced Encryption Standard is a newer method of data encryption that also uses a secret key. This implementation of AES applies a 128-bit key to 128-bit blocks of data. AES is faster than 3DES.	
	Select **NULL** to set up a phase 2 tunnel without encryption.	
Authentication	**MD5** (default) MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.	**MD5** (default) MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.
	SHA1 SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.	**SHA1** SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.
	Select **MD5** for minimal security and **SHA-1** for maximum security.	

9.3 My ZyWALL

My ZyWALL identifies the WAN IP address or domain name of the ZyWALL (if it has one) or leave the field set to **0.0.0.0**. The ZyWALL has to rebuild the VPN tunnel if the **My ZyWALL** IP address changes after setup.

9.4 Secure Gateway Address

Secure Gateway Address is the WAN IP address or domain name of the remote IPSec router (secure gateway).

If the remote secure gateway has a static WAN IP address, enter it in the **Secure Gateway Address** field. You may alternatively enter the remote secure gateway's domain name (if it has one) in the **Secure Gateway Address** field.

You can also enter a remote secure gateway's domain name in the **Secure Gateway Address** field if the remote secure gateway has a dynamic WAN IP address and is using DDNS. The ZyWALL has to rebuild the VPN tunnel each time the remote secure gateway's WAN IP address changes (there may be a delay until the DDNS servers are updated with the remote gateway's new WAN IP address).

9.4.1 Dynamic Secure Gateway Address

If the remote secure gateway has a dynamic WAN IP address and does not use DDNS, enter 0.0.0.0 as the secure gateway's address. In this case only the remote secure gateway can initiate SAs. This may be useful for telecommuters initiating a VPN tunnel to the company network. See Section 9.11 on page 146 for configuration examples.

Note: The Secure Gateway IP Address may be configured as 0.0.0.0 only when using **IKE** key management and not **Manual** key management.

9.4.2 Nailed Up

When you initiate an IPSec tunnel with nailed up enabled, the ZyWALL automatically renegotiates the tunnel when the IPSec SA lifetime period expires (see Section 8.1.2 on page 123 for more on the IPSec SA lifetime). In effect, the IPSec tunnel becomes an always on connection after you initiate it. Both IPSec routers must have a ZyWALL-compatible nailed up feature enabled in order for this feature to work.

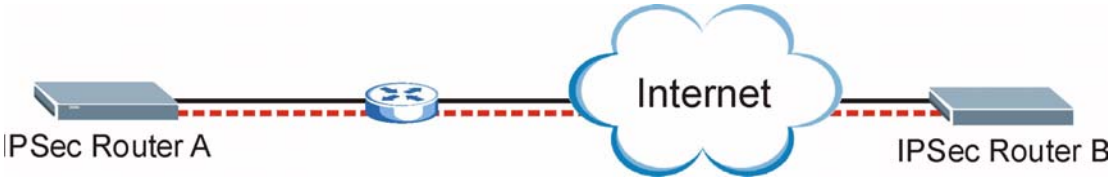
If the ZyWALL has its maximum number of simultaneous IPSec tunnels connected to it and they all have nailed up enabled, then no other tunnels can take a turn connecting to the ZyWALL because the ZyWALL never drops the tunnels that are already connected.

Note: When there is outbound traffic with no inbound traffic, the ZyWALL automatically drops the tunnel after two minutes.

9.5 NAT Traversal

NAT traversal allows you to set up a VPN connection when there are NAT routers between the two IPSec routers.

Figure 51 NAT Router Between IPSec Routers



Normally you cannot set up a VPN connection with a NAT router between the two IPSec routers because the NAT router changes the header of the IPSec packet. In the previous figure, IPSec router A sends an IPSec packet in an attempt to initiate a VPN. The NAT router changes the IPSec packet's header so it does not match the header for which IPSec router B is checking. Therefore, IPSec router B does not respond and the VPN connection cannot be built.

NAT traversal solves the problem by adding a UDP port 500 header to the IPSec packet. The NAT router forwards the IPSec packet with the UDP port 500 header unchanged. IPSec router B checks the UDP port 500 header and responds. IPSec routers A and B build a VPN connection.

9.5.1 NAT Traversal Configuration

For NAT traversal to work you must:

- Use ESP security protocol (in either transport or tunnel mode).
- Use IKE keying mode.
- Enable NAT traversal on both IPSec endpoints.

In order for IPSec router A (see Figure 51 on page 132) to receive an initiating IPSec packet from IPSec router B, set the NAT router to forward UDP port 500 to IPSec router A.

9.5.2 X-Auth (Extended Authentication)

With the Extended authentication feature on a remote IPSec router, added security is provided allowing you to use usernames and passwords for VPN connections. This is especially helpful when multiple ZyWALLs use one VPN rule to connect to a single remote IPSec router. An attacker cannot make a VPN connection without a valid username and password.

The extended authentication server checks the user names and passwords of the extended authentication clients before completing the IPSec connection .

A remote IPSec router can be an extended authentication server for some VPN connections and an extended authentication client for other VPN connections.

9.5.3 Authentication Server

A ZyWALL set to be a VPN extended authentication server can use either the username-password pair to the ZyWALL or an external RADIUS server for VPN authentication.

9.6 ID Type and Content

With aggressive negotiation mode (see Section 3.3.7.1 on page 63), the ZyWALL identifies incoming SAs by ID type and content since this identifying information is not encrypted. This enables the ZyWALL to distinguish between multiple rules for SAs that connect from remote IPSec routers that have dynamic WAN IP addresses. Telecommuters can use separate passwords to simultaneously connect to the ZyWALL from IPSec routers with dynamic IP addresses (see Section 9.11.2 on page 147 for a telecommuter configuration example)

Note: Regardless of the ID type and content configuration, the ZyWALL does not allow you to save multiple active rules with overlapping local and remote IP addresses.

With main mode (see Section 3.3.7.1 on page 63), the ID type and content are encrypted to provide identity protection. In this case the ZyWALL can only distinguish between up to 12 different incoming SAs that connect from remote IPSec routers that have dynamic WAN IP addresses. The ZyWALL can distinguish up to 12 incoming SAs because you can select between three encryption algorithms (DES, 3DES and AES), two authentication algorithms (MD5 and SHA1) and two key groups (DH1 and DH2) when you configure a VPN rule (see Section 9.8.2 on page 140). The ID type and content act as an extra level of identification for incoming SAs.

The type of ID can be a domain name, an IP address or an e-mail address. The content is the IP address, domain name, or e-mail address.

Table 39 Local ID Type and Content Fields

LOCAL ID TYPE=	CONTENT=
IP	Type the IP address of your computer or leave the field blank to have the ZyWALL automatically use its own IP address.
DNS	Type a domain name (up to 31 characters) by which to identify this ZyWALL.
E-mail	Type an e-mail address (up to 31 characters) by which to identify this ZyWALL.
The domain name or e-mail address that you use in the **Content** field is used for identification purposes only and does not need to be a real domain name or e-mail address.	

Table 40 Peer ID Type and Content Fields

PEER ID TYPE=	CONTENT=
IP	Type the IP address of the computer with which you will make the VPN connection or leave the field blank to have the ZyWALL automatically use the address in the **Secure Gateway Address** field.
DNS	Type a domain name (up to 31 characters) by which to identify the remote IPSec router.
E-mail	Type an e-mail address (up to 31 characters) by which to identify the remote IPSec router.

Table 40 Peer ID Type and Content Fields

PEER ID TYPE=	CONTENT=
Subject Name	Type the subject name (up to 255 characters) by which to identify the remote IPSec router. This option is available only when you set **Authentication Method** to **Certificate**.
The domain name or e-mail address that you use in the **Content** field is used for identification purposes only and does not need to be a real domain name or e-mail address. The domain name also does not have to match the remote router's IP address or what you configure in the **Secure Gateway Address** field below.	

9.6.1 ID Type and Content Examples

Two IPSec routers must have matching ID type and content configuration in order to set up a VPN tunnel.

The two ZyWALLs in this example can complete negotiation and establish a VPN tunnel.

Table 41 Matching ID Type and Content Configuration Example

ZYWALL A	ZYWALL B
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

The two ZyWALLs in this example cannot complete their negotiation because ZyWALL B's **Local ID type** is **IP**, but ZyWALL A's **Peer ID type** is set to **E-mail**. An ID mismatched message displays in the IPSEC LOG.

Table 42 Mismatching ID Type and Content Configuration Example

ZYWALL A	ZYWALL B
Local ID type: IP	Local ID type: IP
Local ID content: 1.1.1.10	Local ID content: 1.1.1.10
Peer ID type: E-mail	Peer ID type: IP
Peer ID content: aa@yahoo.com	Peer ID content: N/A

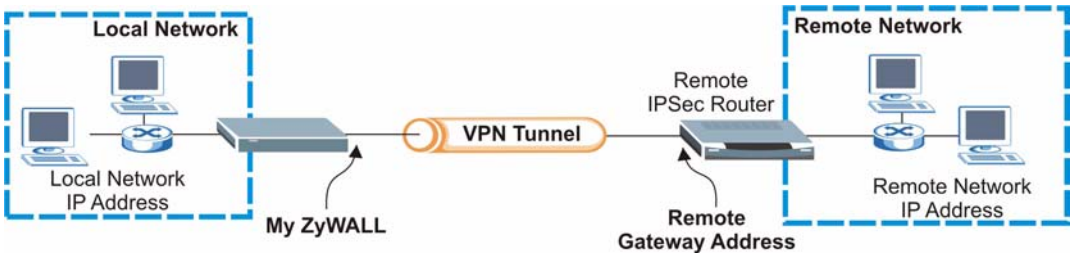
9.7 Pre-Shared Key

A pre-shared key identifies a communicating party during a phase 1 IKE negotiation (see Section 3.3.7 on page 62 for more on IKE phases). It is called pre-shared because you have to share it with another party before you can communicate with them over a secure connection.

9.8 IKE VPN Rule Summary Screen

The following figure helps explain the main fields in the web configurator.

Figure 52 IPSec Summary Fields

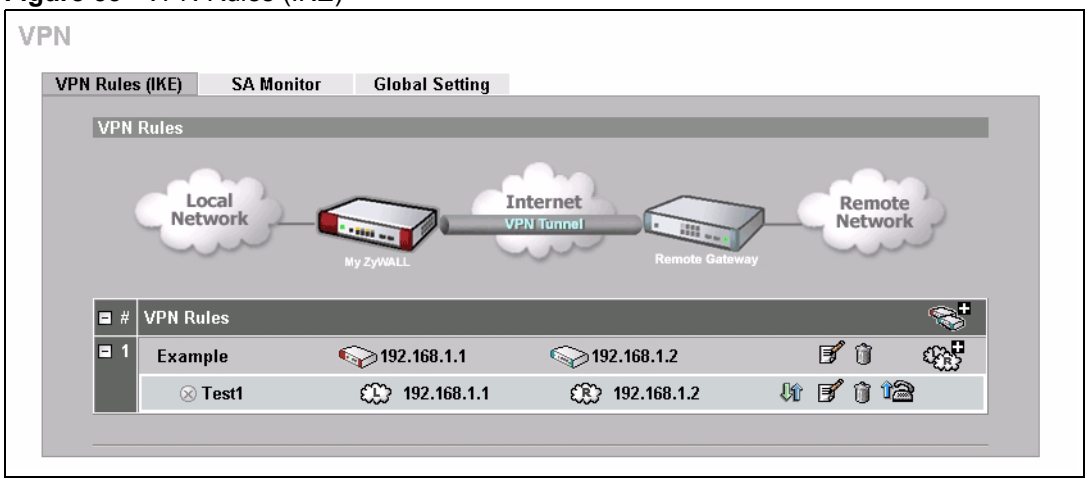


Note: Local and remote IP addresses must be static.

Click **VPN** display the **VPN Rules (IKE)** screen. This is a read-only menu of your IPSec rule (tunnel). To add a rule, click the add ( ) icon. Edit an IPSec rule by clicking the edit ( ) icon to configure the associated submenus.

Note: You can only configure one VPN rule with one IPSec policy.

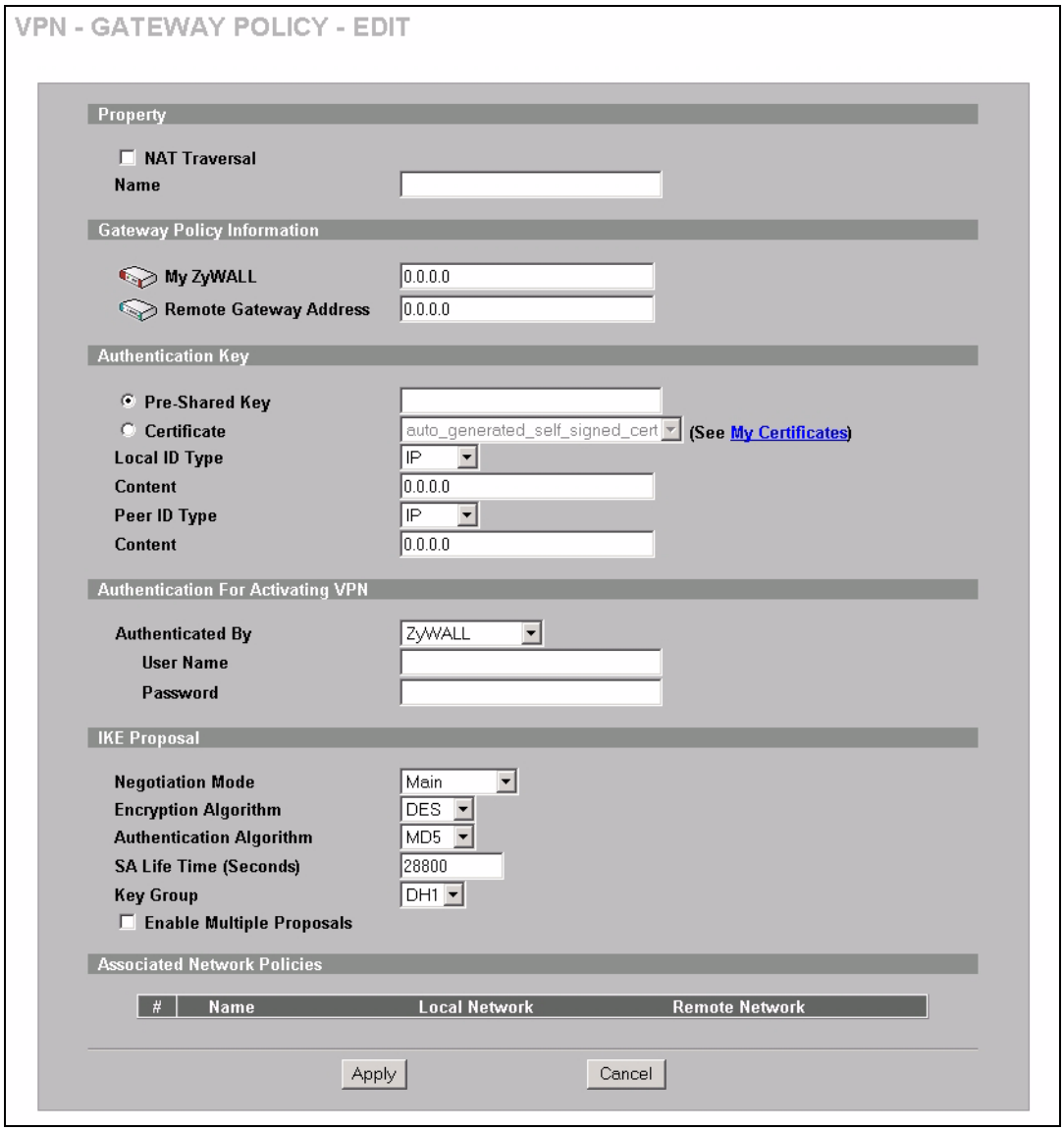
Figure 53 VPN Rules (IKE)



9.8.1 Configurign an IKE VPN Rule

In the **VPN Rule (IKE)** screen, click the add ( ) or edit ( ) icon to display the **VPN-Gateway Policy -Edit** screen.

Figure 54 VPN Rules (IKE): Gateway Policy



The following table describes the labels in this screen. .

Table 43 VPN Rules (IKE): Gateway Policy

LABEL	DESCRIPTION
Property	
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. The remote IPSec router must also have NAT traversal enabled. 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 port 500 to the IPSec router behind the NAT router.
Name	Type up to 32 characters to identify this VPN policy. You may use any character, including spaces, but the ZyWALL drops trailing spaces.

Table 43 VPN Rules (IKE): Gateway Policy (continued)

LABEL	DESCRIPTION
Gateway Policy Information	
My ZyWALL	This field identifies the WAN IP address of the ZyWALL. You can enter the ZyWALL's static WAN IP address (if it has one) or leave the field set to 0.0.0.0. The VPN tunnel has to be rebuilt if the **My ZyWALL** field changes after setup.
Remote Gateway Address	Type the WAN IP addressof 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.
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. 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. 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. 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. Select **DNS** to identify this ZyWALL by a domain name. Select **E-mail** to identify this ZyWALL by an e-mail address. You do not configure the local ID type and content when you set **Authentication Method** 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. 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. • When there is a NAT router between the two IPSec routers. • 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. 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 43 VPN Rules (IKE): Gateway Policy (continued)

LABEL	DESCRIPTION
Peer ID Type	Select from the following when you set **Authentication Method** to **Pre-shared Key**. • Select **IP** to identify the remote IPSec router by its IP address. • Select **DNS** to identify the remote IPSec router by a domain name. • Select **E-mail** to identify the remote IPSec router by an e-mail address. Select from the following when you set **Authentication Method** to **Certificate**. • 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. • 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. • 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. • Select **Subject Name** to identify the remote IPSec router by the subject name of the certificate it uses for this VPN connection. • 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. Do the following when you set **Authentication Method** to **Pre-shared Key**. • 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 **Remote Gateway Address** field (refer to the **Remote Gateway Address** field description). • 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. 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: • When there is a NAT router between the two IPSec routers. • When you want the ZyWALL to distinguish between VPN connection requests that come in from remote IPSec routers with dynamic WAN IP addresses. Do the following when you set **Authentication Method** to **Certificate**. • 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 **Remote Gateway Address** field (refer to the **Remote Gateway Address** field description). • 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. • 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. • For **Any**, the peer **Content** field is not available. • Regardless of how you configure the **ID Type** and **Content** fields, two active SAs cannot have both the local and remote IP address ranges overlap between rules.
Authentication for Activating VPN	Confiugre the fields below to set the authentication method the ZyWALL uses to allow a user to activate a VPN connection.

Table 43 VPN Rules (IKE): Gateway Policy (continued)

LABEL	DESCRIPTION
Authenticated by	Select **XAUTH** to to have the remote IPSec router authenticate user(s) that request this VPN connection. **Note:** You must also configure extended authentication on the remote IPsec router. Select **ZyWALL** to have your ZyWALL authenticate user(s) using a username and password when initiating this VPN connection. Select this option if the remote IPSec router is not configured to authenticate VPN user or does not have the extended authentication function. Select **None** to have the ZyWALL automatically try to establish a VPN connection when packets are sent. No user authentication is required.
User Name	Enter a user name to authenticate the VPN user. The user name can be up to 31 case-sensitive ASCII characters, but spaces are not allowed.
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 **DES**, **3DES** or **AES** from the drop-down list box. When you use one of these encryption algorithms for data communications, both the sending device and the receiving device must use 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	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.
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). 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	You must choose a key group for phase 1 IKE setup. **DH1** (default) refers to Diffie-Hellman Group 1 a 768 bit random number. **DH2** refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number.
Enable Multiple Proposals	Select this check box to allow the ZyWALL to use any of its phase 1 or phase 2 encryption and authentication algorithms when negotiating an IPSec SA. Clear this check box to have the ZyWALL use only the phase 1 or phase 2 encryption and authentication algorithms configured below when negotiating an IPSec SA.
Associated Network Policy	The following table shows the policy(ies) you configure for this rule. To add a VPN policy, click the add policy icon ( ) in the main **VPN Rules (IKE)** screen.
#	This field displays the policy index number.

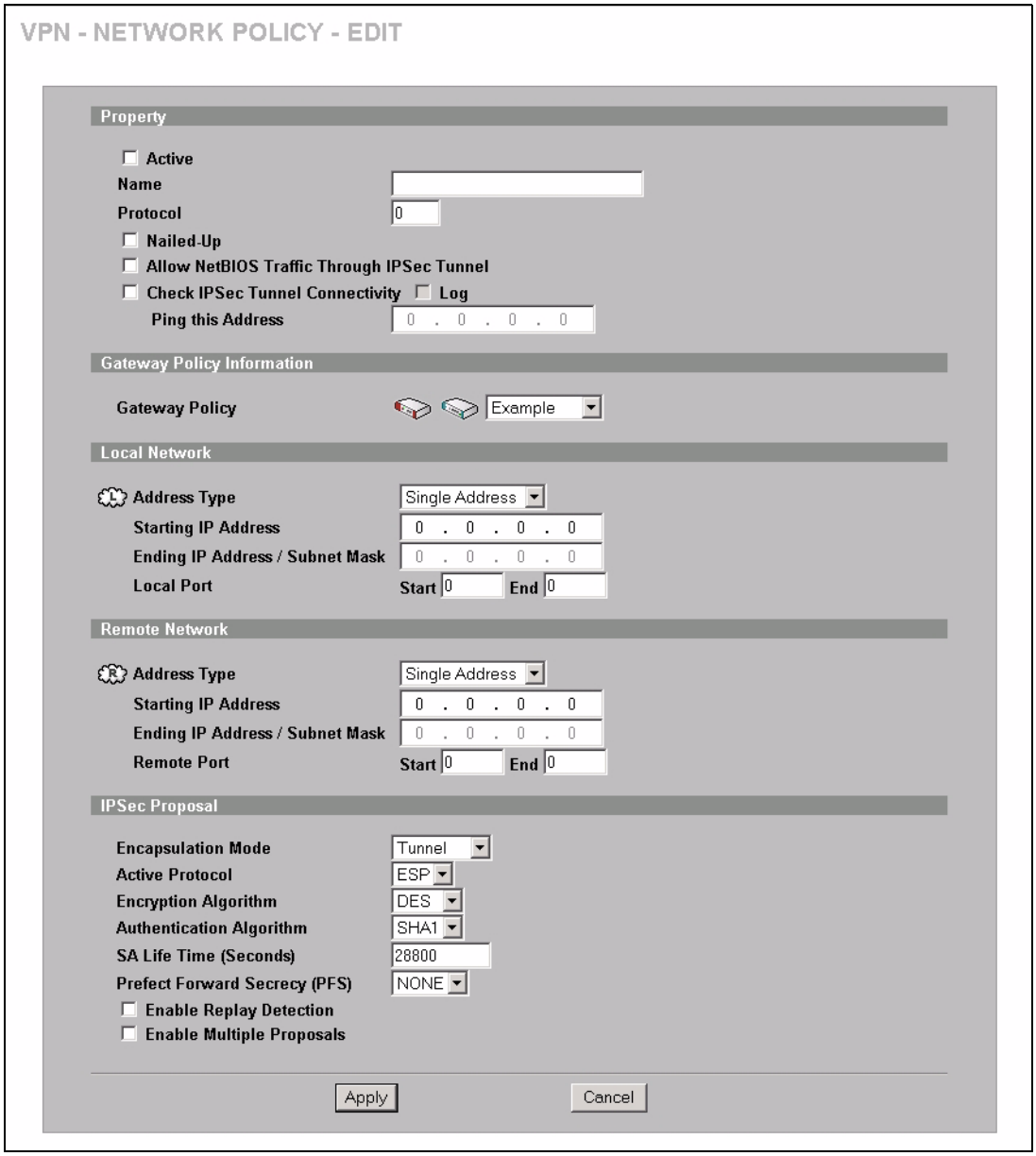
Table 43 VPN Rules (IKE): Gateway Policy (continued)

LABEL	DESCRIPTION
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.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving.

9.8.2 Configuring an IKE VPN Policy

To configure a VPN policy, click the add policy icon ( ) in the **VPN Rules (IKE)** screen. A screen displays as follows.

Figure 55 VPN Rules (IKE): Network Policy



The following table describes the labels in this screen.

Table 44 VPN Rules (IKE): Add Policy

LABEL	DESCRIPTION
Active	Select this check box to activate this VPN tunnel. This option determines whether a VPN rule is applied.
Name	Type a name to identify this VPN policy. You may use any character, including spaces, but the ZyWALL drops trailing spaces.
Protocol	Enter 1 for ICMP, 6 for TCP, 17 for UDP, etc. 0 is the default and signifies any protocol.

Table 44 VPN Rules (IKE): Add Policy (continued)

LABEL	DESCRIPTION
Nailed-Up	Select this check box to turn on the nailed up feature for this SA. 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.
Allow NetBIOS Traffic Through IPSec Tunnel	NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast 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. 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. 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	
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	Select the gateway policy to wich you want to use the VPN policy.
Local Network	Local IP addresses must be static and correspond to the remote IPSec router's configured remote IP addresses. 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.
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	Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses. 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.

Table 44 VPN Rules (IKE): Add Policy (continued)

LABEL	DESCRIPTION
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. 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. A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Perfect Forward Secret (PFS)	Perfect Forward Secret (PFS) is disabled (**None**) by default in phase 2 IPSec SA setup. This allows faster IPSec setup, but is not so secure. Select **DH1** or **DH2** 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).
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 setting this field to **YES**.

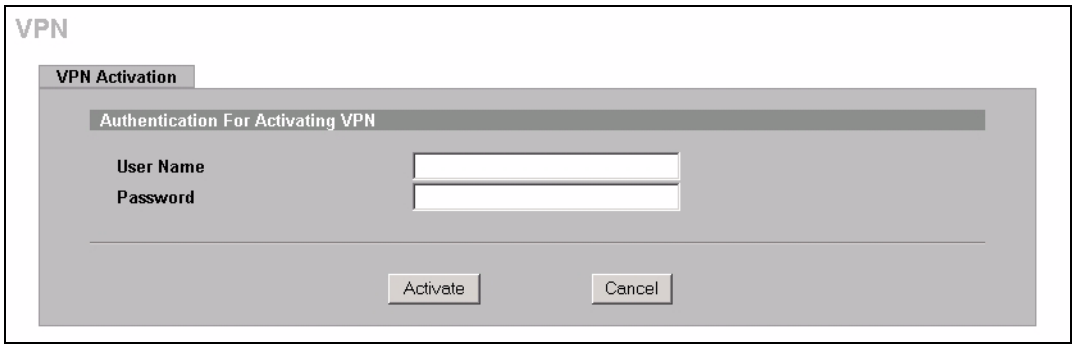
Table 44 VPN Rules (IKE): Add Policy (continued)

LABEL	DESCRIPTION
Enable Multiple Proposal	Select this check box to allow the ZyWALL to use any of its phase 1 or phase 2 encryption and authentication algorithms when negotiating an IKE SA. Clear this check box to have the ZyWALL use only the phase 1 or phase 2 encryption and authentication algorithms configured below when negotiating an IKE SA.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to discard all changes and return to the main VPN screen.

9.8.2.1 Activating a VPN Connection

After you have configured a VPN rule, click the connect icon ( ) in the **VPN Rule (IKE)** screen to establish a VPN tunnel. A **VPN Activation** screen displays as shown.

Figure 56 VPN Rule (IKE): VPN Activation



The following table describes the labels in this screen.

Table 45 VPN Rule (IKE): VPN Activation

LABEL	DESCRIPTION
user Name	Enter the user name for this VPN connection.
Password	Enter the password associated to the user name above.
Activate	Click **Activate** to establish a VPN connection.
Cancel	Click **Cancel** to discard all changes and return to the **VPN Rule (IKE)** screen.

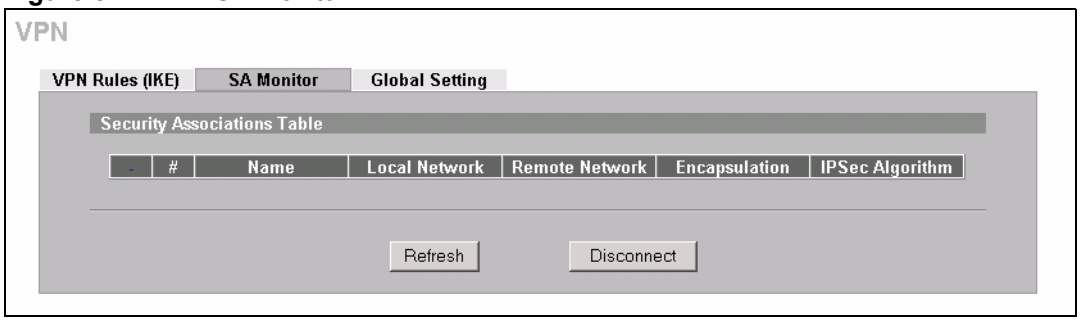
9.9 Viewing SA Monitor

In the web configurator, click **VPN** and the **SA Monitor** tab. 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. This screen is read-only. The following table describes the fields in this tab.

Note: When there is outbound traffic but no inbound traffic, the SA times out automatically after two minutes. A tunnel with no outbound or inbound traffic is "idle" and does not timeout until the SA lifetime period expires. See Section 9.4.2 on page 131 on keep alive to have the ZyWALL renegotiate an IPSec SA when the SA lifetime expires, even if there is no traffic.

Figure 57 VPN: SA Monitor



The following table describes the labels in this screen.

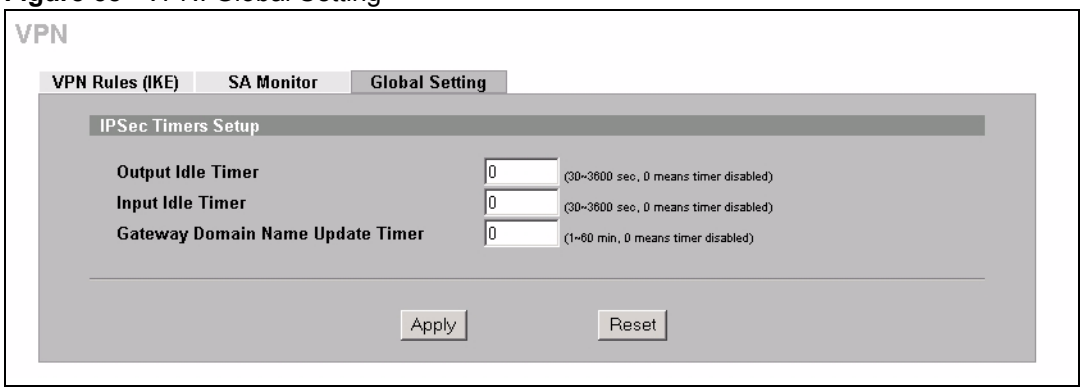
Table 46 SA Monitor

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. 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**.

9.10 Configuring Global Setting

To change your ZyWALL's global settings, click **VPN**, then the **Global Setting** tab. The screen appears as shown.

Figure 58 VPN: Global Setting



The following table describes the labels in this screen.

Table 47 VPN: Global Setting

LABEL	DESCRIPTION
Output Idle Timer	Enter the time period (between 30 and 3600 seconds) to wait before the ZyWALL checks the VPN connection to the remote IPSec router. When traffic is sent to the remote IPSec route from which no reply is received after the specified time period, the ZyWALL checks the VPN connectivity. If the remote IPSec router does not reply with an acknowledgement, the ZyWALL automatically disconnects the VPN tunnel. Enter **0** to disable this feature.
Input Idle Timer	Enter the time period (between 30 and 3600 seconds) to wait before the ZyWALL checks the VPN connection to the remote IPSec router. When no traffic is sent to and/or received from the remote IPSec router after the specified time period, the ZyWALL sends checks the VPN connectivity. If the remote IPSec router does not reply with an acknowledgement, the ZyWALL automatically disconnects the VPN tunnel. Enter **0** to diable this feature.
Gateway Domain Name Update Timers	This field is applicable when you enter a domain name to identify the ZyWALL and/or the remote secure gateway. Enter the time period (between 30 and 3600 seconds) to wait before the ZyWALL updates the domain name and IP address mapping through a DNS server. Enter **0** to disable this feature.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

9.11 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.

9.11.1 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 59 Telecommuters Sharing One VPN Rule Example

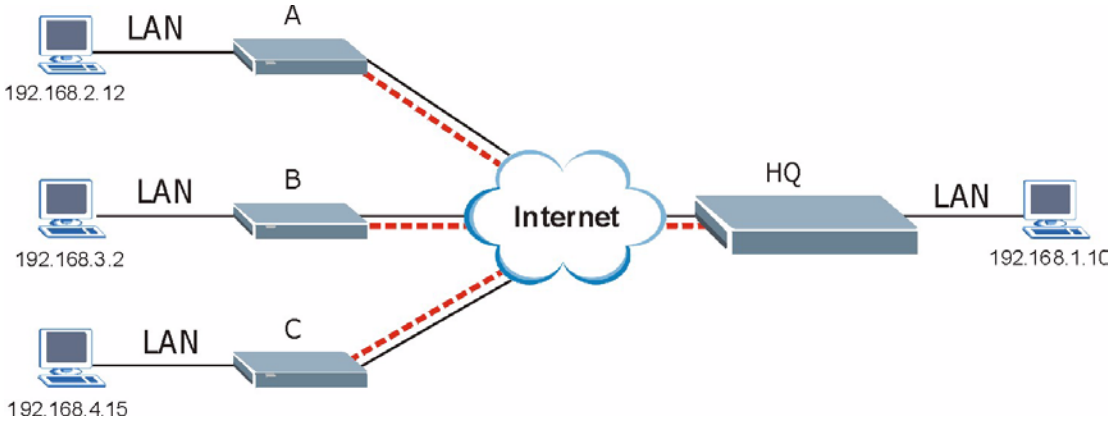


Table 48 Telecommuters Sharing One VPN Rule Example

FIELDS	HEADQUARTERS	TELECOMMUTERS
My IP Address:	Public static IP address	0.0.0.0 (dynamic IP address assigned by the ISP)
Secure Gateway IP Address:	0.0.0.0 With this IP address only the telecommuter can initiate the IPSec tunnel.	Public static IP address
Local IP Address:	192.168.1.10	Telecommuter A: 192.168.2.12 Telecommuter B: 192.168.3.2 Telecommuter C: 192.168.4.15
Remote IP Address:	0.0.0.0 (N/A)	192.168.1.10

9.11.2 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 Section 3.3.7.1 on page 63), 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 60 Telecommuters Using Unique VPN Rules Example

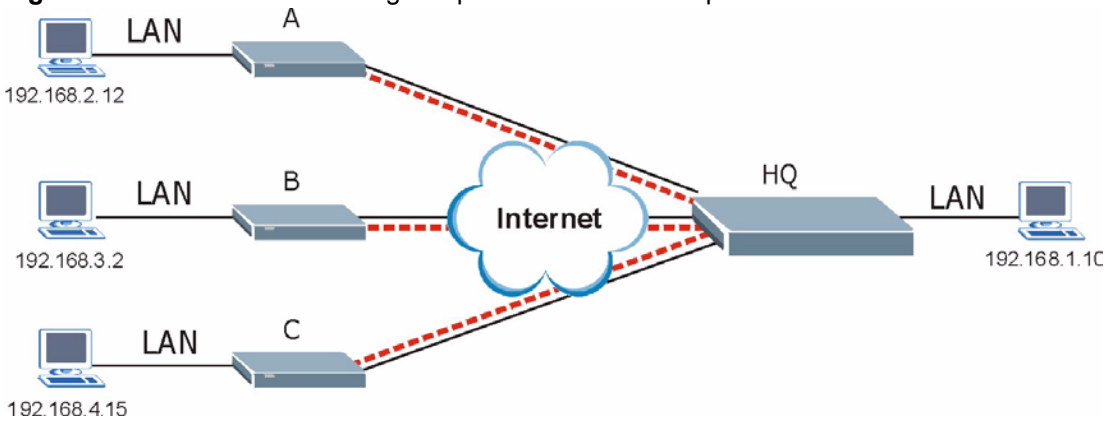


Table 49 Telecommuters Using Unique VPN Rules Example

TELECOMMUTERS	HEADQUARTERS
All Telecommuter Rules:	All Headquarters Rules:
My IP Address 0.0.0.0	My IP Address: bigcompanyhq.com
Secure Gateway Address: bigcompanyhq.com	Local IP Address: 192.168.1.10
Remote 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	Secure Gateway Address: telecommuter1.com
	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	Secure Gateway Address: telecommuterb.com
	Remote Address 192.168.3.2

Table 49 Telecommuters Using Unique VPN Rules Example (continued)

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	Secure Gateway Address: telecommuterc.com
	Remote Address 192.168.4.15

9.12 VPN and Remote Management

If a VPN tunnel uses Telnet, FTP, WWW, SNMP, DNS or ICMP, then you should configure remote management (**REMOTE MGMT**) to allow access for that service.

CHAPTER 10
Certificates

This chapter gives background information about public-key certificates and explains how to use them.

10.1 Certificates 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.

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.

In public-key encryption and decryption, 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 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, not to encrypt the data that you send after establishing a connection. The method used to secure the data that you send through an established connection depends on the type of connection. For example, a VPN tunnel might use the triple DES encryption algorithm.

The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates.

A certification path is the hierarchy of certification authority certificates that validate a certificate. The ZyWALL does not trust a certificate if any certificate on its path has expired or been revoked.

Certification authorities maintain directory servers with databases of valid and revoked certificates. A directory of certificates that have been revoked before the scheduled expiration is called a CRL (Certificate Revocation List). The ZyWALL can check a peer's certificate against a directory server's list of revoked certificates. The framework of servers, software, procedures and policies that handles keys is called PKI (public-key infrastructure).

10.1.1 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.

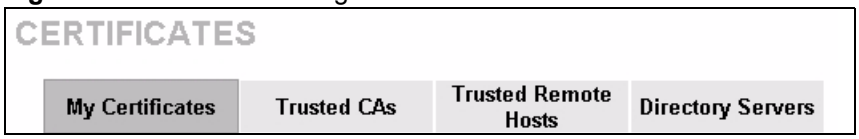
10.2 Self-signed Certificates

Until public-key infrastructure becomes more mature, it may not be available in some areas. You can have the ZyWALL act as a certification authority and sign its own certificates.

10.3 Configuration Summary

This section summarizes how to manage certificates on the ZyWALL.

Figure 61 Certificate Configuration Overview

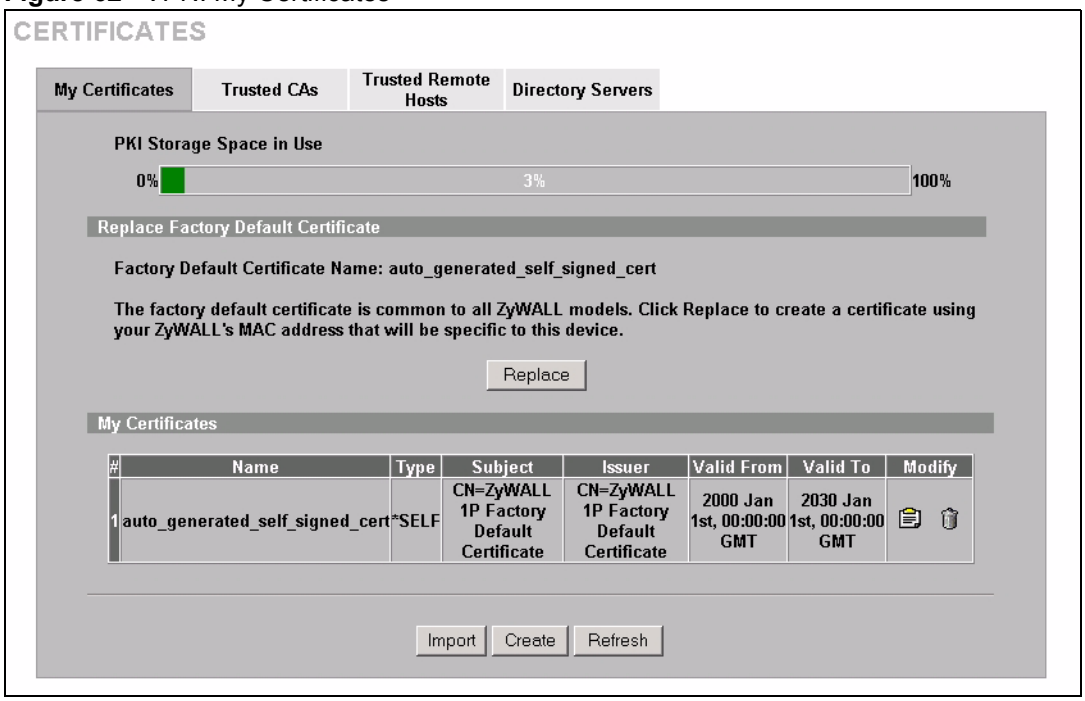


- Use the **My Certificate** screens to generate and export self-signed certificates or certification requests and import the ZyWALL's CA-signed certificates.
- Use the **Trusted CA** screens to save CA certificates to the ZyWALL.
- Use the **Trusted Remote Hosts** screens to import self-signed certificates.
- Use the **Directory Servers** screen to configure a list of addresses of directory servers (that contain lists of valid and revoked certificates).

10.4 My Certificates

Click **CERTIFICATES**, **My Certificates** to open the ZyWALL's summary list of certificates and certification requests. Certificates display in black and certification requests display in gray. See the following figure.

Figure 62 VPN: My Certificates



The following table describes the labels in this screen.

Table 50 Certificate: My Certificates

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the ZyWALL's PKI storage space that is currently in use. When you are using 80% or less of the storage space, the bar is green. When the amount of space used is over 80%, the bar is red. When the bar is red, 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. **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. **SELF** represents a self-signed certificate. ***SELF** represents the default self-signed certificate, which the ZyWALL uses to sign imported trusted remote host certificates. **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 50 Certificate: 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. Click the delete ( ) icon to remove the certificate. A window displays asking you to confirm that you want to delete the certificate. You cannot delete a certificate that one or more features is configured to use. Do the following to delete a certificate that shows ***SELF** in the **Type** field. 1. Make sure that no other features, such as HTTPS, VPN, SSH are configured to use the ***SELF** certificate. 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). 3. Select the **Default self-signed certificate which signs the imported remote host certificates** check box. 4. Click **Apply** to save the changes and return to the **My Certificates** screen. 5. The certificate that originally showed ***SELF** displays **SELF** and you can delete it now. **Note:** Subsequent certificates move up by one when you take this action.
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.

10.5 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.

10.6 Importing a Certificate

Click **CERTIFICATES**, **My Certificates** and then **Import** to open the **My Certificate Import** screen. Follow the instructions in this screen to save an existing certificate to the ZyWALL, see the following figure.

Note: You can only import a certificate that matches a corresponding certification request that was generated by the ZyWALL.

The certificate you import replaces the corresponding request in the **My Certificates** screen.

You must remove any spaces from the certificate's filename before you can import it.

Figure 63 Certificate: My Certificate: Import

The following table describes the labels in this screen.

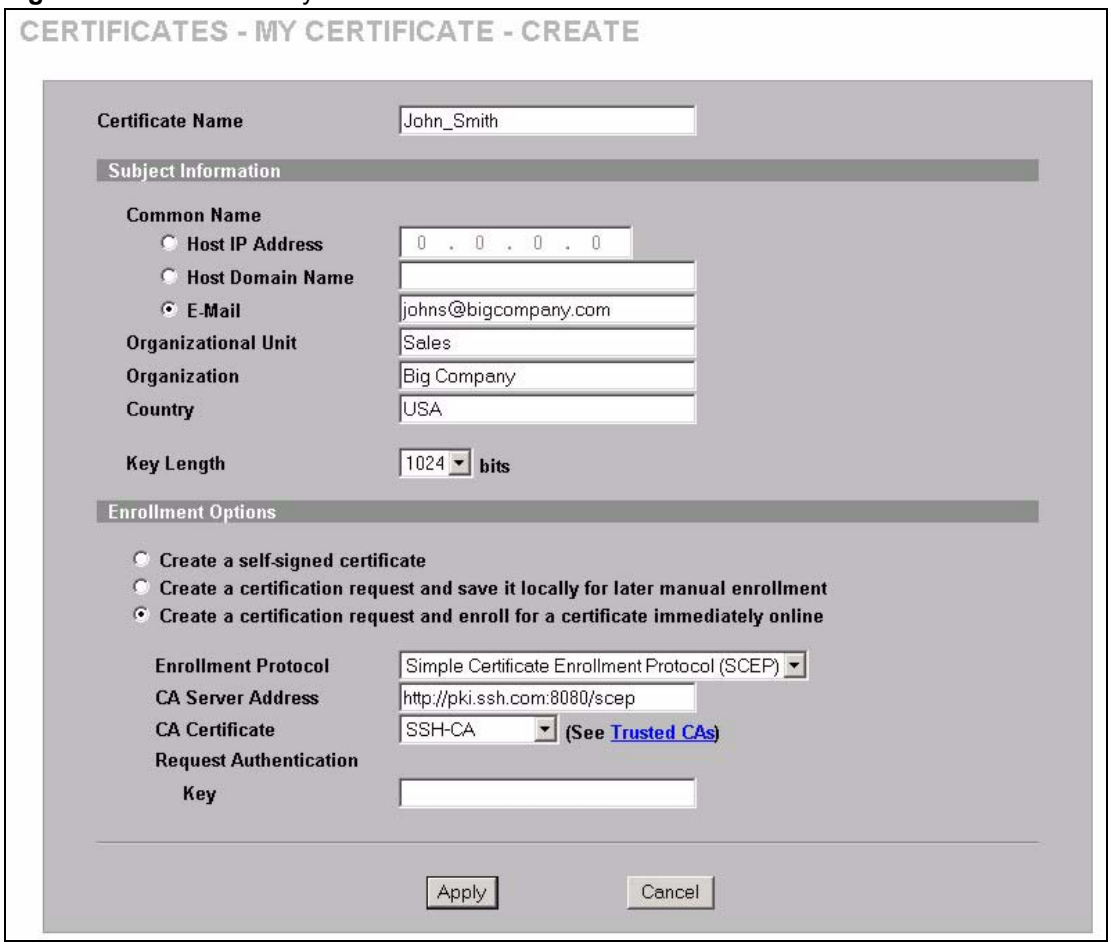
Table 51 Certificate: My Certificate: Import

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.

10.7 Creating a Certificate

Click **CERTIFICATES**, **My Certificates** and then **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, see the following figure.

Figure 64 Certificate: My Certificate: Create



The following table describes the labels in this screen.

Table 52 Certificate: My Certificate: 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, although the **Common Name** is mandatory. The certification authority may add fields (such as a serial number) to the subject information when it issues a certificate. It is recommended that each certificate have unique subject information.

Table 52 Certificate: My Certificate: 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 127 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 127 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 127 characters to identify the nation where the certificate owner is located. You may use any character, including spaces, but the ZyWALL drops trailing spaces.
Key Length	Select a number from the drop-down list box to determine how many bits the key should use (512 to 2048). The longer the key, the more secure it is. A longer key also uses more PKI storage space.
Enrollment Options	These radio buttons deal with how and when the certificate is to be generated.
Create a self-signed certificate	Select **Create a self-signed certificate** to have the ZyWALL generate the certificate and act as the Certification Authority (CA) itself. This way you do not need to apply to a certification authority for certificates.
Create a certification request and save it locally for later manual enrollment	Select **Create a certification request and save it locally for later manual enrollment** to have the ZyWALL generate and store a request for a certificate. Use the **My Certificate Details** screen to view the certification request and copy it to send to the certification authority. Copy the certification request from the **My Certificate Details** screen (see Section 10.8 on page 158) 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. You must have the certification authority's certificate already imported in the **Trusted CAs** screen. 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. **Simple Certificate Enrollment Protocol (SCEP)** is a TCP-based enrollment protocol that was developed by VeriSign and Cisco. **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. 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.

Table 52 Certificate: My Certificate: Create (continued)

LABEL	DESCRIPTION
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 SECP enrollment protocol.
Key	Type the key that the certification authority gave you.
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.

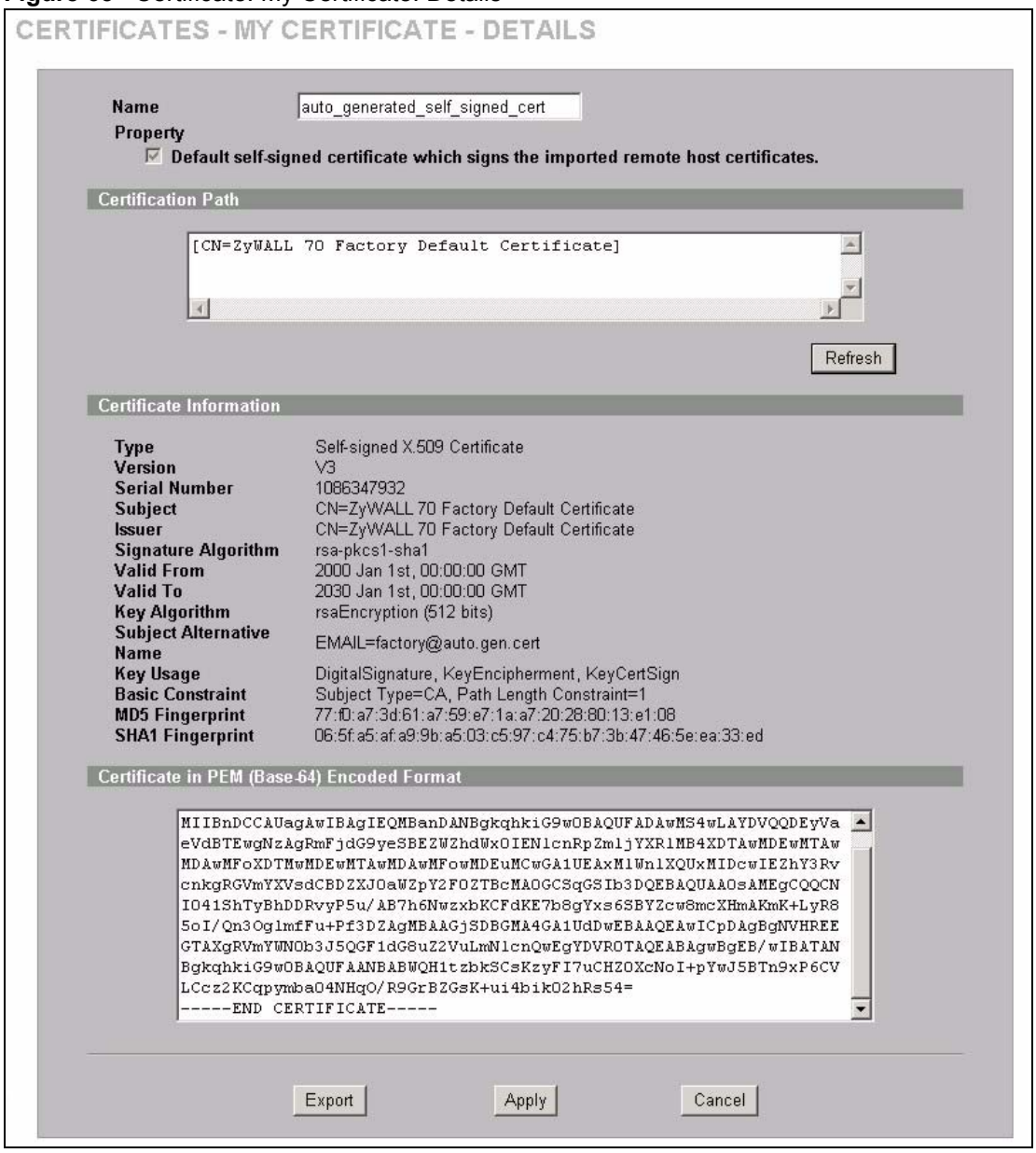
After the ZyWALL successfully enrolls a certificate or generates a certification request or a self-signed certificate, you see a screen with a **Return** button that takes you back to the **My Certificates** screen.

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.

10.8 My Certificate Details

Click **CERTIFICATES**, and then **My Certificates** to open the **My Certificates** screen (see Figure 62 on page 153). 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. In the case of a self-signed certificate, you can set it to be the one that the ZyWALL uses to sign the trusted remote host certificates that you import to the ZyWALL.

Figure 65 Certificate: My Certificate: Details



The following table describes the labels in this screen.

Table 53 Certificate: My Certificate: 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).
Property Default self-signed certificate which signs the imported remote host certificates.	Select this check box to have the ZyWALL use this certificate to sign the trusted remote host certificates that you import to the ZyWALL. This check box is only available with self-signed certificates. If this check box is already selected, you cannot clear it in this screen, you must select this check box in another self-signed certificate's details screen. This automatically clears the check box in the details screen of the certificate that was previously set to sign the imported trusted remote host certificates.
Certification Path	Click the **Refresh** button to have this read-only text box display the hierarchy of certification authorities that validate the certificate (and the certificate itself). If the issuing certification authority is one that you have imported as a trusted certification authority, it may be the only certification authority in the list (along with the certificate itself). If the certificate is a self-signed certificate, the certificate itself is the only one in the list. The ZyWALL does not trust the certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.
Refresh	Click **Refresh** to display the certification path.
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). "X.509" means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority or generated by the ZyWALL.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country. 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).

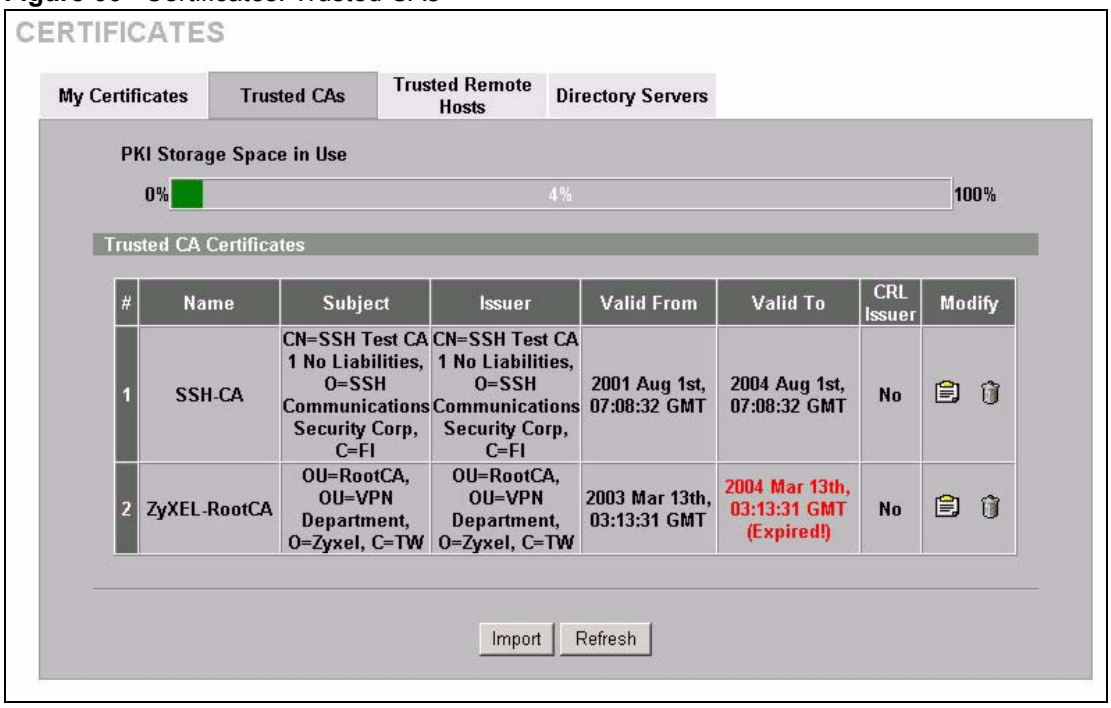
Table 53 Certificate: My Certificate: Details (continued)

LABEL	DESCRIPTION
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. 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. You can copy and paste a certificate into an e-mail to send to friends or colleagues or you can copy and paste a certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Export	Click this button and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.
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.

10.9 Trusted CAs

Click **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. See the following figure.

Figure 66 Certificates: Trusted CAs



The following table describes the labels in this screen.

Table 54 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 you are using 80% or less of the storage space, the bar is green. When the amount of space used is over 80%, the bar is red. When the bar is red, 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.

Table 54 Certificates: Trusted CAs (continued)

LABEL	DESCRIPTION
CRL Issuer	This field displays **Yes** if the certification authority issues Certificate Revocation Lists for the certificates that it has issued and you have selected the **Issues certificate revocation lists (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**.
Modify	Click the details icon to open a screen with an in-depth list of information about the certificate. 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.

10.10 Importing a Trusted CA's Certificate

Click **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 to the ZyWALL, see the following figure.

Note: You must remove any spaces from the certificate's filename before you can import the certificate.

Figure 67 Trusted CA Import

The following table describes the labels in this screen.

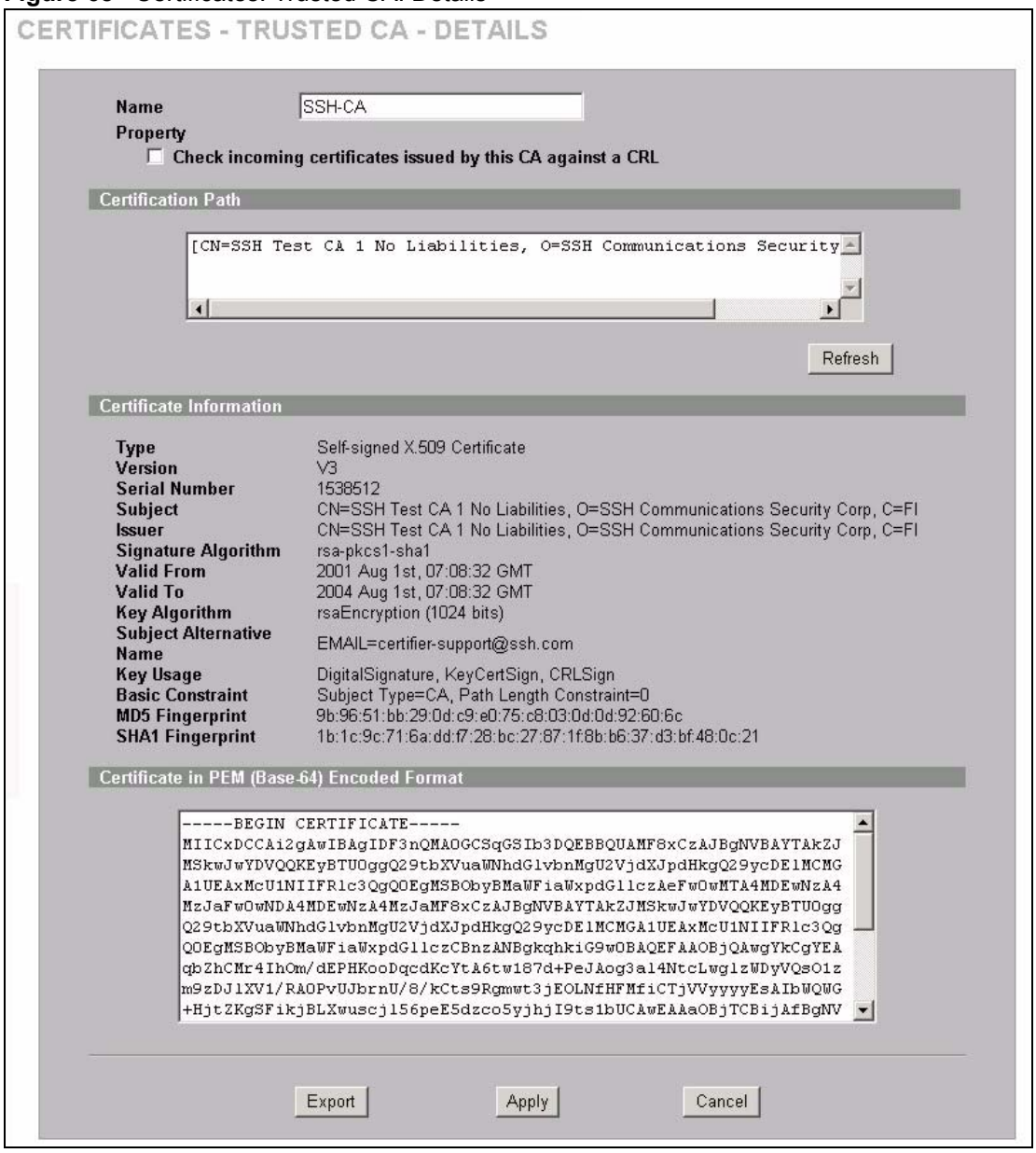
Table 55 Certificates: Trusted CA: Import

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.

10.11 Trusted CA Certificate Details

Click **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 68 Certificates: Trusted CA: Details



The following table describes the labels in this screen.

Table 56 Certificates: Trusted CA: 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 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). 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 56 Certificates: Trusted CA: 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. 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 56 Certificates: Trusted CA: Details (continued)

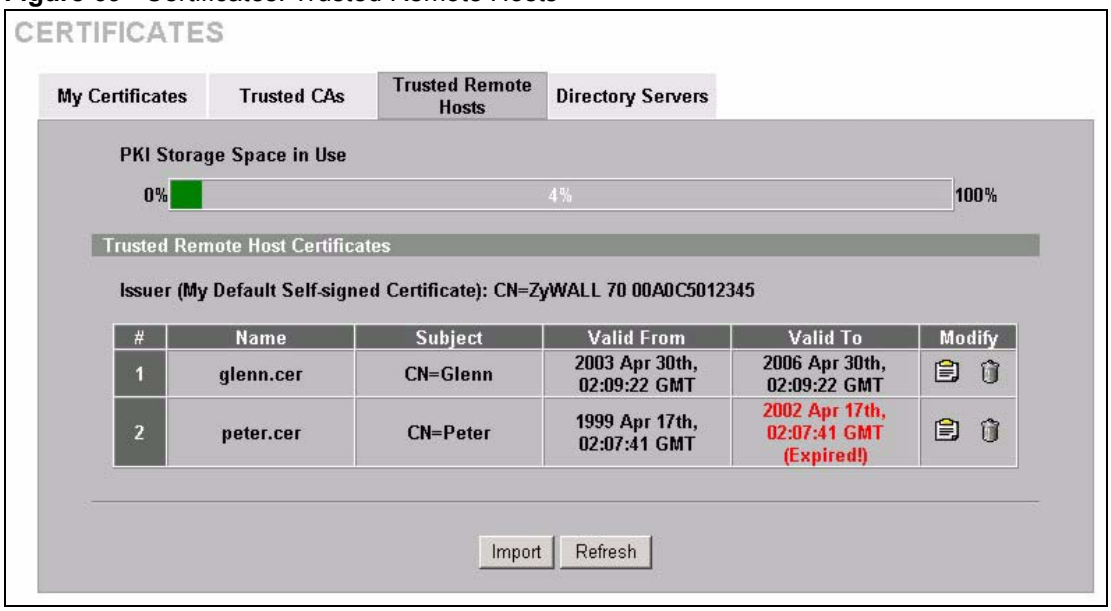
LABEL	DESCRIPTION
CRL Distribution Points	This field displays how many directory servers with Lists of revoked certificates the issuing certification authority of this certificate makes available. This field also displays the domain names or IP addresses of the servers.
MD5 Fingerprint	This is the certificate's 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. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Export	Click this button and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.
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.

10.12 Trusted Remote Hosts

Click **CERTIFICATES**, **Trusted Remote Hosts** to open the **Trusted Remote Hosts** screen (see the following figure). 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 69 Certificates: Trusted Remote Hosts



The following table describes the labels in this screen.

Table 57 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 you are using 80% or less of the storage space, the bar is green. When the amount of space used is over 80%, the bar is red. When the bar is red, 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.

Table 57 Certificates: Trusted Remote Hosts (continued)

LABEL	DESCRIPTION
Modify	Click the details icon to open a screen with an in-depth list of information about the certificate. Click the delete icon to remove the certificate. A window displays asking you to confirm that you want to delete the certificate. **Note:** 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.

10.13 Verifying a Trusted Remote Host's Certificate

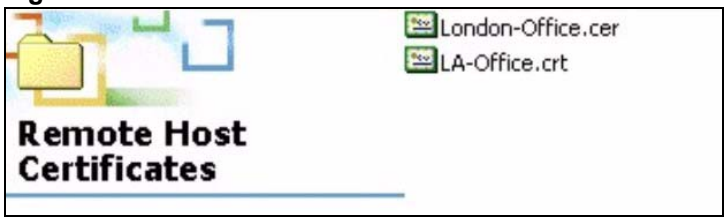
Certificates issued by certification authorities have the certification authority's signature for you to check. Self-signed certificates only have the signature of the host itself. This means that you must be very careful when deciding to import (and thereby trust) a remote host's self-signed certificate.

10.13.1 Trusted Remote Host Certificate Fingerprints

A certificate's fingerprints are message digests calculated using the MD5 or SHA1 algorithms. The following procedure describes how to use a certificate's fingerprint to verify that you have the remote host's actual certificate.

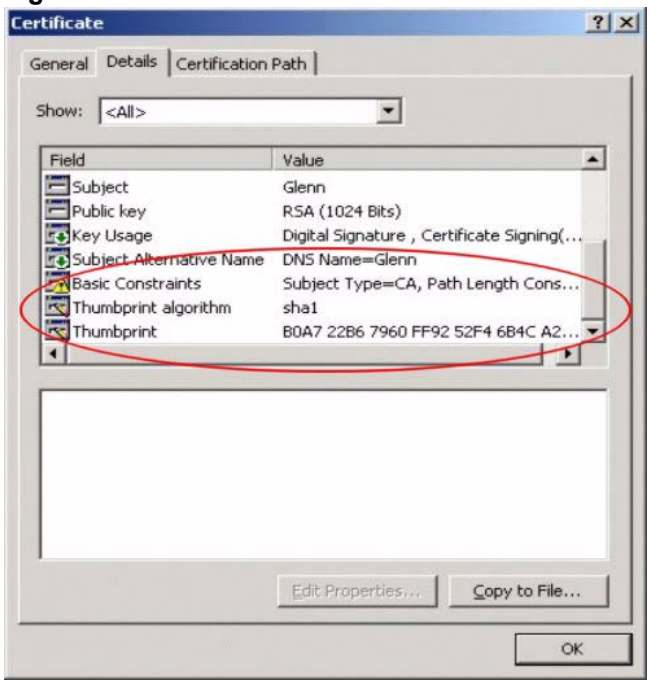
1. Browse to where you have the remote host's certificate saved on your computer.
2. Make sure that the certificate has a ".cer" or ".crt" file name extension.

Figure 70 Remote Host Certificates



3. Double-click the certificate's icon to open the **Certificate** window. Click the **Details** tab and scroll down to the **Thumbprint Algorithm** and **Thumbprint** fields.

Figure 71 Certificate Details



Verify (over the phone for example) that the remote host has the same information in the **Thumbprint Algorithm** and **Thumbprint** fields.

10.14 Importing a Trusted Remote Host's Certificate

Click **CERTIFICATES**, **Trusted Remote Hosts** to open the **Trusted Remote Hosts** screen and then click **Import** to open the **Trusted Remote Host Import** screen. Follow the instructions in this screen to save a trusted host's certificate to the ZyWALL, see the following figure.

Note: 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 72 Certificates: Trusted Remote Host: Import

The following table describes the labels in this screen.

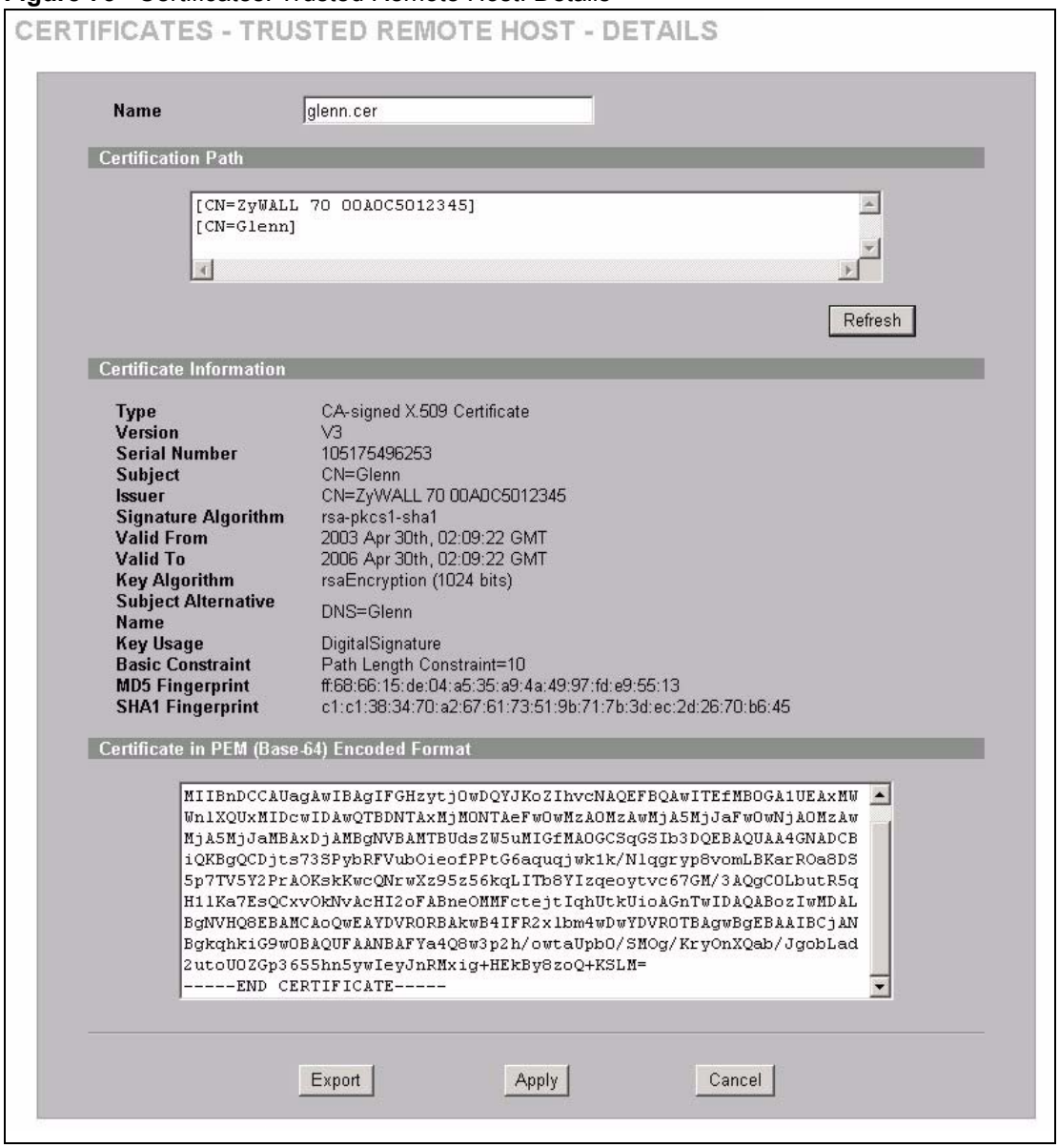
Table 58 Certificates: Trusted Remote Host: Import

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.

10.15 Trusted Remote Host Certificate Details

Click **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 73 Certificates: Trusted Remote Host: Details



The following table describes the labels in this screen.

Table 59 Certificates: Trusted Remote Host: 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.

Table 59 Certificates: Trusted Remote Host: Details (continued)

LABEL	DESCRIPTION
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.
MD5 Fingerprint	This is the certificate's message digest that the ZyWALL calculated using the MD5 algorithm. You cannot use this value to verify that this is the remote host's actual certificate because the ZyWALL has signed the certificate; thus causing this value to be different from that of the remote hosts actual certificate. See Section 10.13 on page 169 for how to verify a remote host's certificate.
SHA1 Fingerprint	This is the certificate's message digest that the ZyWALL calculated using the SHA1 algorithm. You cannot use this value to verify that this is the remote host's actual certificate because the ZyWALL has signed the certificate; thus causing this value to be different from that of the remote hosts actual certificate. See Section 10.13 on page 169 for how to verify a remote host's certificate.

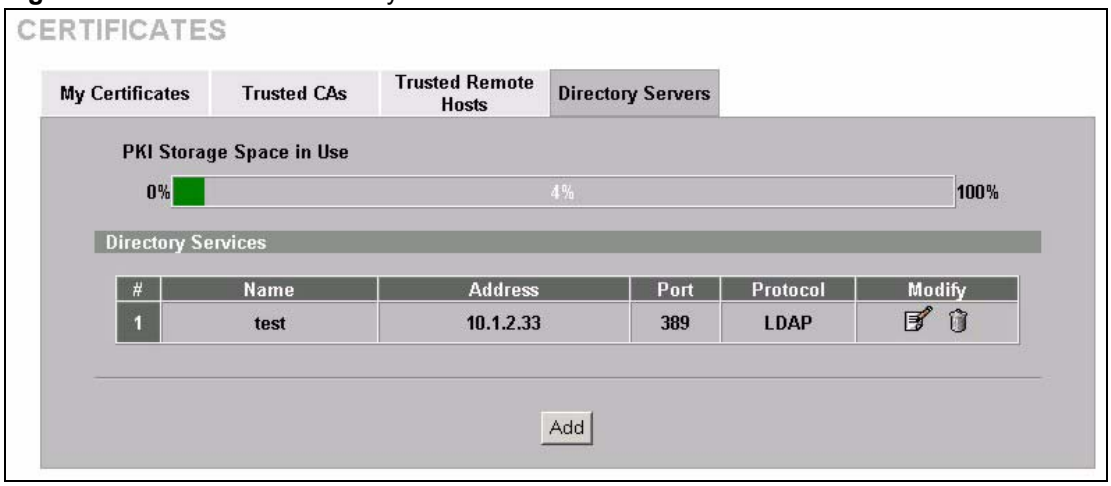
Table 59 Certificates: Trusted Remote Host: Details (continued)

LABEL	DESCRIPTION
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. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Export	Click this button and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.
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.

10.16 Directory Servers

Click **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 74 Certificates: Directory Servers



The following table describes the labels in this screen.

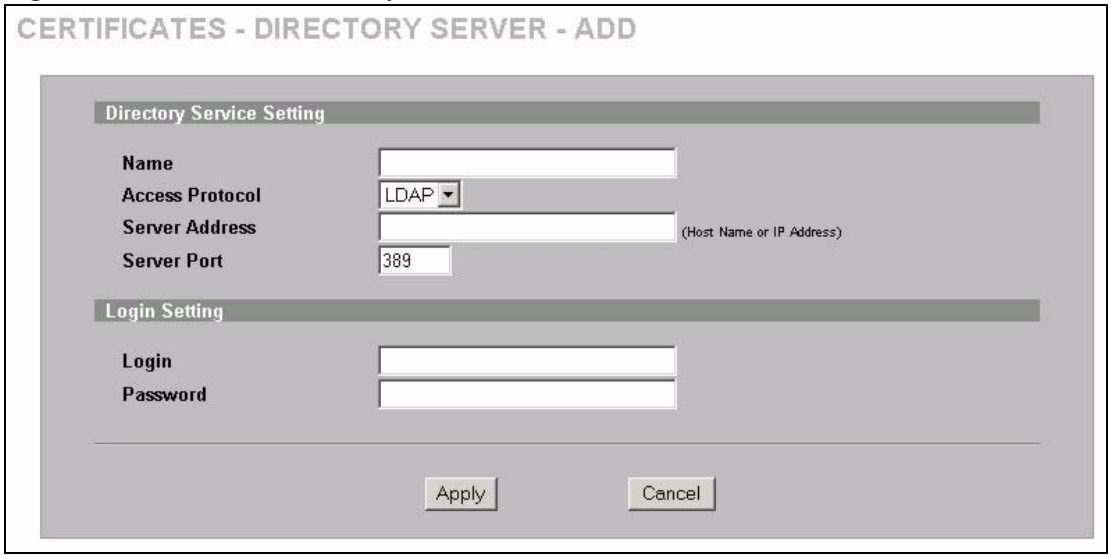
Table 60 Certificates: Directory Servers

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 you are using 80% or less of the storage space, the bar is green. When the amount of space used is over 80%, the bar is red. When the bar is red, 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. 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.

10.17 Add or Edit a Directory Server

Click **CERTIFICATES**, **Directory Servers** to open the **Directory Servers** screen. Click **Add** (or the details icon) to open the following screen. Use this screen to configure information about a directory server that the ZyWALL can access.

Figure 75 Certificates: Directory Server: Add



The following table describes the labels in this screen.

Table 61 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. **LDAP** (Lightweight Directory Access Protocol) is a protocol over TCP that specifies how clients access directories 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. You may change the server port number if needed, however you must use the same server port number that the directory server uses. 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.

CHAPTER 11
Network Address Translation (NAT)

This chapter discusses how to configure NAT on the ZyWALL.

11.1 NAT 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.

11.1.1 NAT Definitions

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. The following table summarizes this information.

Table 62 NAT Definitions

TERM	DESCRIPTION
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Global	This refers to the packet address (source or destination) as the packet travels on the WAN.

Note: NAT never changes the IP address (either local or global) of an outside host.

11.1.2 What NAT Does

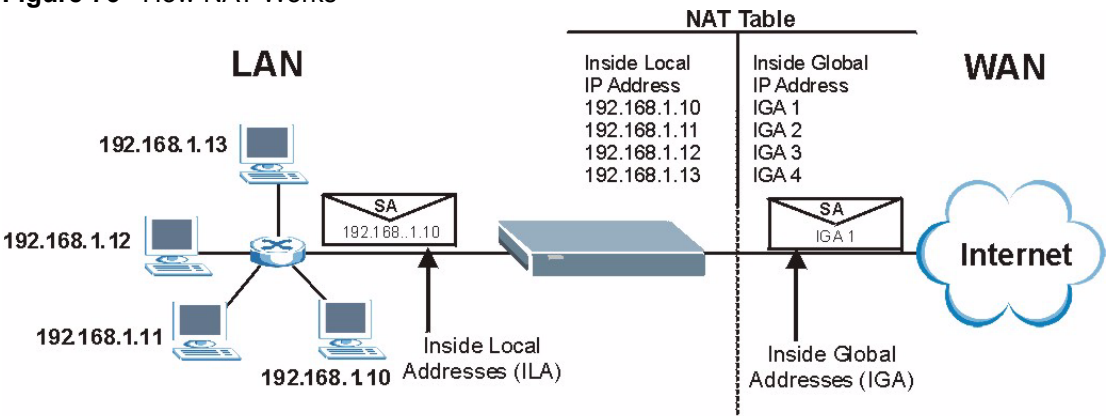
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) 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. If you do not define any servers, 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)*.

11.1.3 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. The following figure illustrates this.

Figure 76 How NAT Works



11.1.4 NAT Mapping Types

NAT supports five types of IP/port mapping. They are:

- **One to One**: In One-to-One mode, one local IP address is mapped 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), ZyWALL's Single User Account feature.
- **Many to Many Overload**: In Many-to-Many Overload mode, multiple local IP addresses are mapped to shared global IP addresses.
- **Many One to One**: In Many-One-to-One mode, each local IP address is mapped 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.

Note: Port numbers do **not** change for One-to-One and Many-One-to-One NAT mapping types.

The following table summarizes these types.

Table 63 NAT Mapping Types

TYPE	IP MAPPING	ABBREVIATION
One-to-One	ILA1←→ IGA1	1-1
Many-to-One (SUA/PAT)	ILA1←→ IGA1 ILA2←→ IGA1 …	M-1
Many-to-Many Overload	ILA1←→ IGA1 ILA2←→ IGA2 ILA3←→ IGA1 ILA4←→ IGA2 …	M-M Ov
Many-One-to-One	ILA1←→ IGA1 ILA2←→ IGA2 ILA3←→ IGA3 …	M-1-1
Server	Server 1 IP←→ IGA1 Server 2 IP←→ IGA1 Server 3 IP←→ IGA1	Server

11.2 Using NAT

Note: You must create a firewall rule in addition to setting up NAT, to allow traffic from the WAN to be forwarded through the ZyWALL.

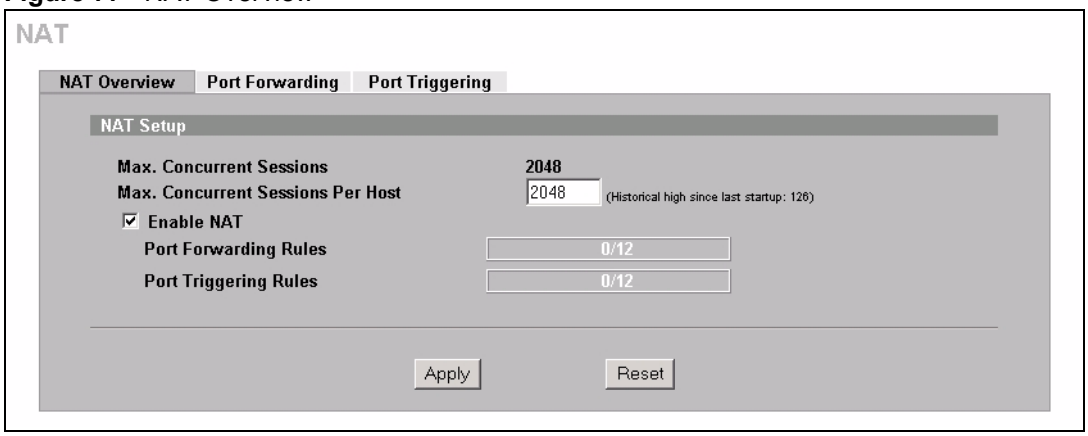
11.2.1 SUA (Single User Account) Versus NAT

Your ZyWALL supports SUA (Single User Account) which is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**.

11.3 Configuring NAT Overview

Click **NAT** to open the **NAT Overview** screen shown next.

Figure 77 NAT Overview



The following table describes the labels in this screen.

Table 64 NAT Overview

LABEL	DESCRIPTION
NAT Setup	
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.
Enable NAT	Select this check box to turn on the NAT feature for the WAN port. Clear this check box to turn off the NAT feature for the WAN port. **Note:** Your ZyWALL supports SUA which is a subset of NAT that supports two types of mapping, Many-to-One and Server (refer to Section 11.1.4 on page 178 for more information).
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.

Table 64 NAT Overview (continued)

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

11.4 Port Forwarding

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.

11.4.1 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.

Note: 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.

11.4.2 Port Forwarding: Services and Port Numbers

The ZyWALL provides the additional safety for connecting your publicly accessible 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 following table. Please refer to RFC 1700 for further information about port numbers. Please also refer to the Supporting CD for more examples and details on port forwarding and NAT.

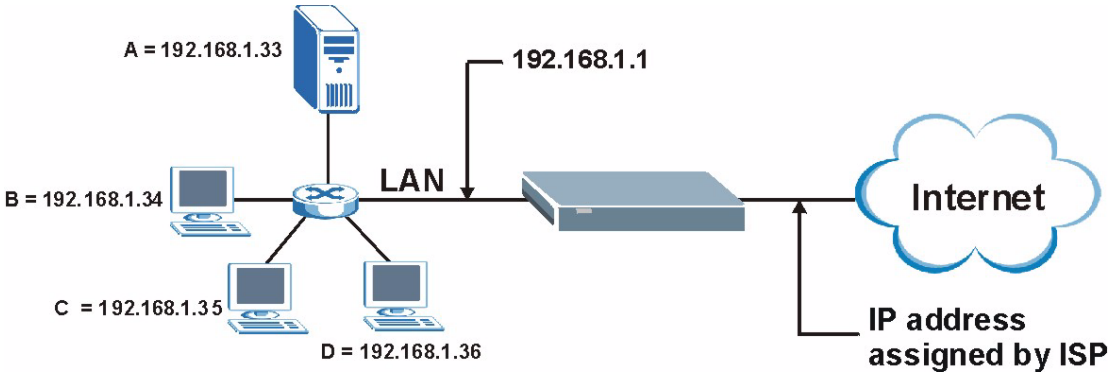
Table 65 Services and Port Numbers

SERVICES	PORT NUMBER
ECHO	7
FTP (File Transfer Protocol)	21
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)	161
SNMP trap	162
PPTP (Point-to-Point Tunneling Protocol)	1723

11.4.3 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 78 Multiple Servers Behind NAT Example



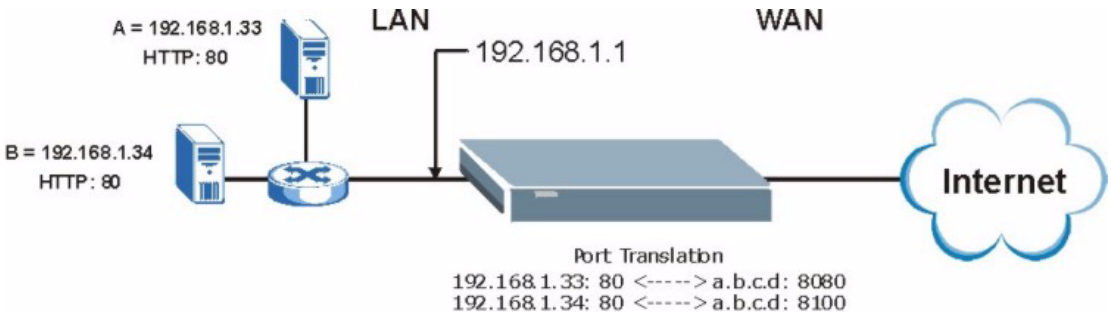
11.4.4 Port Translation

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 LAN. When you use port forwarding without port translation, a single server on the LAN 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 LAN 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).

Note: 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 79 Port Translation Example



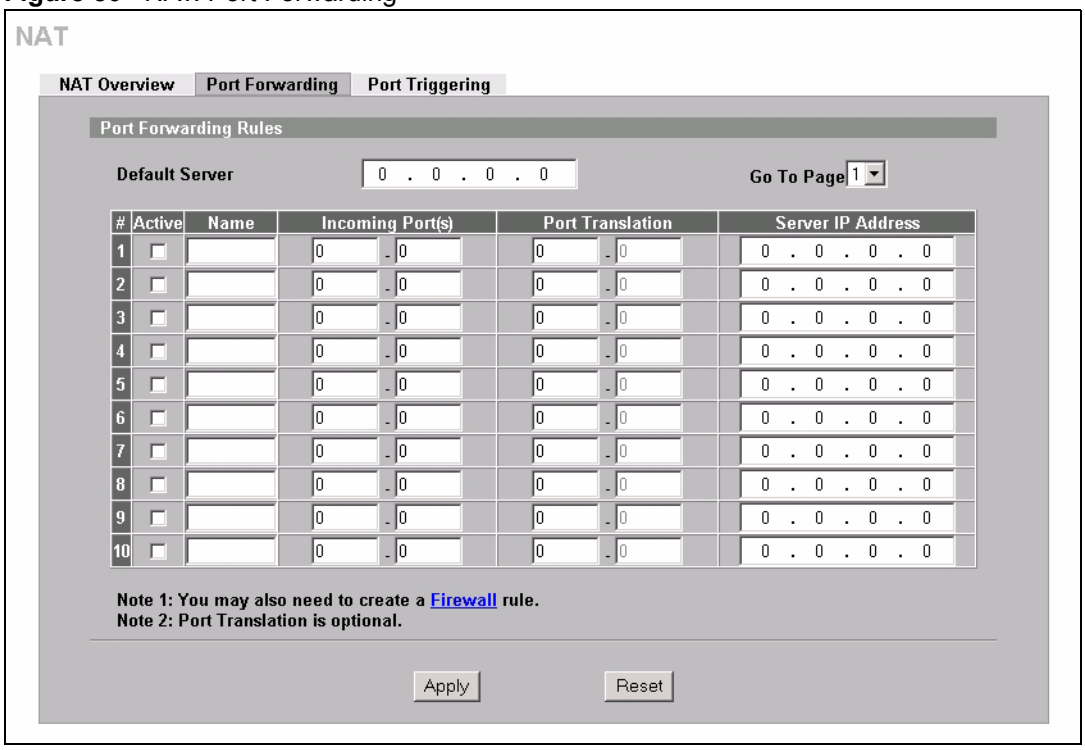
11.5 Configuring Port Forwarding

Note: 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.

Click **NAT** and **Port Forwarding** to open the **Port Forwarding** screen.

Refer to Figure 65 on page 182 for port numbers commonly used for particular services.

Figure 80 NAT: Port Forwarding



The following table describes the labels in this screen.

Table 66 NAT: 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, 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.
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.

Table 66 NAT: Port Forwarding (continued)

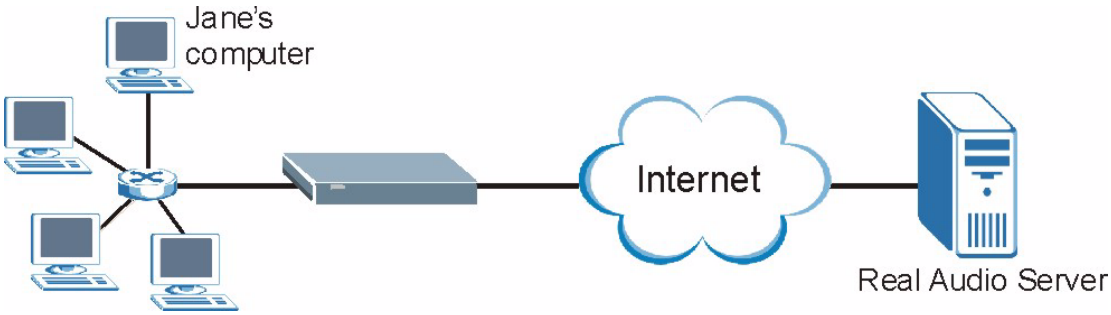
LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

11.6 Configuring Trigger Port

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:

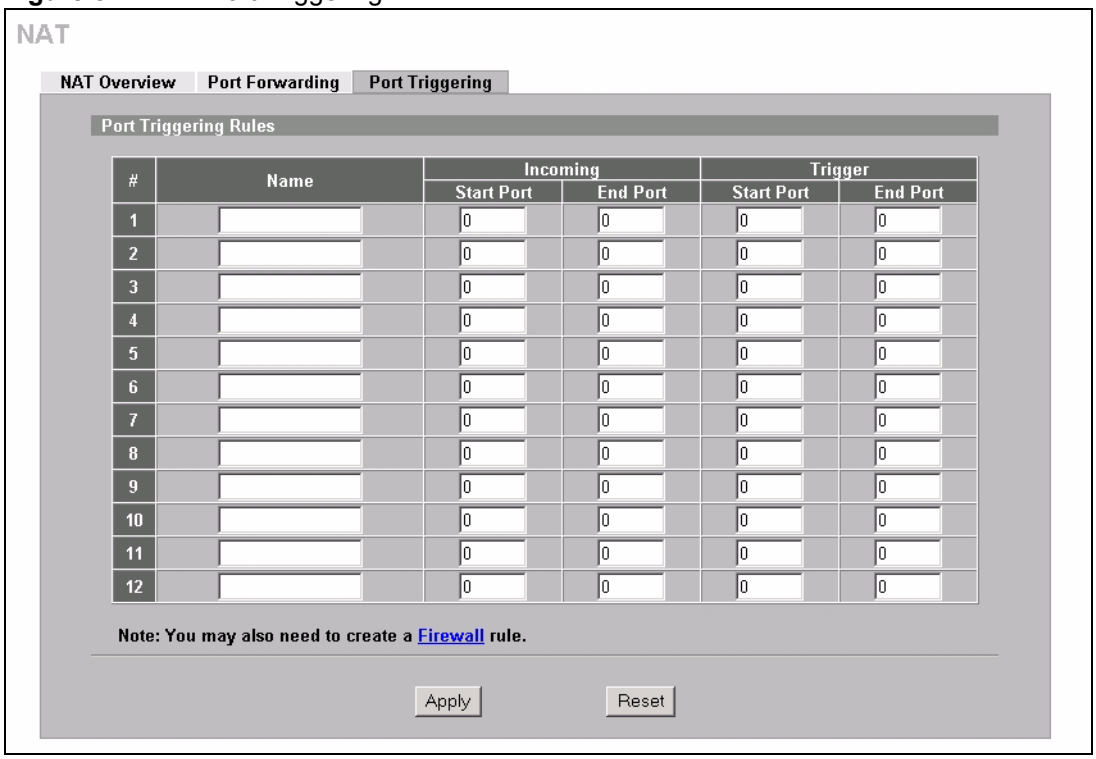
Figure 81 Trigger Port Forwarding Process: Example



1. Jane 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).

To change your ZyWALL's trigger port settings, click **NAT** and the **Port Triggering** tab. The screen appears as shown.

Figure 82 NAT: Port Triggering



The following table describes the labels in this screen.

Table 67 NAT: Port Triggering

LABEL	DESCRIPTION
#	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.
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.

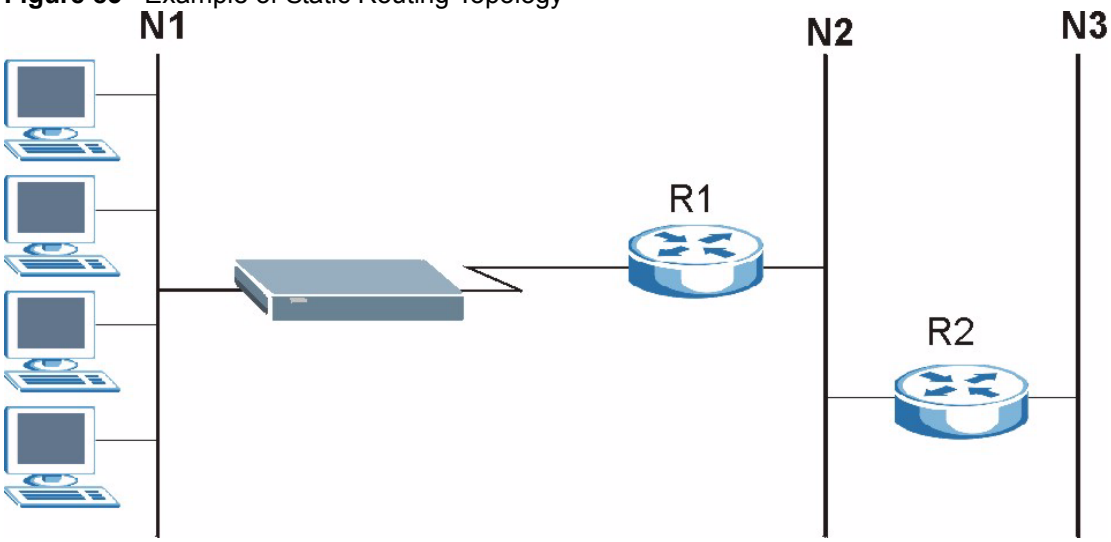
CHAPTER 12
Static Route

This chapter shows you how to configure static routes for your ZyWALL.

12.1 Static Route Overview

Each remote node specifies only the network to which the gateway is directly connected, and the ZyWALL has no knowledge of the networks beyond. For instance, the ZyWALL knows about network N2 in the following figure through remote node Router 1. However, the ZyWALL is unable to route a packet to network N3 because it doesn't know that there is a route through the same remote node Router 1 (via gateway Router 2). The static routes are for you to tell the ZyWALL about the networks beyond the remote nodes.

Figure 83 Example of Static Routing Topology



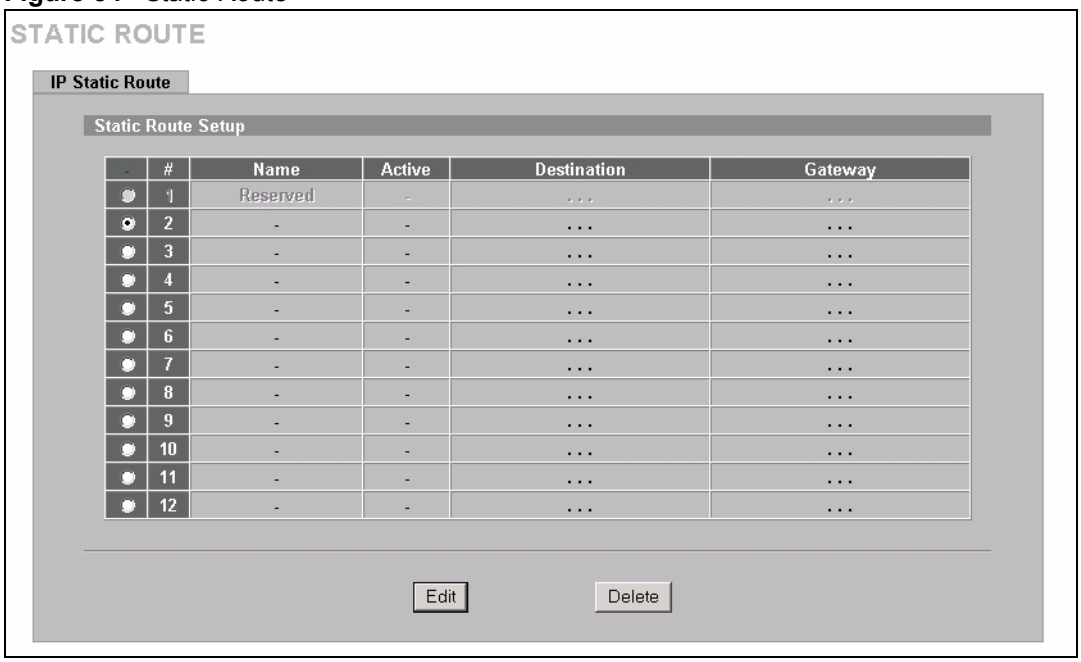
12.2 Configuring IP Static Route

Click **STATIC ROUTE** to open the **IP Static Route** screen (some of the screen's blank rows are not shown).

Note: The first static route entry is for default WAN route and cannot be modified or deleted. The name of the default static route is left blank unless you configure a static WAN IP address.

The default route is disabled after you change the static WAN IP address to a dynamic WAN IP address.

Figure 84 Static Route



-	#	Name	Active	Destination	Gateway
	1	Reserved	-	...	...
	2	-	-	...	...
	3	-	-	...	...
	4	-	-	...	...
	5	-	-	...	...
	6	-	-	...	...
	7	-	-	...	...
	8	-	-	...	...
	9	-	-	...	...
	10	-	-	...	...
	11	-	-	...	...
	12	-	-	...	...

The following table describes the labels in this screen.

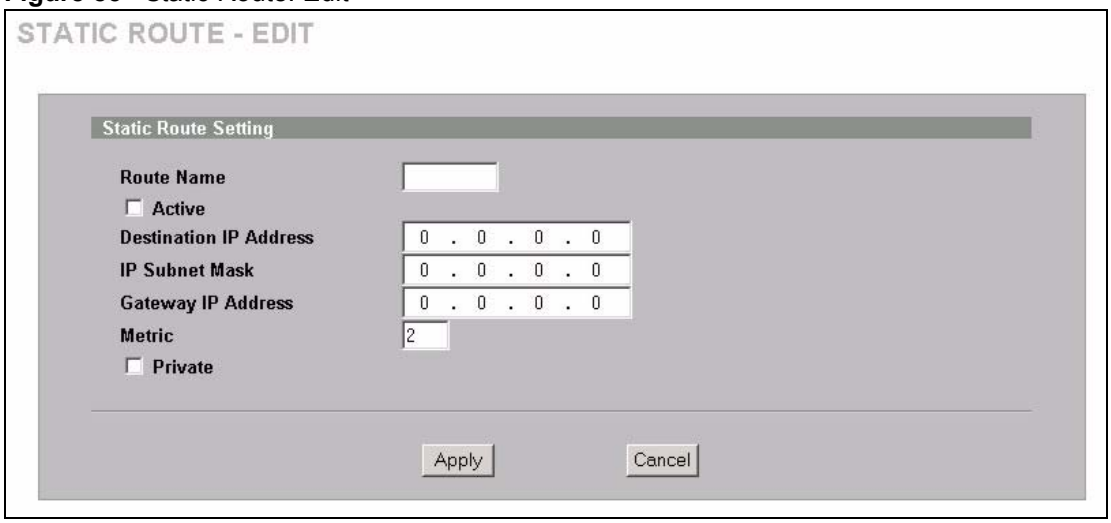
Table 68 Static Route

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.
Gateway	This is 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.
Edit	Select the radio button next to a static route index number and then click **Edit** to set up a static route on the ZyWALL.
Delete	Select the radio button next to a static route index number and then click **Delete** to remove a static route on the ZyWALL.

12.2.1 Configuring a Static Route Entry

Select a static route index number and click **Edit**. The screen shown next appears. Fill in the required information for each static route.

Figure 85 Static Route: Edit



The following table describes the labels in this screen.

Table 69 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.
Private	This parameter determines if the ZyWALL will include this route to a remote node in its RIP broadcasts. Select this check box to keep this route private and not included in RIP broadcasts. Clear this checkbox 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.

CHAPTER 13
Remote Management

This chapter provides information on the Remote Management screens.

13.1 Remote Management Overview

Remote management allows you to determine which services/protocols can access which ZyWALL interface (if any) from which computers.

Note: When you configure remote management to allow management from the WAN, you still need to configure a firewall rule to allow access. See Chapter 7 on page 103 for details on configuring firewall rules.

You may manage your ZyWALL from a remote location via:

- Internet (WAN only)
- LAN only,
- Neither (Disable).
- ALL (LAN&WAN)

Note: When you choose **WAN only** or **LAN & WAN**, you still need to configure a firewall rule to allow access.

To disable remote management of a service, select **Disable** in the corresponding **Server Access** field.

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. SSH
2. Telnet
3. HTTPS and HTTP

13.1.1 Remote Management Limitations

1. Remote management over LAN or WAN will not work when:
2. A filter is applied to block a Telnet, FTP or Web service.
3. You have disabled that service in one of the remote management screens.

4 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.

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.

13.1.2 Remote Management and NAT

When NAT is enabled:

- Use the ZyWALL's WAN IP address when configuring from the WAN.
- Use the ZyWALL's LAN IP address when configuring from the LAN.

13.1.3 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 **System** screen.

13.2 Introduction to HTTPS

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 10 on page 151 for more information).

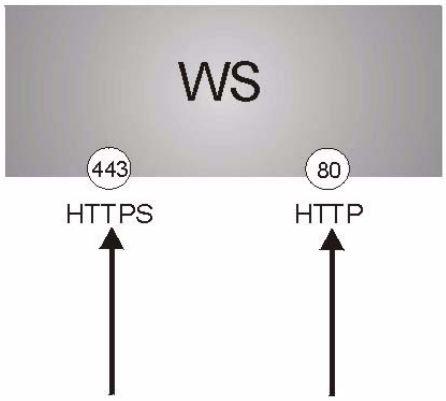
HTTPS on the ZyWALL is used so that you may securely access the ZyWALL using the web configurator. The SSL protocol specifies that the SSL server (the ZyWALL) must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the ZyWALL), whereas the SSL client only 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 86 HTTPS Implementation

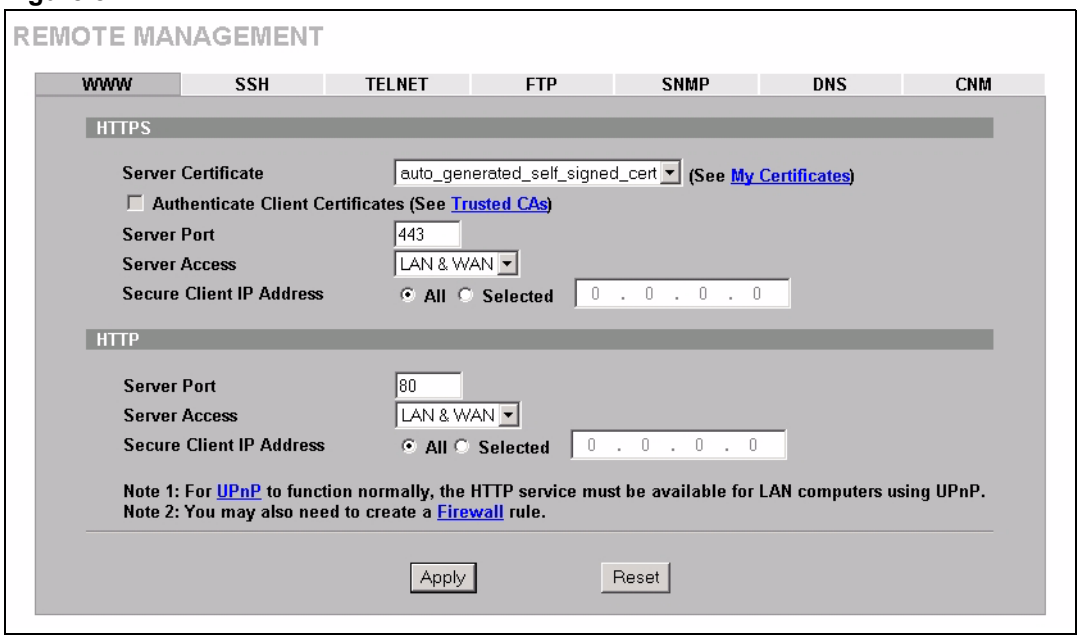


Note: If you disable **HTTP Server Access** (**Disable**) in the **REMOTE MGMT WWW** screen, then the ZyWALL blocks all HTTP connection attempts.

13.3 Configuring WWW

To change your ZyWALL's web settings, click **REMOTE MGMT** to open the **WWW** screen.

Figure 87 WWW



The following table describes the labels in this screen.

Table 70 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 Appendix H on page 317 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 a ZyWALL interface from **Server Access** on which incoming HTTPS access is allowed. You can allow only secure web configurator access by setting the **HTTP Server Access** field to **Disable** 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. Select **All** to allow any computer to access the ZyWALL using this service. 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.
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. Select **All** to allow any computer to access the ZyWALL using this service. 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.

13.4 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.

13.4.1 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 88 Security Alert Dialog Box (Internet Explorer)

13.4.2 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 ZZyWALL's certificate into the SSL client.

Figure 89 Security Certificate 1 (Netscape)

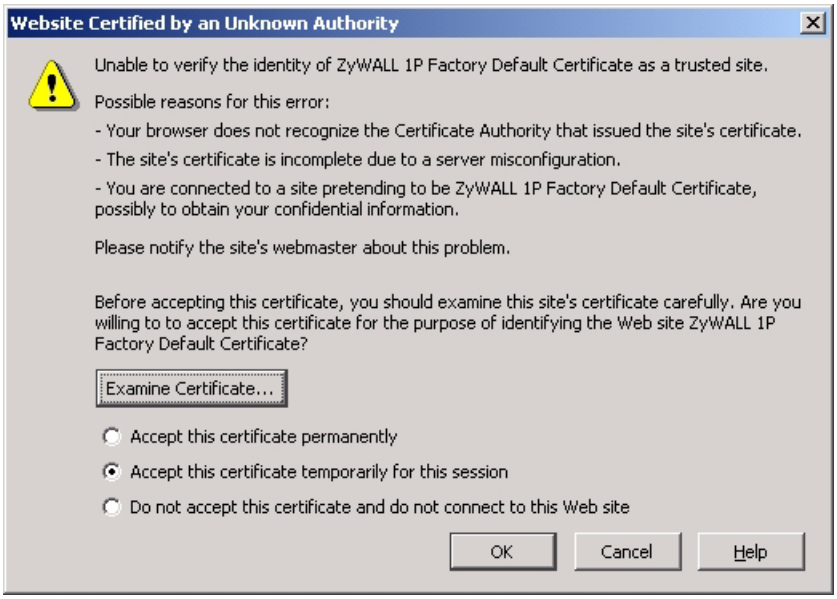


Figure 90 Security Certificate 2 (Netscape)

13.4.3 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 H on page 317 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.

  a Click **REMOTE MGMT**. Write down the name of the certificate displayed in the **Server Certificate** field.

  b Click **CERTIFICATES**. Find the certificate and check its **Subject** column. **CN** stands for certificate's common name (Figure 94 on page 199 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.

a 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 192.168.167.1, create a certificate that uses 192.168.167.1 as the common name.

b Go to the remote management **WWW** screen and select the newly created certificate in the **Server Certificate** field. Click **Apply**.

13.4.4 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 91 Login Screen (Internet Explorer)

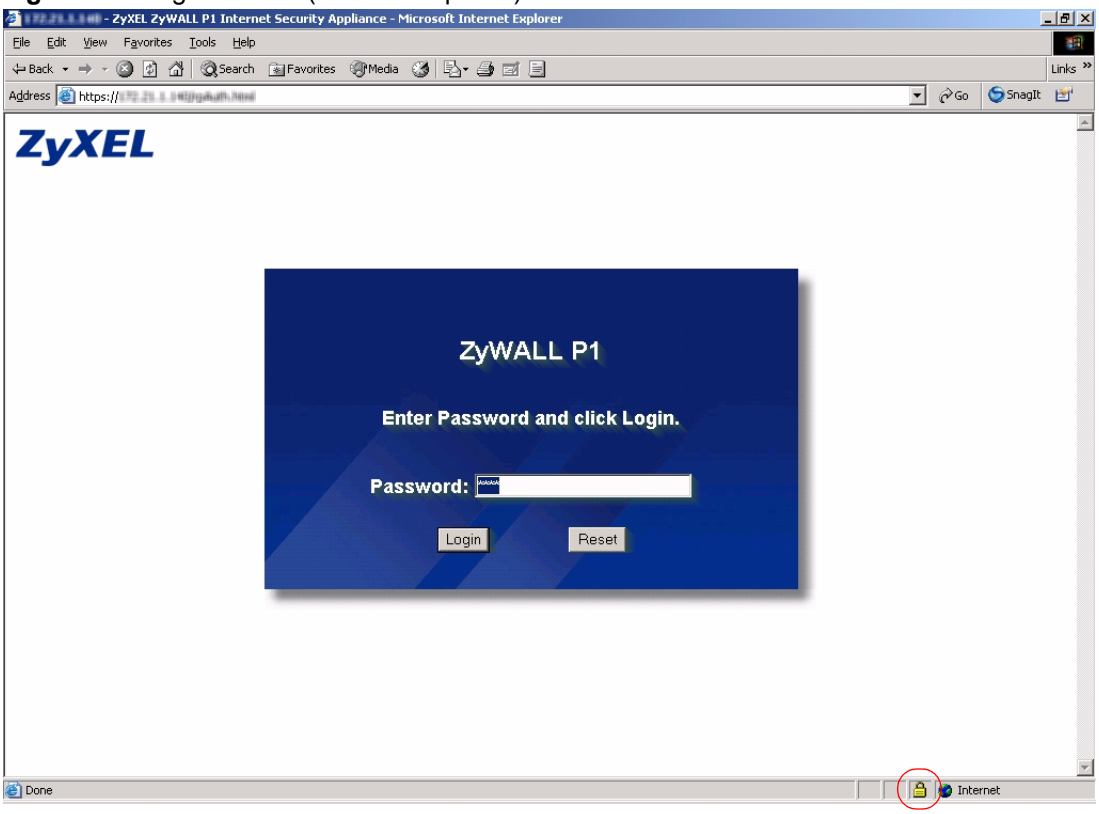
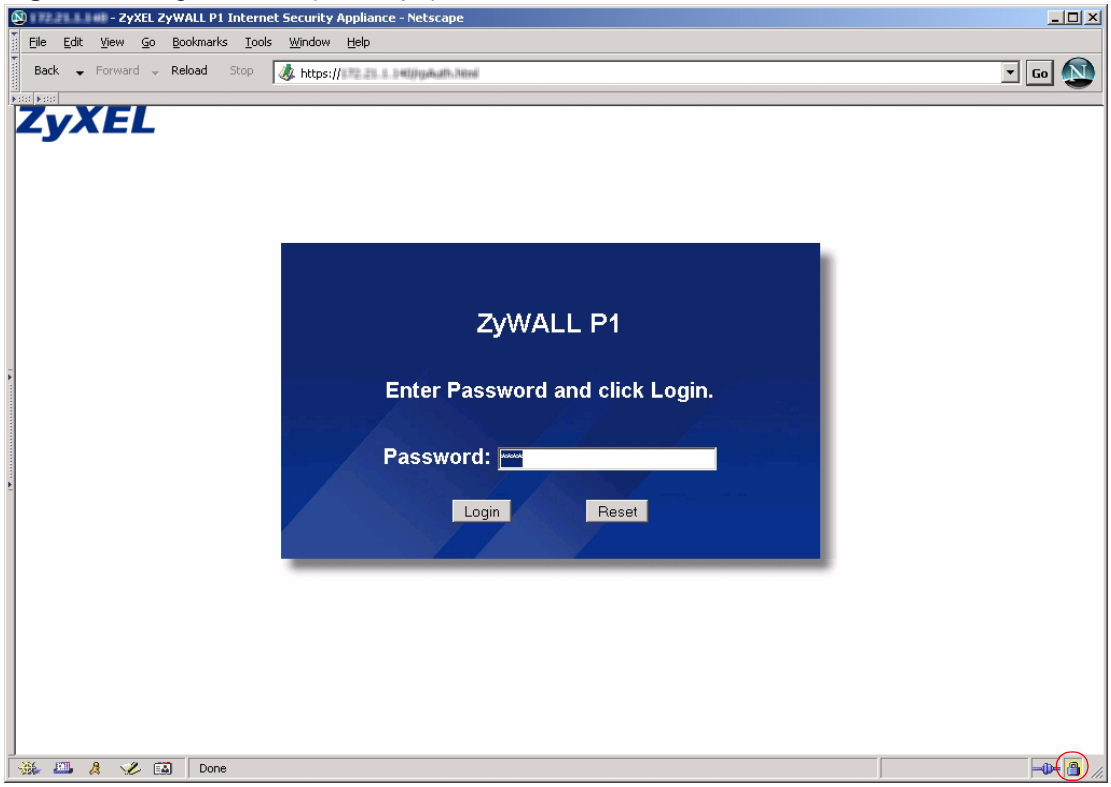


Figure 92 Login Screen (Netscape)



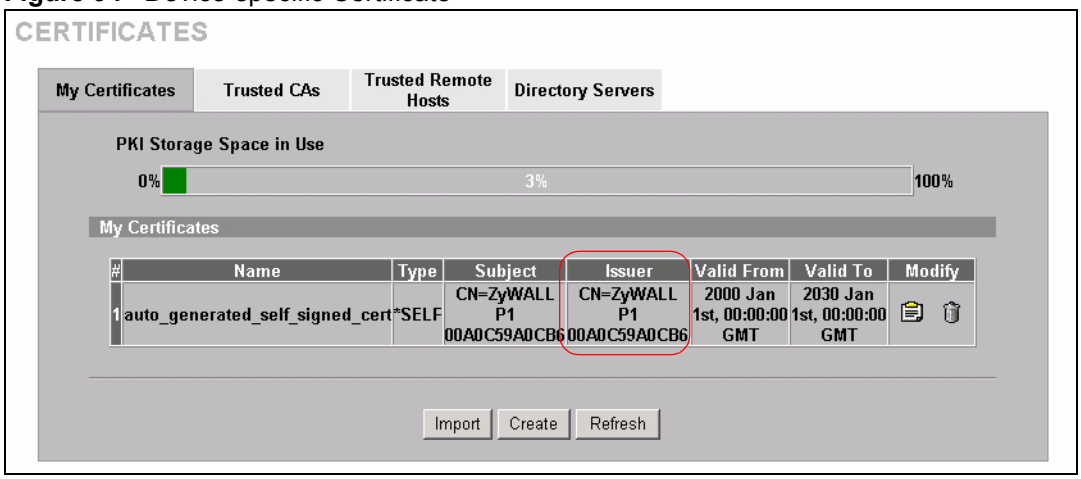
Click **Login** and you then see the next screen.

The factory default certificate is a common default certificate.

Figure 93 Replace Certificate

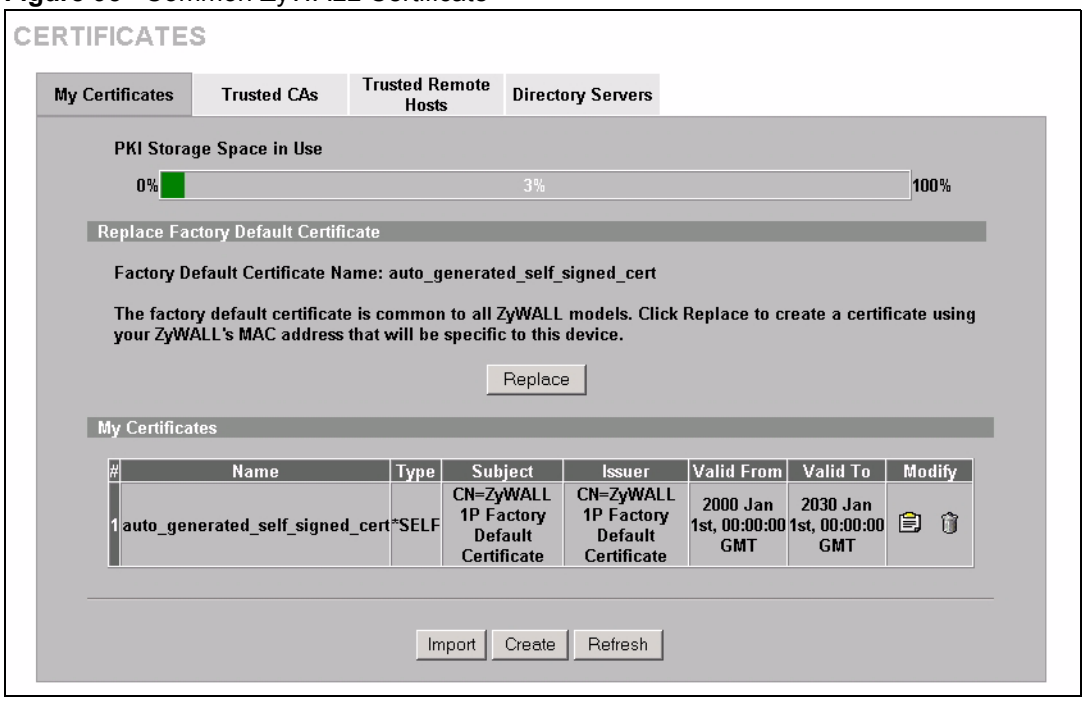
Click **Apply** in the **Replace Certificate** screen to create a certificate using your ZyWALL's MAC address that will be specific to this device. Click **CERTIFICATES** to open the **My Certificates** screen. You will see information similar to that shown in the following figure.

Figure 94 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 95 Common ZyWALL Certificate



13.5 SSH Overview

Unlike Telnet or FTP, which transmit data in clear text, SSH (Secure Shell) is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication

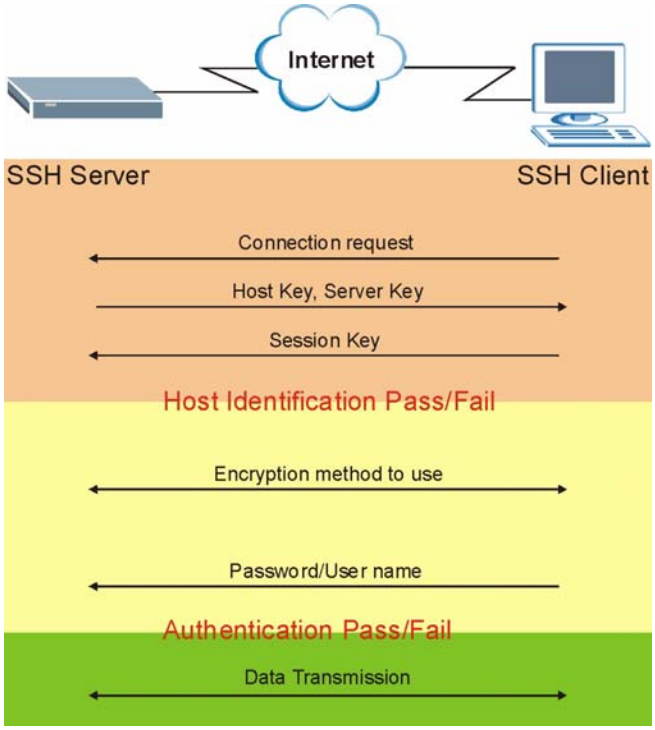
between two hosts over an unsecured network.

Figure 96 SSH Communication Example

13.6 How SSH works

The following table summarizes how a secure connection is established between two remote hosts.

Figure 97 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.

13.7 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 management and file transfer on port 22. Only one SSH connection is allowed at a time.

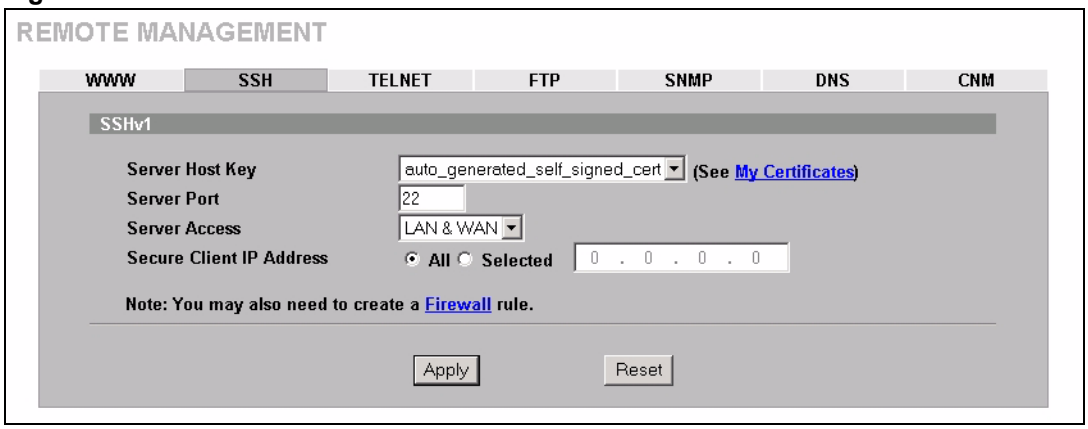
13.7.1 Requirements for Using SSH

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.

13.8 Configuring SSH

To change your ZyWALL's Secure Shell settings, click **REMOTE MGMT**, then the **SSH** tab. The screen appears as shown.

Figure 98 SSH



The following table describes the labels in this screen.

Table 71 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 refer to Chapter 10 on page 151 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. Select **All** to allow any computer to access the ZyWALL using this service. 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.

Note: It is recommended that you disable Telnet and FTP when you configure SSH for secure connections.

13.9 Secure Telnet Using SSH Examples

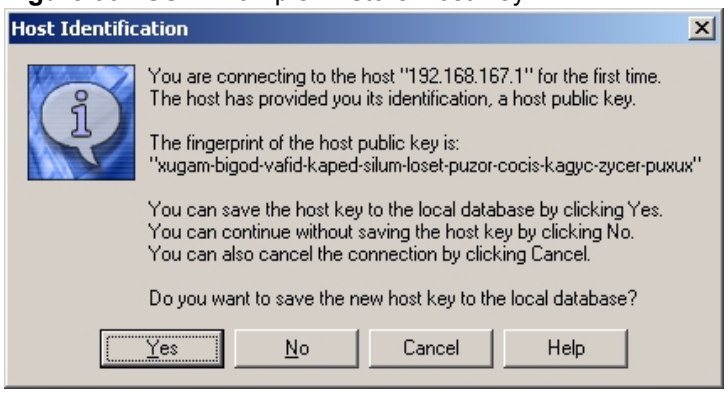
This section shows two examples using a command interface and a graphical interface SSH client program to remotely access the ZyWALL. The configuration and connection steps are similar for most SSH client programs. Refer to your SSH client program user's guide.

13.9.1 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 99 SSH Example 1: Store Host Key



Enter the password to log in to the ZyWALL. The CLI prompt displays next.

13.9.2 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 192.168.167.1 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 192.168.167.1).

   A message displays indicating the SSH protocol version supported by the ZyWALL.

Figure 100 SSH Example 2: Test

```
$ telnet 192.168.167.1 22
Trying 192.168.167.1...
Connected to 192.168.167.1.
Escape character is '^]'.
SSH-1.5-1.0.0
```

2 Enter `ssh -1 192.168.167.1`. 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 101 SSH Example 2: Log in

```
$ ssh -1 192.168.167.1
The authenticity of host '192.168.167.1 (192.168.167.1)' 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 '192.168.167.1' (RSA1) to the list
of known hosts.
Administrator@192.168.167.1's password:
```

3 The CLI prompt displays next.

13.10 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 -1 192.168.167.1`. 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.

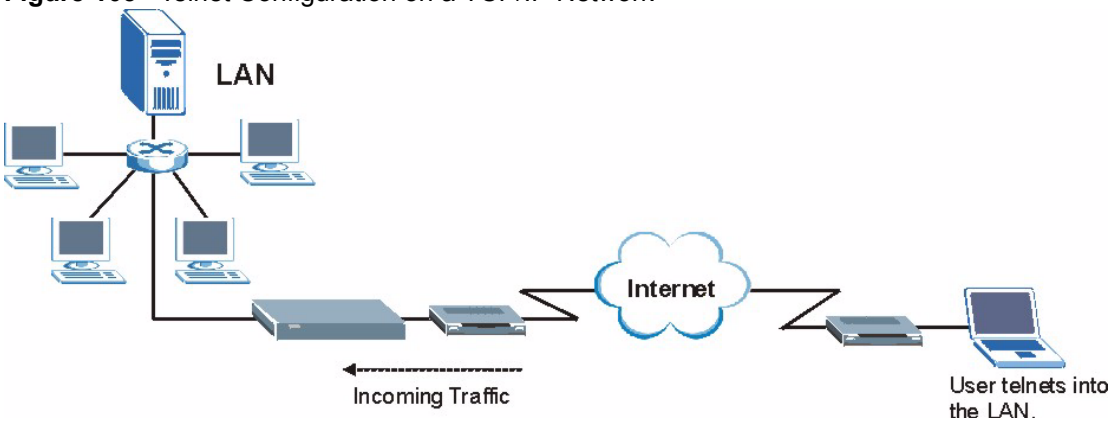
Figure 102 Secure FTP: Firmware Upload Example

```
$ sftp -1 192.168.167.1
Connecting to 192.168.167.1...
The authenticity of host '192.168.167.1 (192.168.167.1)' 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 '192.168.167.1' (RSA1) to the list
of known hosts.
Administrator@192.168.167.1's password:
sftp> put firmware.bin ras
Uploading firmware.bin to /ras
Read from remote host 192.168.167.1: Connection reset by peer
Connection closed
$
```

13.11 Telnet

You can configure your ZyWALL for remote Telnet access as shown next.

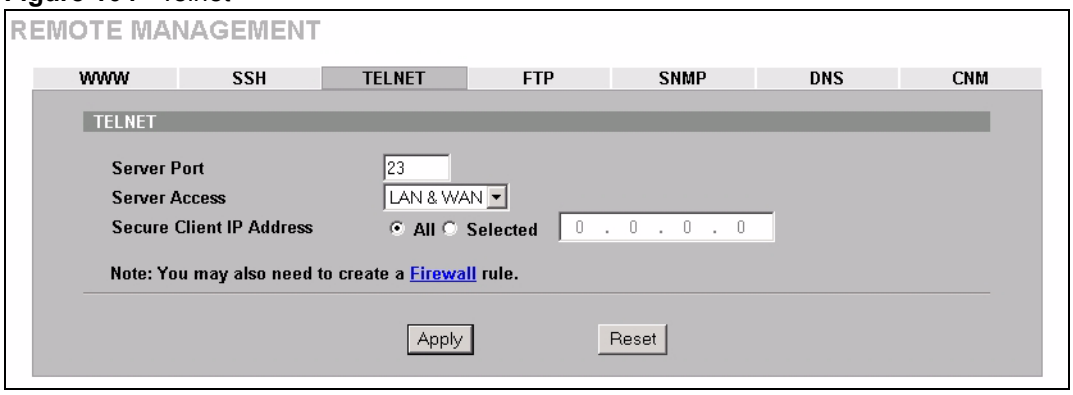
Figure 103 Telnet Configuration on a TCP/IP Network



13.12 Configuring TELNET

Click **REMOTE MGMT**, then the **TELNET** tab. The screen appears as shown.

Figure 104 Telnet



The following table describes the labels in this screen.

Table 72 Telnet

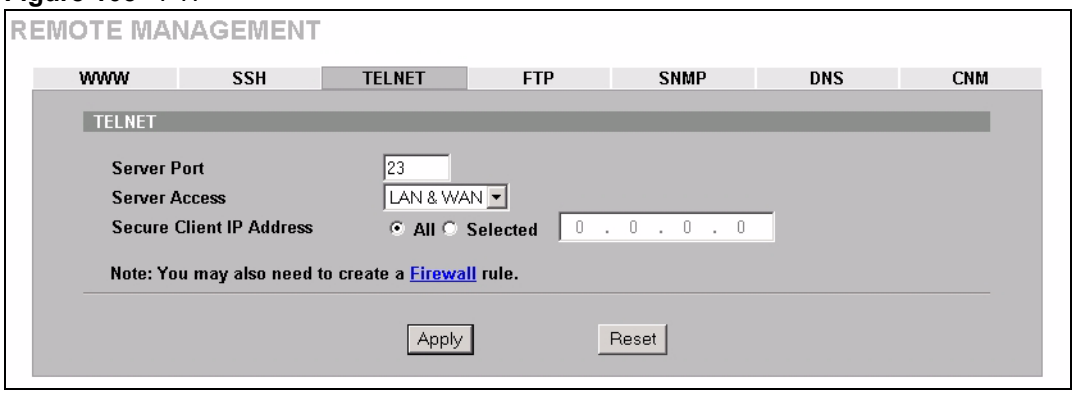
LABEL	DESCRIPTION
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the ZyWALL using this service.
Secure Client IP Address	A secure client is a "trusted" computer that is allowed to communicate with the ZyWALL using this service. Select **All** to allow any computer to access the ZyWALL using this service. 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.

13.13 Configuring FTP

You can upload and download the ZyWALL's firmware and configuration files using FTP, please see the chapter 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 **REMOTE MGMT**, then the **FTP** tab. The screen appears as shown.

Figure 105 FTP



The following table describes the labels in this screen.

Table 73 FTP

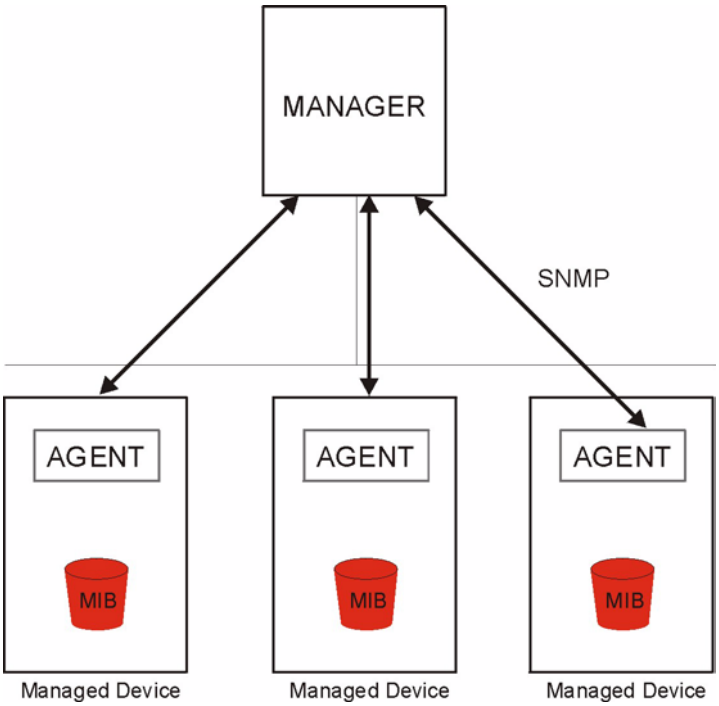
LABEL	DESCRIPTION
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the ZyWALL using this service.
Secure Client IP Address	A secure client is a "trusted" computer that is allowed to communicate with the ZyWALL using this service. Select **All** to allow any computer to access the ZyWALL using this service. 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.

13.14 Configuring SNMP

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.

Note: SNMP is only available if TCP/IP is configured.

Figure 106 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.

13.14.1 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.

13.14.2 SNMP Traps

The ZyWALL will send traps to the SNMP manager when any one of the following events occurs:

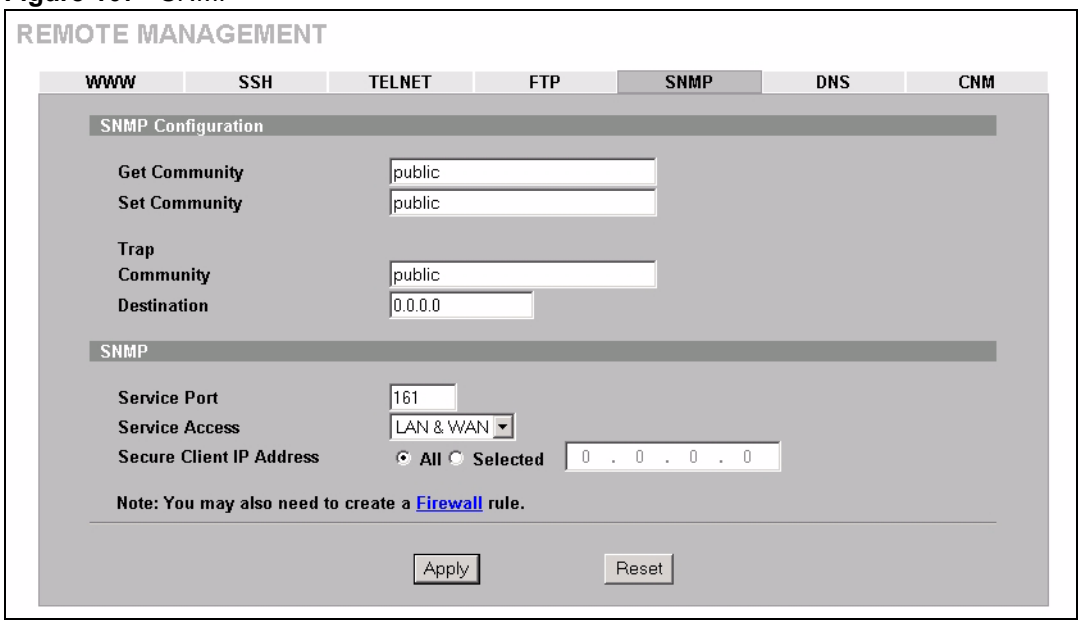
Table 74 SNMP Traps

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.

13.14.3 REMOTE MANAGEMENT: SNMP

To change your ZyWALL's SNMP settings, click **REMOTE MGMT**, then the **SNMP** tab. The screen appears as shown.

Figure 107 SNMP



The following table describes the labels in this screen.

Table 75 SNMP

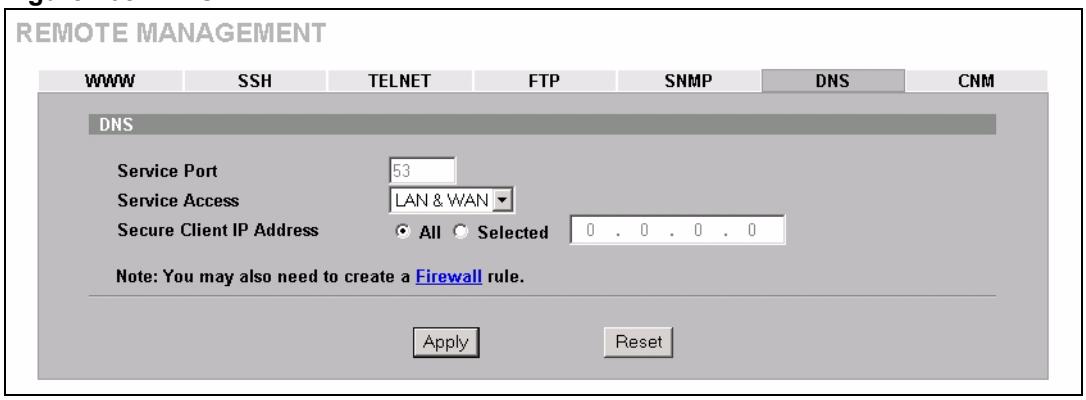
LABEL	DESCRIPTION
SNMP Configuration	
Get Community	Enter the **Get Community**, which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.
Set Community	Enter the **Set community**, which is the password for incoming Set 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. Select **All** to allow any computer to access the ZyWALL using this service. 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.

13.15 Configuring DNS

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa. Refer to Chapter 5 on page 79 for more information.

To change your ZyWALL's DNS settings, click **REMOTE MGMT**, then the **DNS** tab. The screen appears as shown. This feature is not available when the ZyWALL is set to bridge mode.

Figure 108 DNS



The following table describes the labels in this screen.

Table 76 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. Select **All** to allow any computer to send DNS queries to the ZyWALL. 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.

13.16 Introducing Vantage CNM

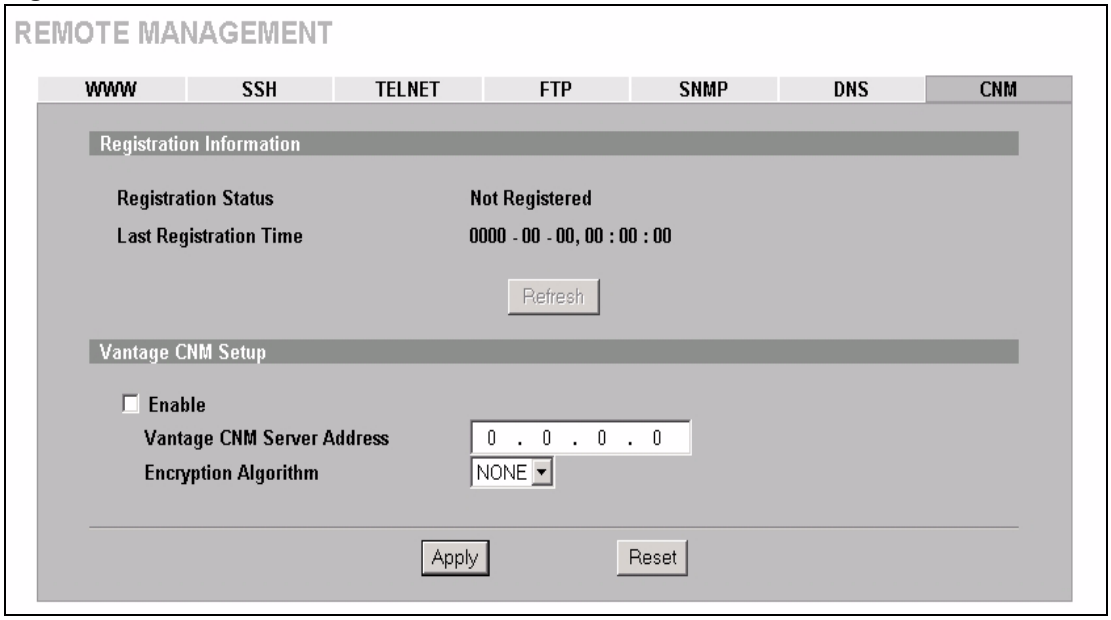
Vantage CNM (Centralized Network Management) is a browser-based global management solution that allows an administrator from any location to easily configure, manage, monitor and troubleshoot ZyWALL devices located worldwide. See the *Vantage CNM User's Guide* for details.

If you allow your ZyWALL to be managed by the Vantage CNM server, then you should not do any configurations directly to the ZyWALL (using either the web configurator or commands) without notifying the Vantage CNM administrator.

13.17 Configuring CNM

Vantage CNM is disabled on the ZyWALL by default. Click **REMOTE MGMT** in the navigation panel and then click the **CNM** tab.

Figure 109 CNM



The following table describes the labels in this screen.

Table 77 CNM

LABEL	DESCRIPTION
Registration Information	
Registration Status	This read only field displays **Not Registered** when **Enable** is not selected. 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. The ZyWALL will not be able to register with the Vantage CNM server if: • The Vantage CNM server is down. • The Vantage CNM server IP address is incorrect. • The Vantage CNM server is behind a NAT router or firewall that does not forward packets through to the Vantage CNM server. • The encryption algorithms and/or encryption keys do not match between the ZyWALL and the Vantage CNM server.

Table 77 CNM (continued)

LABEL	DESCRIPTION
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 checkbox 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. If the Vantage CNM server is on a different subnet to the ZyWALL, enter the public IP address of the Vantage server. If the Vantage CNM server is on a different subnet to the ZyWALL and is behind a NAT router, enter the WAN IP address of the NAT router here and configure the NAT router to forward UDP port 1864 traffic to the Vantage CNM server. If the Vantage CNM server is behind a firewall, you may have to create a rule on the firewall to allow UDP port 1864 traffic through to the Vantage CNM server (most (new) ZyXEL firewalls automatically allow this).
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.

CHAPTER 14
UPnP

This chapter introduces the Universal Plug and Play feature.

14.1 Universal Plug and Play Overview

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.

14.1.1 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.

14.1.2 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 11 on page 177 for further information about NAT.

14.1.3 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.

All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

14.2 UPnP and ZyXEL

ZyXEL has achieved UPnP certification from the Universal Plug and Play Forum Creates UPnP™ Implementers Corp. (UIC). ZyXEL's UPnP implementation supports IGD 1.0 (Internet Gateway Device). At the time of writing ZyXEL's UPnP implementation supports Windows Messenger 4.6 and 4.7 while Windows Messenger 5.0 and Xbox are still being tested.

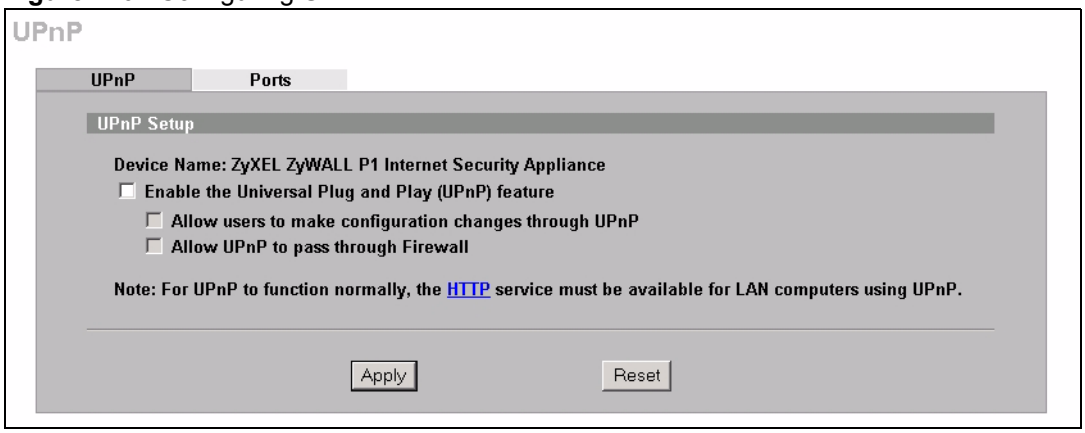
The ZyWALL only sends UPnP multicasts to the LAN.

Please see later in this *User's Guide* for examples of installing UPnP in Windows XP and Windows Me as well as an example of using UPnP in Windows.

14.3 Configuring UPnP

Click **UPnP** to display the screen shown next.

Figure 110 Configuring UPnP



The following table describes the fields in this screen.

Table 78 Configuring UPnP

LABEL	DESCRIPTION
UPnP Setup	
Device Name	This identifies the ZyWALL in UPnP applications.
Enable the Universal Plug and Play (UPnP) feature	Select this checkbox 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).

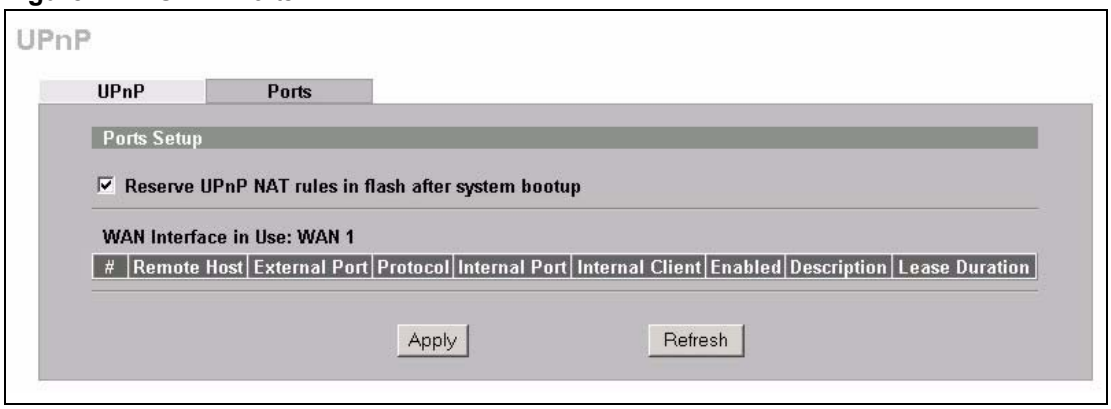
Table 78 Configuring UPnP

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. Clear this check box to have the firewall block all UPnP application packets (for example, MSN packets).
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

14.4 Displaying UPnP Port Mapping

Click **UPnP** and then **Ports** to display the screen as shown next. Use this screen to view the NAT port mapping rules that UPnP creates on the ZyWALL.

Figure 111 UPnP Ports



The following table describes the labels in this screen.

Table 79 UPnP Ports

LABEL	DESCRIPTION
Reserve UPnP NAT rules in flash after system bootup	Select this checkbox 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 port 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 79 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.

14.5 Installing UPnP in Windows Example

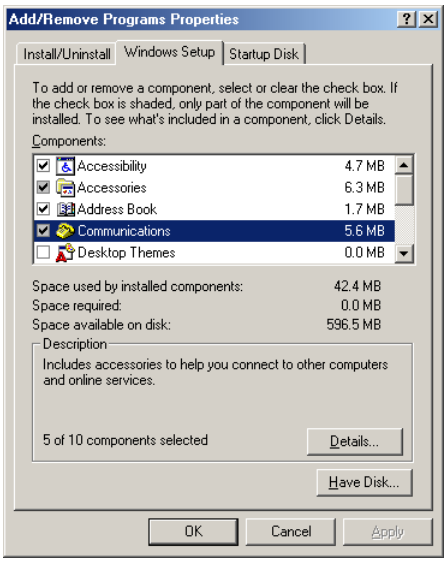
This section shows how to install UPnP in Windows Me and Windows XP.

14.5.1 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**.

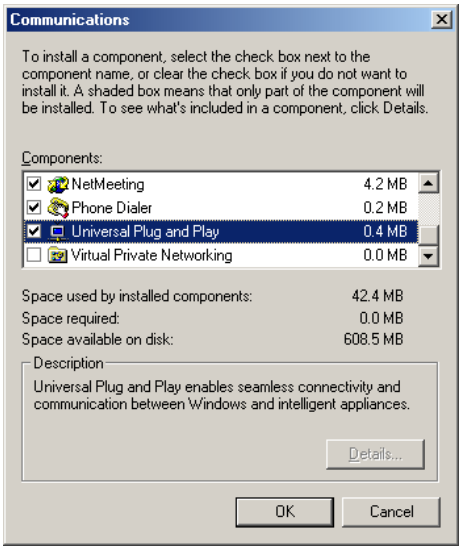
2 Click on the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.



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.



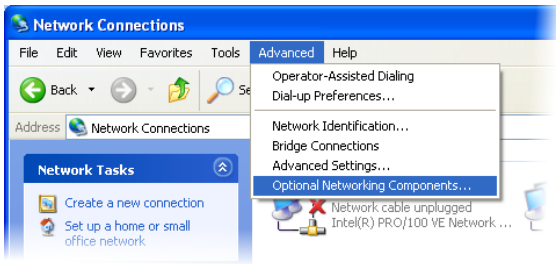
14.5.2 Installing UPnP in Windows XP

Follow the steps below to install UPnP in Windows XP.

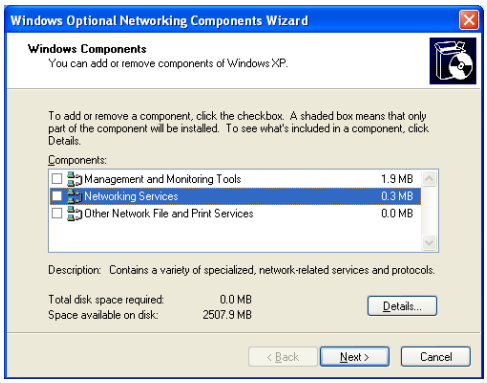
1 Click **Start**, **Settings** and **Control Panel**.

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.

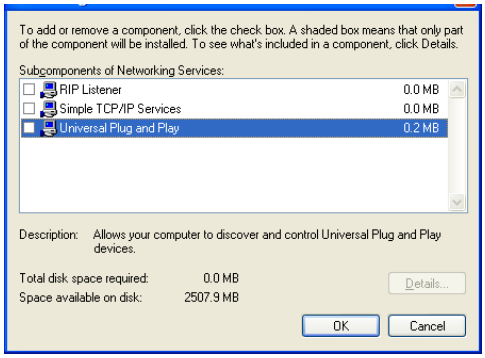


4 Select **Networking Service** in the **Components** selection box and click **Details**.



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**.



14.6 Using UPnP in Windows XP Example

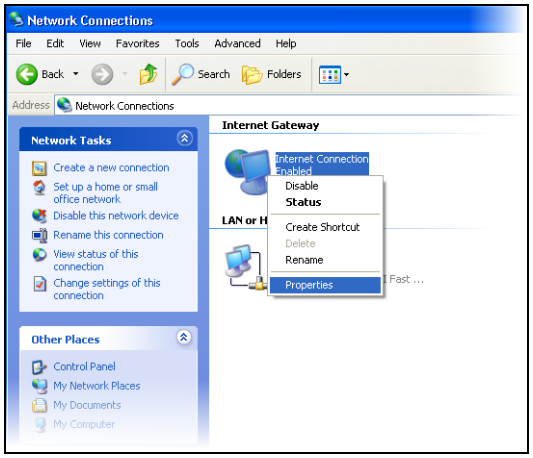
This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the ZyXEL device.

Make sure the computer is connected to a LAN port of the ZyXEL device. Turn on your computer and the ZyXEL device.

14.6.1 Auto-discover Your UPnP-enabled Network Device

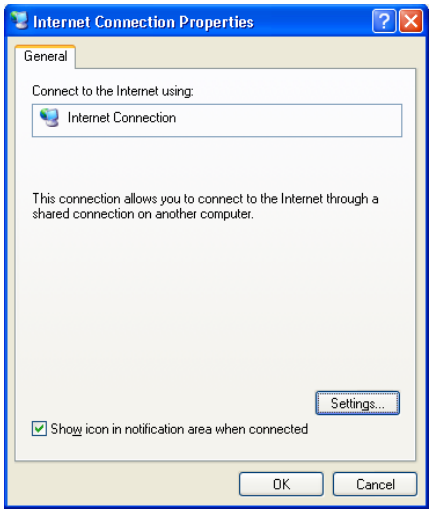
1 Click **Start** and **Control Panel**. Double-click **Network Connections**. An icon displays under **Internet Gateway**.

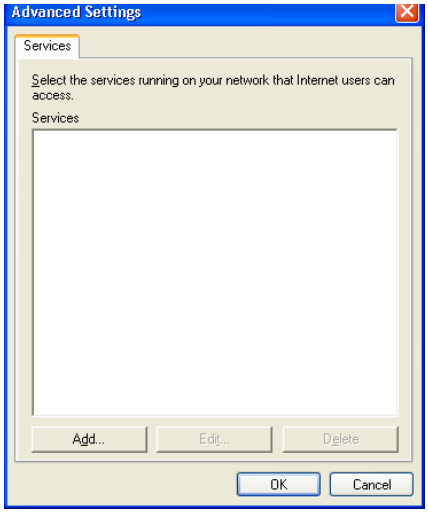
2 Right-click the icon and select **Properties**.

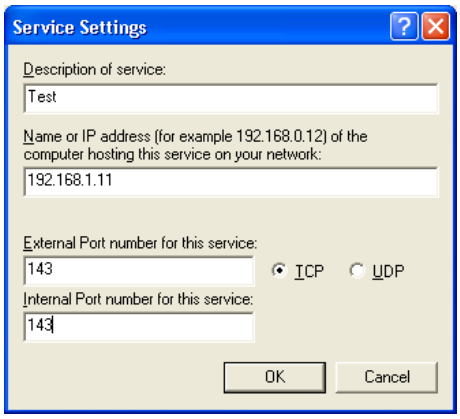


3 In the **Internet Connection Properties** window, click **Settings** to see the port mappings that were automatically created.

You may edit or delete the port mappings or click **Add** to manually add port mappings.

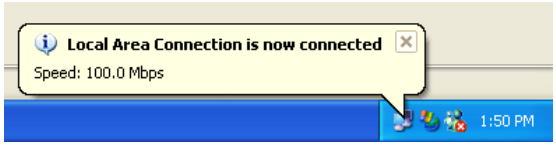




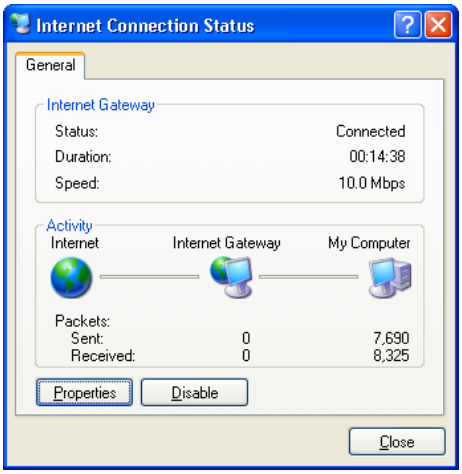


Note: When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

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.



14.6.2 Web Configurator Easy Access

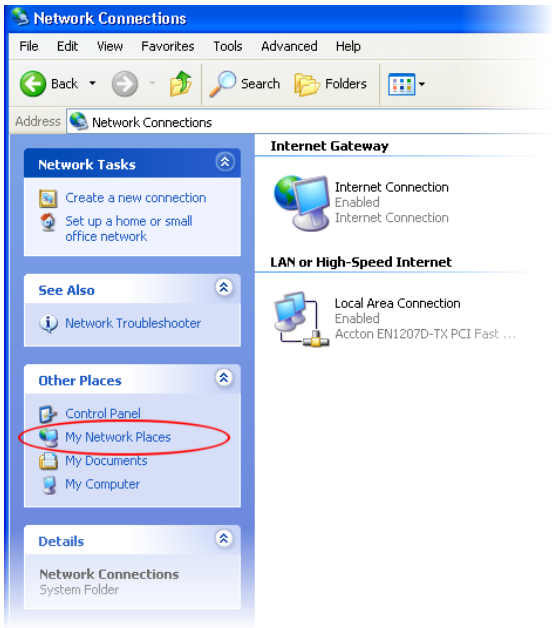
With UPnP, you can access the web-based configurator on the ZyXEL device without finding out the IP address of the ZyXEL device first. This is helpful if you do not know the IP address of the ZyXEL device.

Follow the steps below to access the web configurator.

1 Click **Start** and then **Control Panel**.

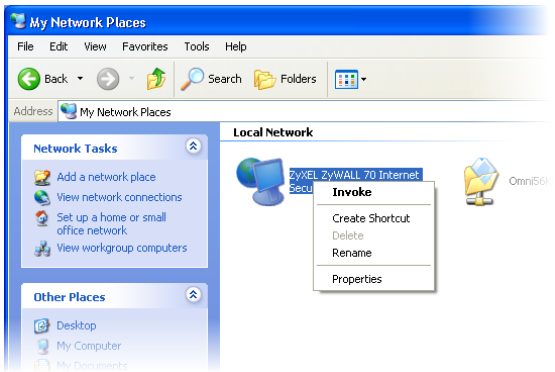
2 Double-click **Network Connections**.

3 Select **My Network Places** under **Other Places**.

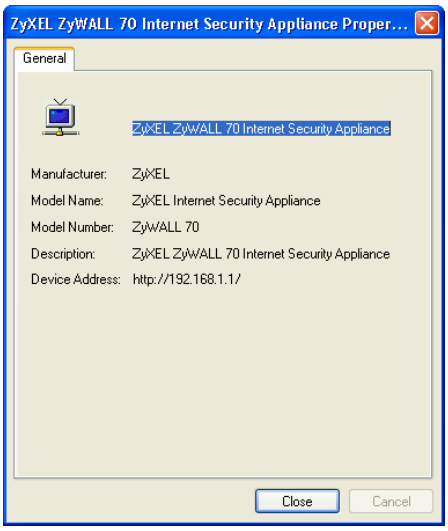


4 An icon with the description for each UPnP-enabled device displays under **Local Network**.

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.



CHAPTER 15
Logs Screens

This chapter contains information about configuring general log settings and viewing the ZyWALL's logs. Refer to Appendix N on page 347 for example log message explanations.

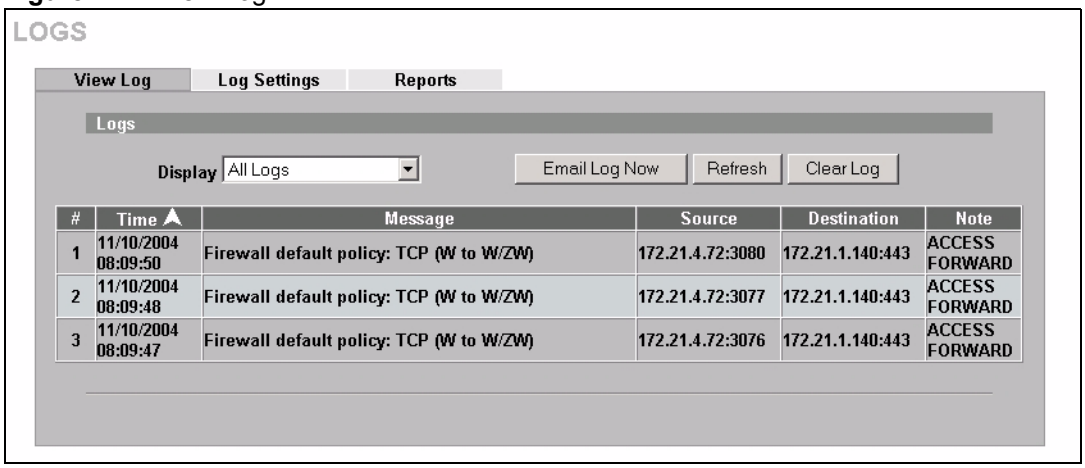
15.1 Configuring View Log

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 15.3 on page 227). Options include logs about 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.

Log entries in red indicate system error logs. The log wraps around and deletes the old entries after it fills. Click a column heading to sort the entries. A triangle indicates ascending or descending sort order.

Figure 112 View Log



The following table describes the labels in this screen.

Table 80 View Log

LABEL	DESCRIPTION
Display	The categories that you select in the **Log Settings** page (see Section 15.3 on page 227) display in the drop-down list box. 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.
#	This field displays the log number.
Time	This field displays the time the log was recorded. See Section 16.4 on page 238 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.
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 15.3 on page 227).
Refresh	Click **Refresh** to renew the log screen.
Clear Log	Click **Clear Log** to delete all the logs.

15.2 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 the appendices for more log message descriptions and details on using the command line interpreter to display logs.

Figure 113 Log Example

```
#  .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 81 Example Log Description

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.

Table 81 Example Log Description (continued)

LABEL	DESCRIPTION
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.

15.3 Configuring Log Settings

To change your ZyWALL's log settings, click **LOGS**, then the **Log Settings** tab. 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.

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.

Note: 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 114 Log Settings

LOGS

View Log | Log Settings | Reports

E-mail Log Settings

Mail Server (Outgoing SMTP Server Name or IP Address)
Mail Subject
Send Log to (E-Mail Address)
Send Alerts to (E-Mail Address)
Log Schedule When Log is Full
Day for Sending Log Sunday
Time for Sending Log 0 (Hour) 0 (Minute)

SMTP Authentication
User Name
Password

Syslog Logging

Active
Syslog Server 0.0.0.0 (Server Name or IP Address)
Log Facility Local 1

Active Log and Alert

Log	Send Immediate Alert
System Maintenance	System Errors
System Errors	Access Control
Access Control	Attacks
Asymmetrical Routes	IPSec
Multicasts / Broadcasts	IKE
TCP Reset	PKI
Packet Filter	
ICMP	
Remote Management	
Call Record	
PPP	
UPnP	
Attacks	
IPSec	
IKE	
PKI	
SSL/TLS	

Log Consolidation

Active
Log Consolidation Period 10 1 ~ 600 (Seconds)

Apply Reset

The following table describes the labels in this screen.

Table 82 Log Settings

LABEL	DESCRIPTION
E-mail Log 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.
Mail Subject	Type a title that you want to be in the subject line of the log e-mail message that the ZyWALL sends.
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.
Log Schedule	This drop-down me nu is used to configure the frequency of log messages being sent as E-mail: • **Daily** • **Weekly** • **Hourly** • **When Log is Full** • **None**. 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.
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 e-mail logs.
User Name	Enter the user name (up to 31 characters) (usually the user name of a mail account).
Password	Enter the password associated with the user name above.
Syslog Logging	Syslog logging sends a log to an external syslog server used to store logs.
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 82 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.
Log Consolidation Period	You can use the `sys log consolidate msglist` command to see what log messages will be consolidated. 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.

15.4 Configuring Reports

The **Reports** page displays which computers on the LAN send and receive the most traffic, what kinds of traffic are used the most and which web sites are visited the most often. Use the **Reports** screen to have the ZyWALL record and display the following network usage details:

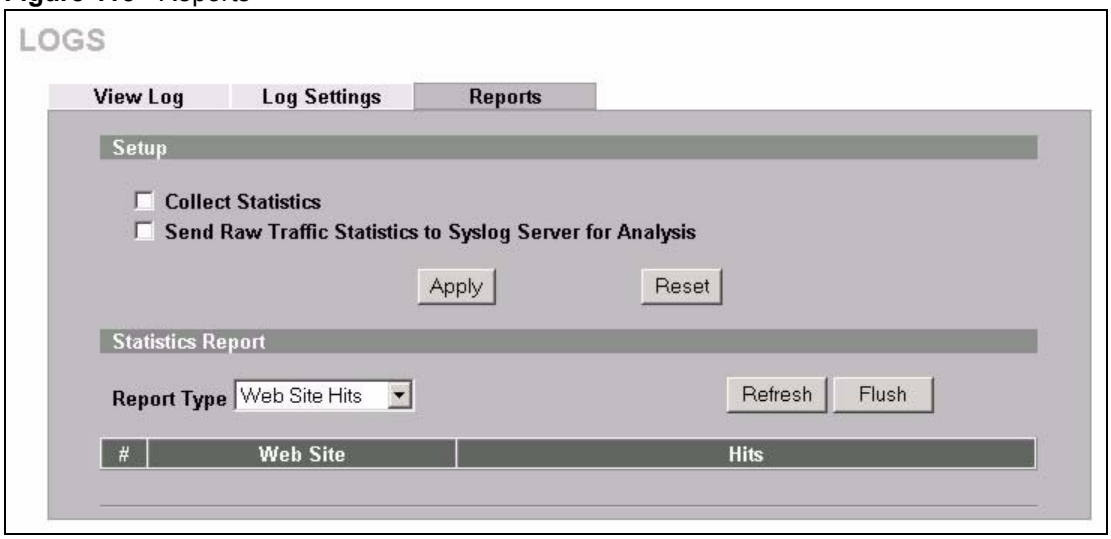
- Web sites visited the most often
- Number of times the most visited web sites were visited
- The most-used protocols or service ports
- The amount of traffic for the most used protocols or service ports
- The LAN IP addresses to and/or from which the most traffic has been sent
- How much traffic has been sent to and from the LAN IP addresses to and/or from which the most traffic has been sent

Note: 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.

The ZyWALL records web site hits by counting the HTTP GET packets. Many web sites include HTTP GET references to other web sites and the ZyWALL may count these as hits, thus the web hit count is not (yet) 100% accurate.

To change your ZyWALL's log reports, click **LOGS**, then the **Reports** tab. The screen appears as shown.

Figure 115 Reports



Note: Enabling the ZyWALL's reporting function decreases the overall throughput by about 1 Mbps.

The following table describes the labels in this screen.

Table 83 Reports

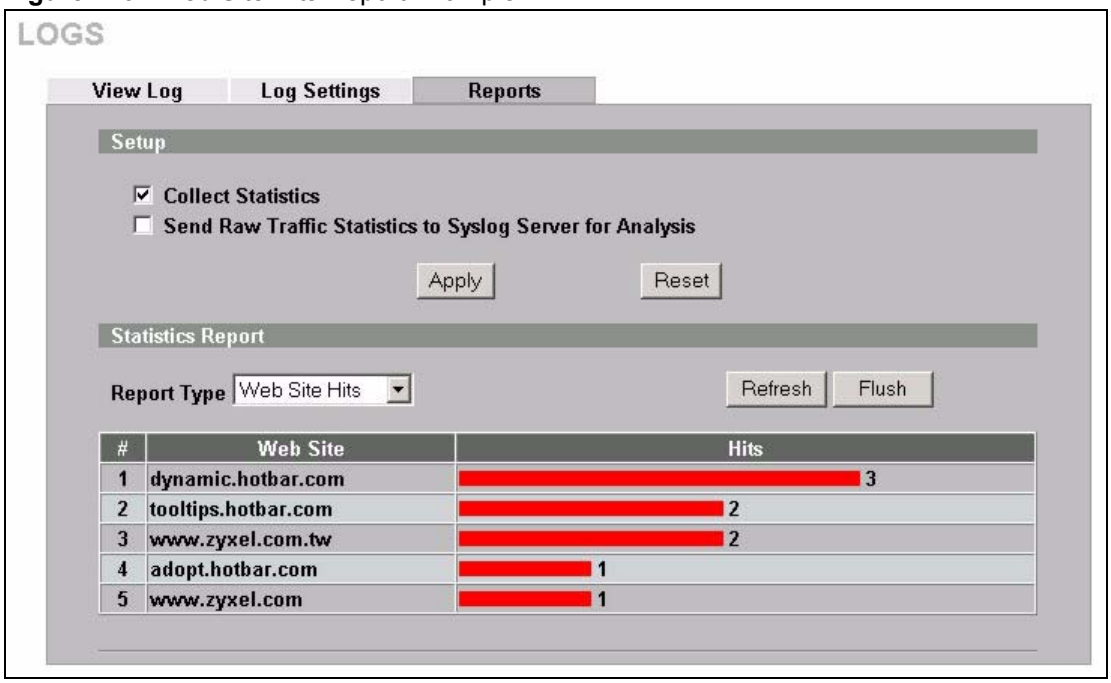
LABEL	DESCRIPTION
Collect Statistics	Select the check box and click **Apply** to have the ZyWALL record report data.
Send Raw Traffic Statistics to Syslog Server for Analysis	Select the check box and click **Apply** to have the ZyWALL send unprocessed traffic statistics to a syslog server for analysis. You must have the syslog server already configured in the **Log Settings** screen.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.
Report Type	Use the drop-down list box to select the type of reports to display. **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. **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. **LAN IP Address** displays the LAN 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.

Note: All of the recorded reports data is erased when you turn off the ZyWALL.

15.4.1 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 116 Web Site Hits Report Example



The following table describes the label in this screen.

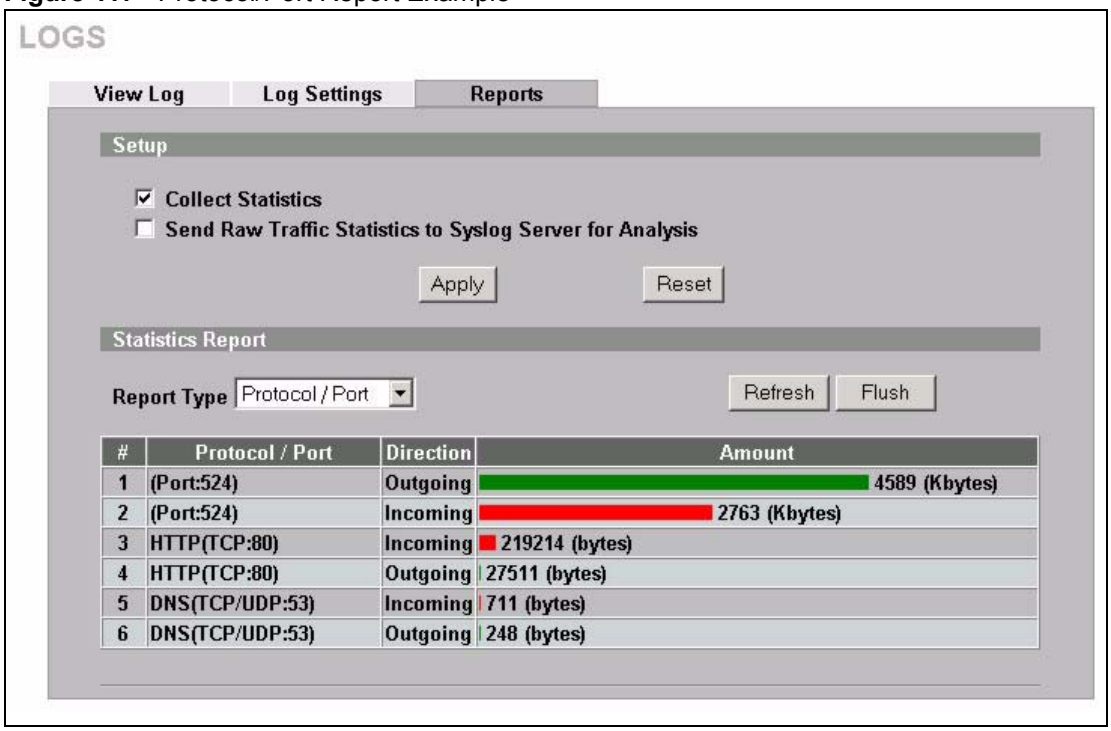
Table 84 Web Site Hits Report

LABEL	DESCRIPTION
Web Site	This column lists the domain names of the web sites visited most often from computers on the LAN. 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 87 on page 234).

15.4.2 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 117 Protocol/Port Report Example



The following table describes the labels in this screen.

Table 85 Protocol/ Port Report

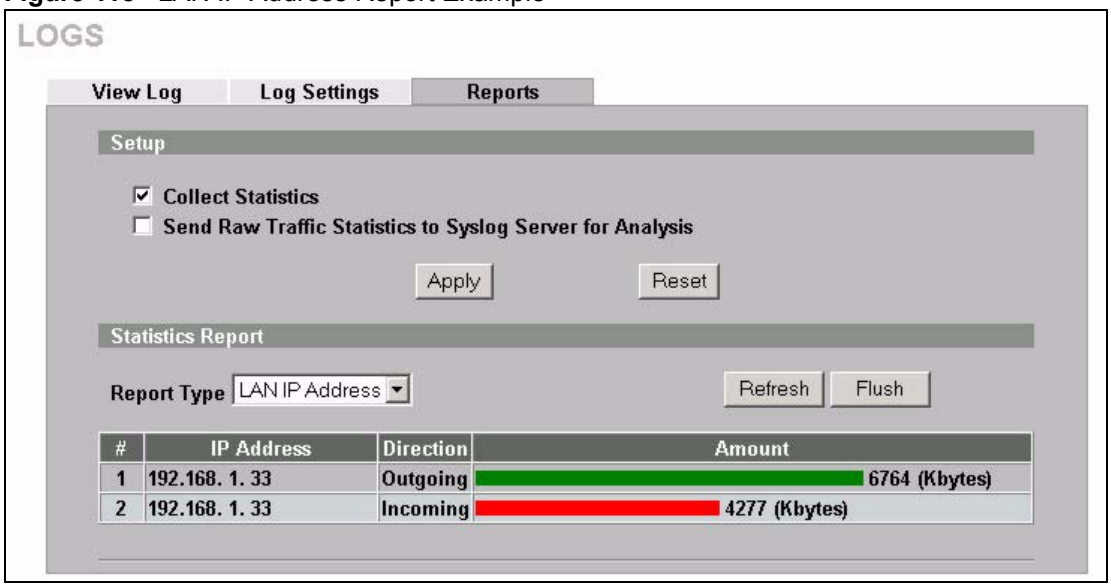
LABEL	DESCRIPTION
Protocol/Port	This column lists the protocols or service ports for which the most traffic has gone through the ZyWALL. The protocols or service ports are listed in descending order with the most used protocol or service port listed first.
Direction	This field displays **Incoming** to denote traffic that is coming in from the WAN to the LAN. This field displays **Outgoing** to denote traffic that is going out from the LAN 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 87 on page 234).

15.4.3 Viewing LAN IP Address

In the **Reports** screen, select **LAN IP Address** from the **Report Type** drop-down list box to have the ZyWALL record and display the LAN 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.

Note: Computers take turns using dynamically assigned LAN IP addresses. The ZyWALL continues recording the bytes sent to or from a LAN IP address when it is assigned to a different computer.

Figure 118 LAN IP Address Report Example



The following table describes the labels in this screen.

Table 86 LAN IP Address Report

LABEL	DESCRIPTION
IP Address	This column lists the LAN IP addresses to and/or from which the most traffic has been sent. The LAN IP addresses are listed in descending order with the LAN 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. This field displays **Outgoing** to denote traffic that is going out from the LAN to the WAN.
Amount	This column displays how much traffic has gone to and from the listed LAN IP addresses. The measurement unit shown (bytes, Kbytes, Mbytes or Gbytes) varies with the amount of traffic sent to and from the LAN IP address. The count starts over at 0 if the total traffic sent to and from a LAN IP passes the bytes count limit (see Table 87 on page 234).

15.4.4 Reports Specifications

The following table lists detailed specifications on the reports feature.

Table 87 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.

CHAPTER 16
Maintenance

This chapter displays information on the maintenance screens.

16.1 Maintenance Overview

The maintenance screens can help you view system information, upload new firmware, manage configuration and restart your ZyWALL.

16.1.1 General Setup and System Name

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".

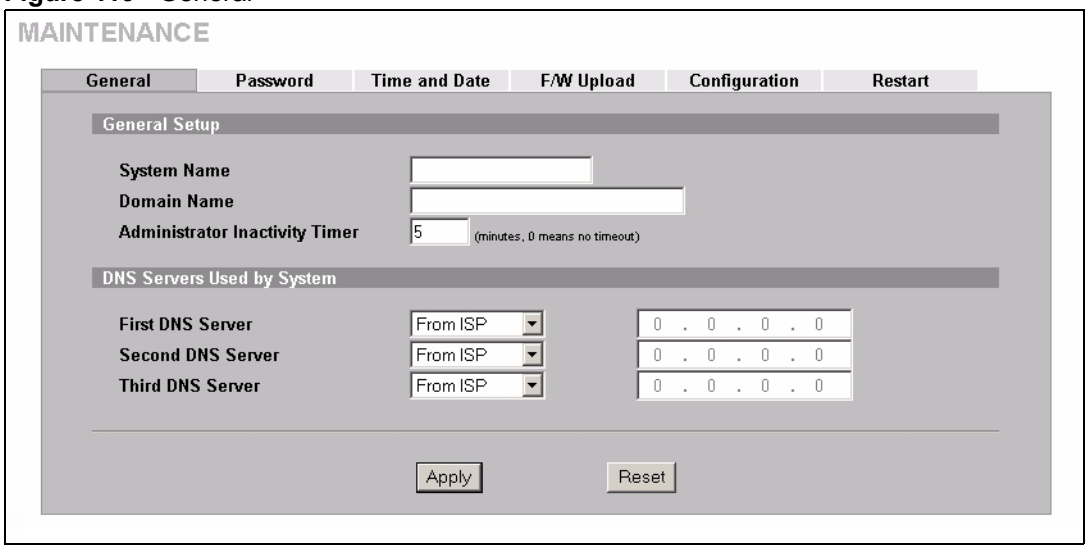
- In Windows 95/98 click **Start**, **Settings**, **Control Panel**, **Network**. Click the Identification tab, note the entry for the **Computer Name** field and enter it as the **System Name**.
- In Windows 2000, click **Start**, **Settings**, **Control Panel** and then double-click **System**. Click 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**.

16.1.2 Domain Name

The **Domain Name** entry is what is propagated to the DHCP client 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.

Click **MAINTENANCE** to open the **General** screen.

Figure 119 General



The following table describes the labels in this screen.

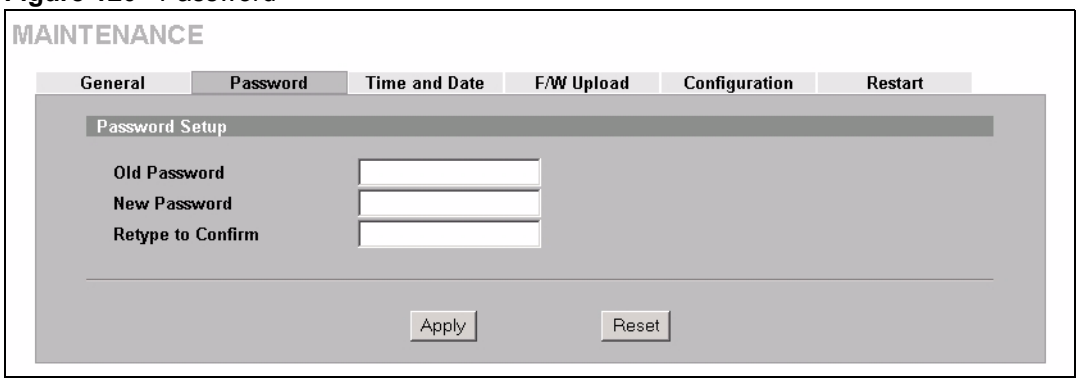
Table 88 General

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	Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. 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 CLI) 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.

16.2 Configuring Password

To change your ZyWALL's password (recommended), click **MAINTENANCE**, then the **Password** tab. The screen appears as shown. This screen allows you to change the ZyWALL's password.

Figure 120 Password



The following table describes the labels in this screen.

Table 89 Password

LABEL	DESCRIPTION
Old Password	Type the default password or the existing password you use to access the system in this field.
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.

16.3 Pre-defined NTP Time Servers List

The ZyWALL uses the following pre-defined list of NTP time servers if you do not specify a time server or it cannot synchronize with the time server you specified.

Note: When you turn on the ZyWALL, the date and time start at 2000-01-01 00:00:00. The ZyWALL then attempts to synchronize with a time server.

The ZyWALL can use this pre-defined list of time servers regardless of the **Time Protocol** you select.

When the ZyWALL uses the pre-defined list of NTP time servers, it randomly selects one server and tries to synchronize with it. If the synchronization fails, then the ZyWALL goes through the rest of the list in order from the first one tried until either it is successful or all the pre-defined NTP time servers have been tried.

Table 90 Default Time Servers

ntp1.cs.wisc.edu
ntp1.gbg.netnod.se
ntp2.cs.wisc.edu

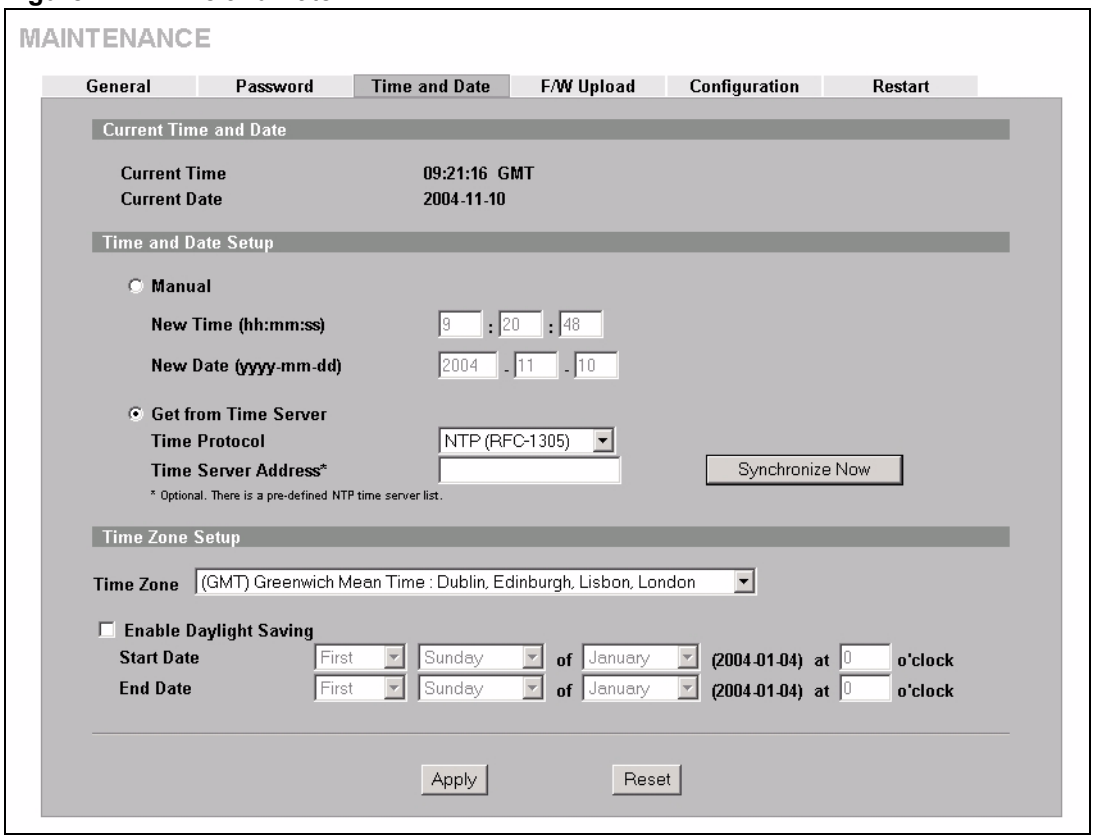
Table 90 Default Time Servers (continued)

tock.usno.navy.mil
ntp3.cs.wisc.edu
ntp.cs.strath.ac.uk
ntp1.sp.se
time1.stupi.se
tick.stdtime.gov.tw
tock.stdtime.gov.tw
time.stdtime.gov.tw

16.4 Configuring Time and Date

To change your ZyWALL's time and date, click **MAINTENANCE**, then the **Time and Date** tab. The screen appears as shown. Use this screen to configure the ZyWALL's time based on your local time zone.

Figure 121 Time and Date



The following table describes the labels in this screen.

Table 91 Time and Date

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the time of your ZyWALL. Each time you reload this page, the ZyWALL synchronizes the time with the time server.
Current Date	This field displays the date of your ZyWALL. Each time you reload this page, the ZyWALL synchronizes the date with the time server.
Time and Date Setup	
Manual	Select this radio button to enter the time and date manually. If you configure a new time and date, Time Zone and Daylight Saving at the same time, the 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. 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. 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 sends when you turn on the ZyWALL. 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 difference between them is the format. • **Daytime (RFC 867)** format is day/month/year/time zone of the server. • **Time (RFC 868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. • 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. Select this option if you use daylight savings time.

Table 91 Time and Date (continued)

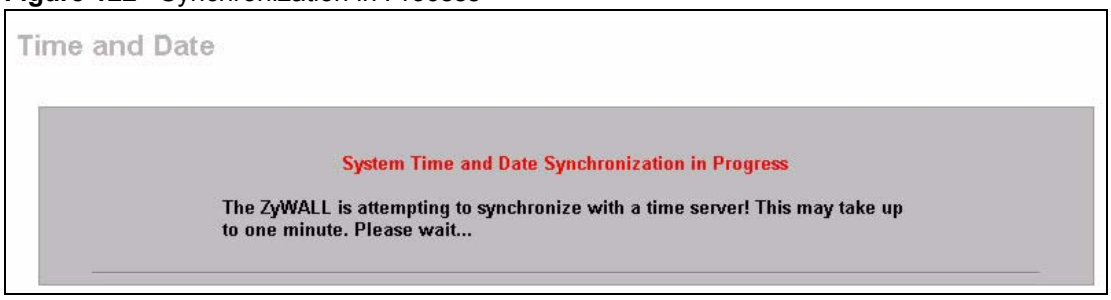
LABEL	DESCRIPTION
Start Date	Configure the day and time when Daylight Saving Time starts if you selected **Enable Daylight Saving**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the first Sunday of April. 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 **First**, **Sunday**, **April** and type 2 in the **o'clock** field. 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).
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: Daylight Saving Time ends in the United States on the last Sunday of October. 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 **Last**, **Sunday**, **October** and type 2 in the **o'clock** field. 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.

16.4.1 Time Server Synchronization

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.

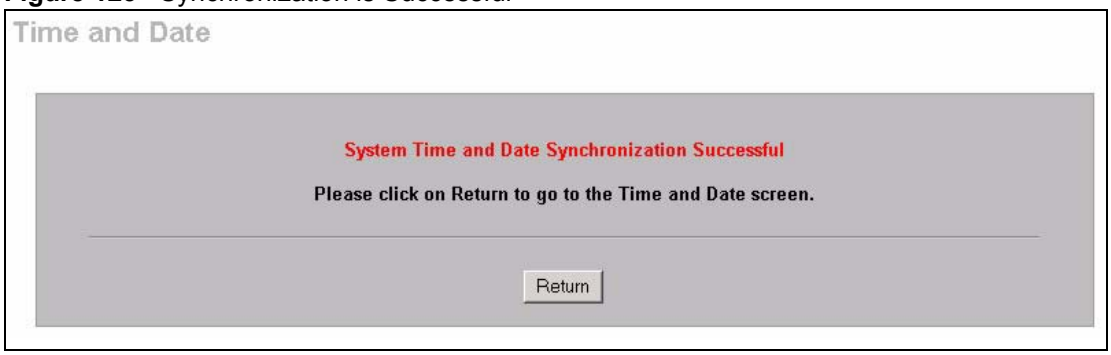
When the **System Time and Date Synchronization in Process** screen appears, wait up to one minute.

Figure 122 Synchronization in Process



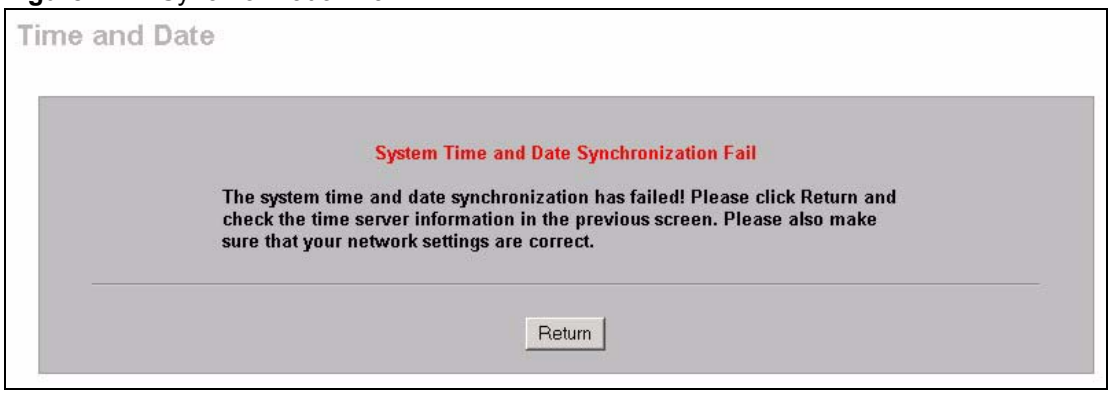
Click the **Return** button to go back to the **Time and Date** screen after the time and date is updated successfully.

Figure 123 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 124 Synchronization Fail

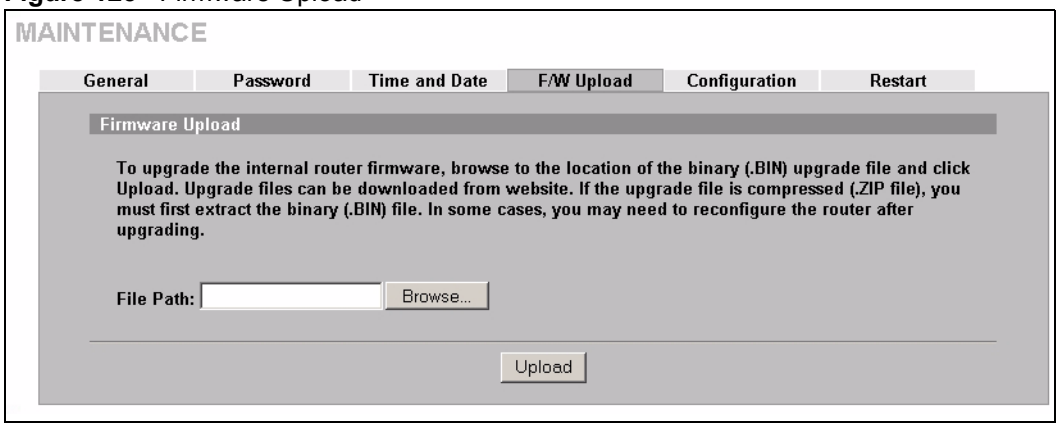


16.5 F/W Upload Screen

Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a ".bin" extension, e.g., "zywall.bin". The upload process may take up to two minutes. After a successful upload, the system will reboot. See Chapter 17 on page 249 for upgrading firmware using FTP/TFTP commands.

Click **MAINTENANCE**, and then the **F/W UPLOAD** tab. Follow the instructions in this screen to upload firmware to your ZyWALL.

Figure 125 Firmware Upload



The following table describes the labels in this screen.

Table 92 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.

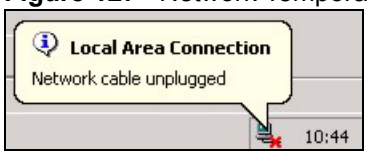
Note: Do NOT turn off the ZyWALL while firmware upload is in progress!

After you see the **Firmware Upload in Process** screen, wait two minutes before logging into the ZyWALL again.

Figure 126 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 127 Network Temporarily Disconnected



After about two minutes, log in again and check your new firmware version in the **System Status** screen.

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **F/W Upload** screen.

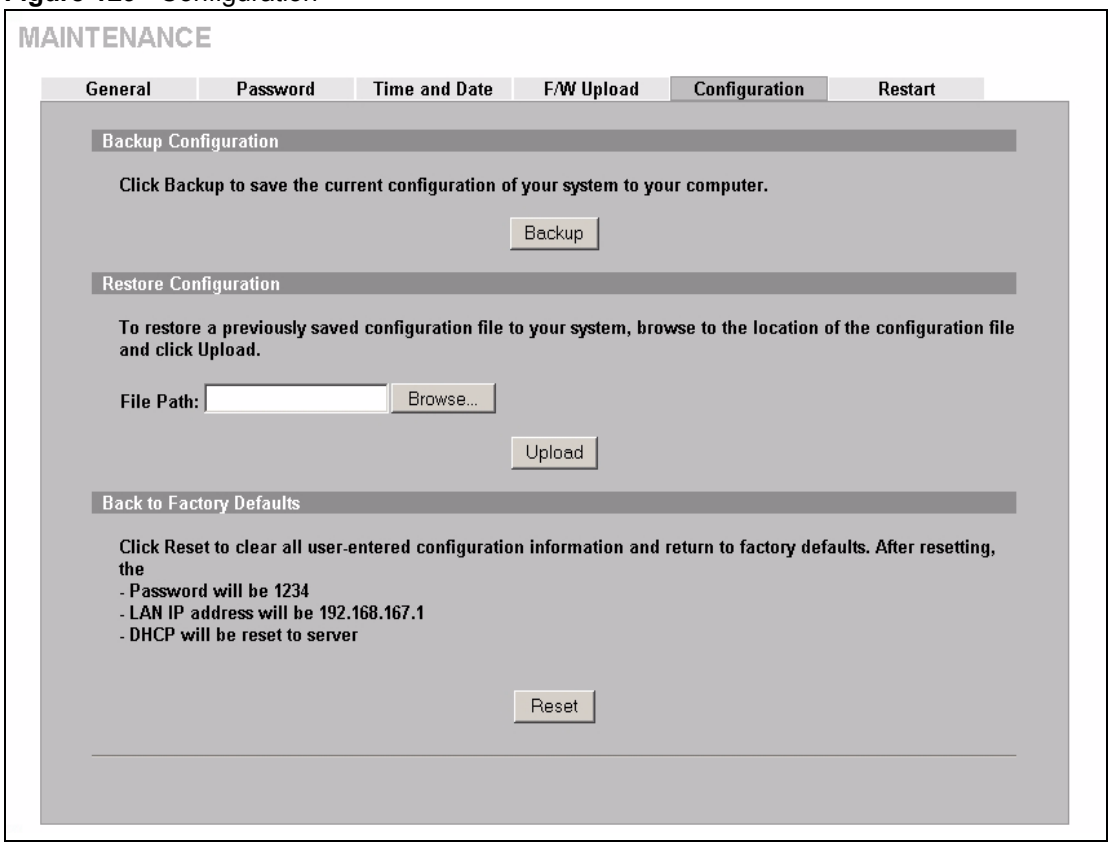
Figure 128 Firmware Upload Error

16.6 Configuration Screen

See Section 17.5 on page 254 for transferring configuration files using FTP/TFTP commands.

Click **MAINTENANCE**, and then the **Configuration** tab. Information related to factory defaults, backup configuration, and restoring configuration appears as shown next.

Figure 129 Configuration



16.6.1 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.

16.6.2 Restore Configuration

Restore Configuration allows you to upload a new or previously saved configuration file from your computer to your ZyWALL.

Table 93 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.

Note: 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 130 Configuration Upload Successful

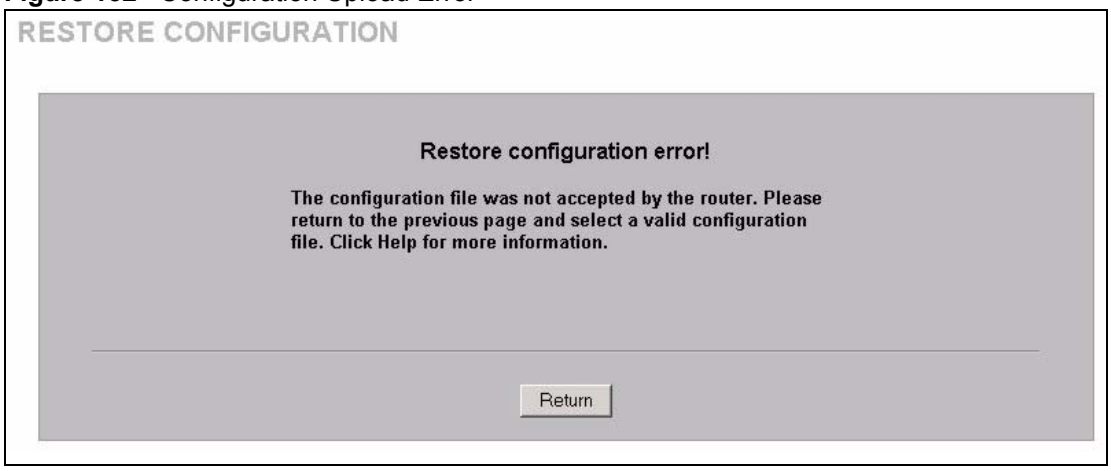
The ZyWALL automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 131 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 ZyWALL LAN IP address (192.168.167.1). See your Quick Start Guide or the appendix 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.

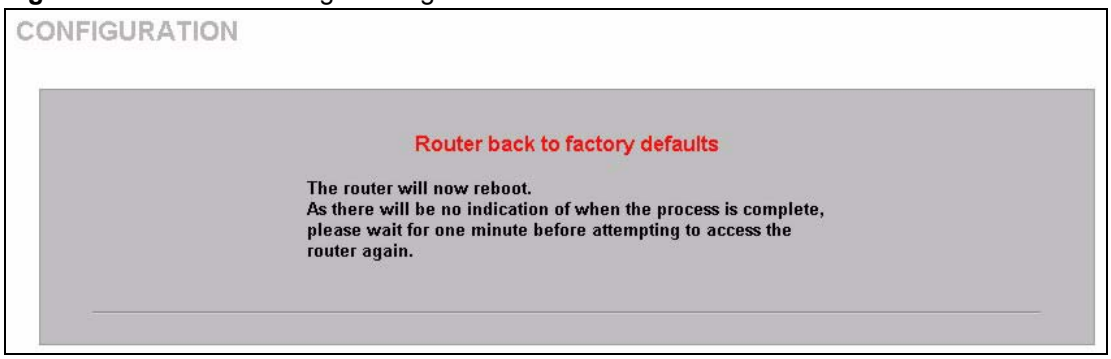
Figure 132 Configuration Upload Error



16.6.3 Back to Factory Defaults

Pressing the **Reset** button in this section clears all user-entered configuration information and returns the ZyWALL to its factory defaults as shown on the screen. The following warning screen will appear.

Figure 133 Reset Warning Message



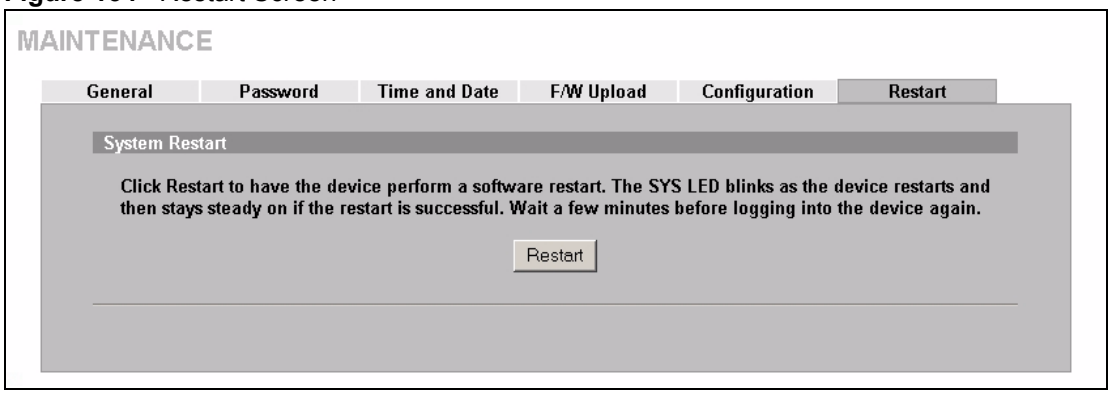
You can also press the **RESET** button on the rear panel to reset the factory defaults of your ZyWALL. Refer to Section 2.3 on page 41 for more information on the **RESET** button.

16.7 Restart Screen

System restart allows you to reboot the ZyWALL without turning the power off.

Click **MAINTENANCE**, and then **Restart**. Click **Restart** to have the ZyWALL reboot. This does not affect the ZyWALL's configuration.

Figure 134 Restart Screen



CHAPTER 17
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.

17.1 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.

17.2 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 **Home** screen to confirm that you have uploaded the correct firmware version.

Table 94 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

17.3 Backup Configuration

Note: The ZyWALL displays messages explaining how to backup, restore and upload files via FTP.

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.

17.3.1 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.

Figure 135 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
```

17.3.2 GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

Table 95 General Commands for GUI-based FTP Clients

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	Anonymous. 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. Normal. 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).

17.3.3 File Maintenance Over WAN

TFTP and FTP over the WAN will not work when:

1. The firewall is active (turn the firewall off or create a firewall rule to allow access from the WAN).
2. You have disabled Telnet service in the **Remote Management** screen.
3. The IP you entered in the **Secured Client IP** field in the **Remote Management** screen does not match the client IP. If it does not match, the ZyWALL will disconnect the session immediately.

17.3.4 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.

17.3.5 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.

17.3.6 GUI-based TFTP Clients

The following table describes some of the fields that you may see in GUI-based TFTP clients.

Table 96 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 17.3.3 on page 251 to read about configurations that disallow FTP over WAN.

17.4 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.

Note: 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.

17.4.1 Restore Using FTP

For details about backup using (T)FTP please refer to earlier sections on FTP and TFTP file upload in this chapter.

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.

17.4.2 Restore Using FTP Session Example

Figure 136 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 17.3.3 on page 251 to read about configurations that disallow TFTP and FTP over WAN.

17.5 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 17.4 on page 253. .

Note: WARNING! Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE YOUR ZyWALL.

17.5.1 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.

17.5.2 FTP File Upload Command from the Command Prompt Example

Follow the steps below to upload the firmware.

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.

17.5.3 FTP Session Example of Firmware File Upload

Figure 137 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 17.3.3 on page 251 to read about configurations that disallow TFTP and FTP over WAN.

17.5.4 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 management session timeout, so the TFTP transfer will not be interrupted. Enter "command sys stdio 5" to restore the five-minute management session 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.

17.5.5 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.

CHAPTER 18
Troubleshooting

This chapter covers potential problems and possible remedies. After each problem description, some instructions are provided to help you to diagnose and to solve the problem. Please see our included disk for further information.

18.1 Problems Starting Up the ZyWALL

Table 97 Troubleshooting the Start-Up of Your ZyWALL

PROBLEM	CORRECTIVE ACTION
None of the LEDs turn on when you turn on the ZyWALL.	If supplying power via the **USB** port, use only the included USB cable.
	Power to the ZyWALL is too low. Disconnect the USB cable from the ZyWALL and connect the power adaptor.
	If the error persists, you may have a hardware problem. In this case, you should contact your vendor.
All LEDs blink at the same time.	Power to the ZyWALL is too low. Disconnect the USB cable from the ZyWALL and connect the power adaptor.

18.2 Problems Accessing the ZyWALL

Table 98 Troubleshooting Accessing the ZyWALL

PROBLEM	CORRECTIVE ACTION
I cannot access the ZyWALL.	The username is "admin". The default password is "1234". The **Password** and **Username** fields are case-sensitive. Make sure that you enter the correct password and username using the proper casing. If you have changed the password and have now forgotten it, you will need to upload the default configuration file. This restores all of the factory defaults including the password.
I cannot access the web configurator.	Make sure that there is no console session running. Use the ZyWALL's WAN IP address when configuring from the WAN. Refer to the instructions on checking your WAN connection. Use the ZyWALL's LAN IP address when configuring from the LAN. Refer to for instructions on checking your LAN connection. Check that you have enabled web service access. If you have configured a secured client IP address, your computer's IP address must match it. Refer to the chapter on remote management for details. Your computer's and the ZyWALL's IP addresses must be on the same subnet for LAN access. See the following section to check that pop-up windows, JavaScripts and Java permissions are allowed.

18.2.1 Pop-up Windows, JavaScripts and Java Permissions

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

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

Note: Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

18.2.1.1 Internet Explorer Pop-up Blockers

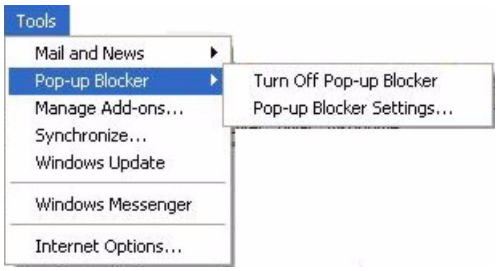
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

18.2.1.1.1 Disable pop-up Blockers

1. In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 138 Pop-up Blocker

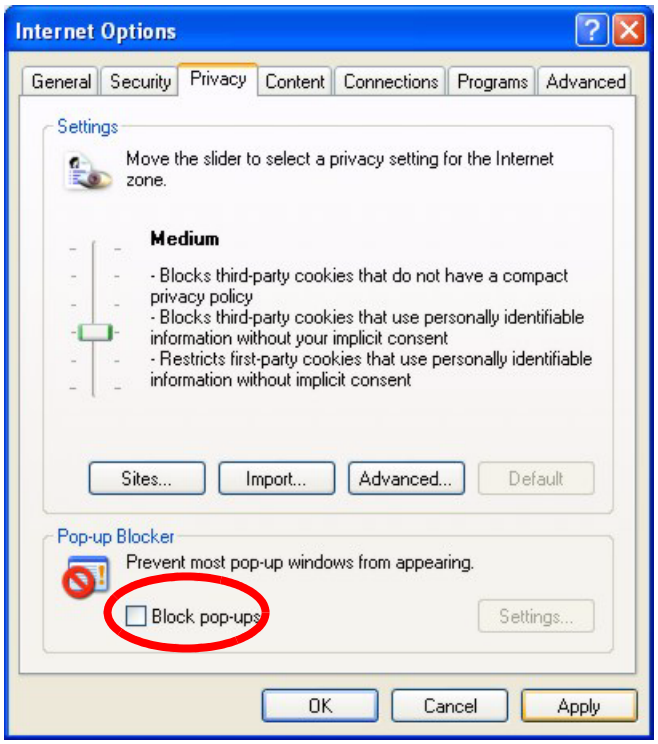


You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.

2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 139 Internet Options



3 Click **Apply** to save this setting.

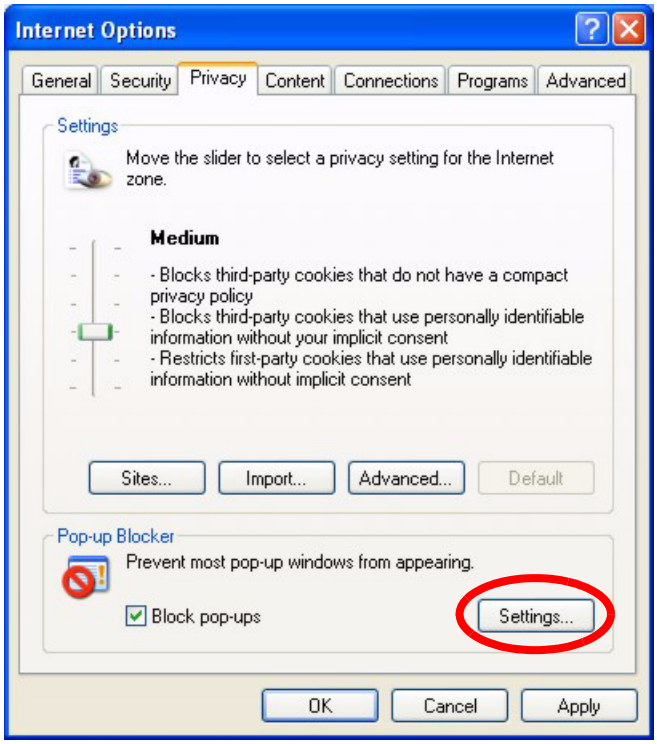
18.2.1.1.2 Enable pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings…**to open the **Pop-up Blocker Settings** screen.

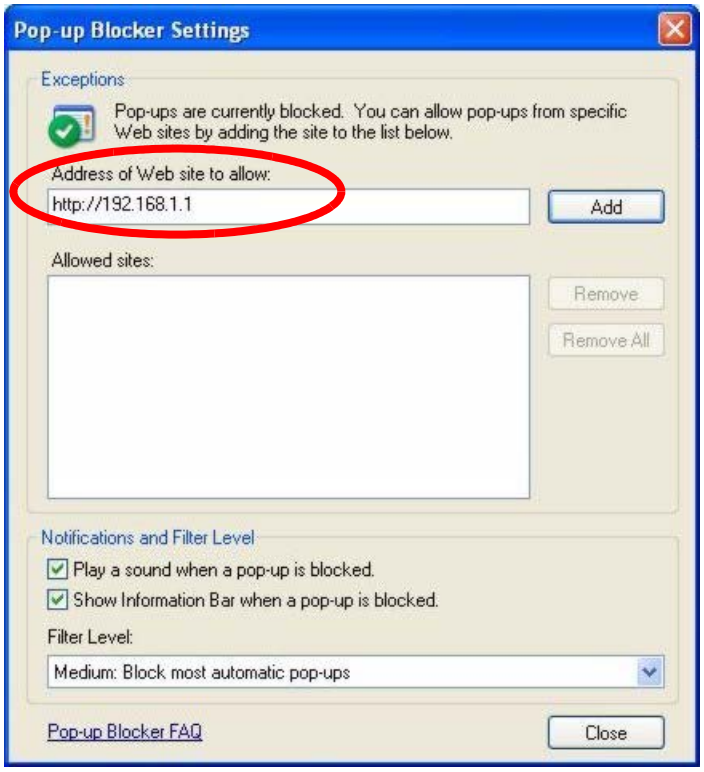
Figure 140 Internet Options



3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix "http://". For example, http://192.168.1.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 141 Pop-up Blocker Settings



5 Click **Close** to return to the **Privacy** screen.

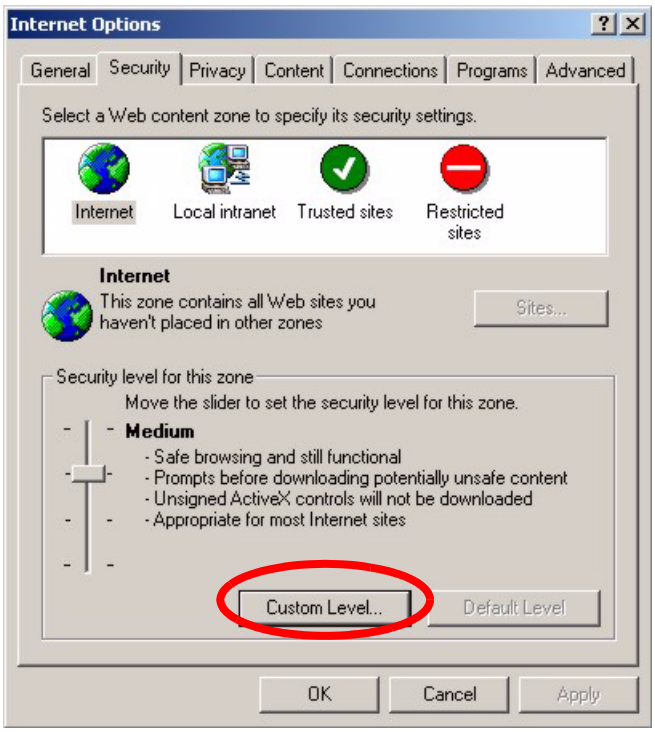
6 Click **Apply** to save this setting.

18.2.1.2 JavaScripts

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

Figure 142 Internet Options



2 Click the **Custom Level...** button.

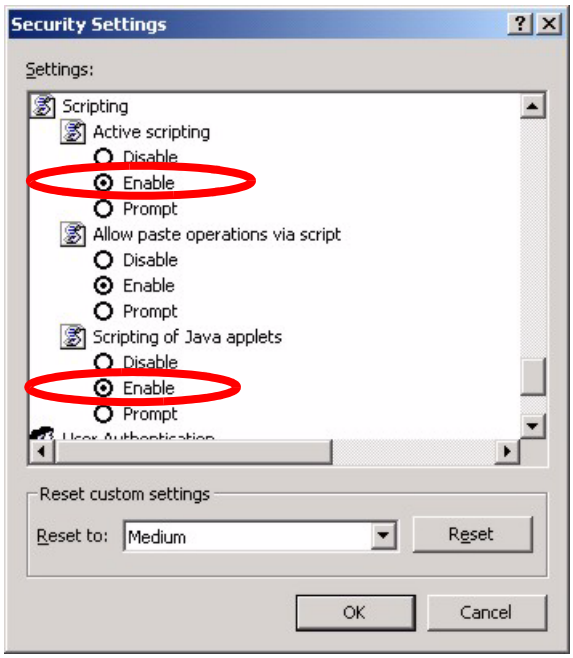
3 Scroll down to **Scripting**.

4 Under **Active scripting** make sure that **Enable** is selected (the default).

5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

6 Click **OK** to close the window.

Figure 143 Security Settings - Java Scripting



18.2.1.3 Java Permissions

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

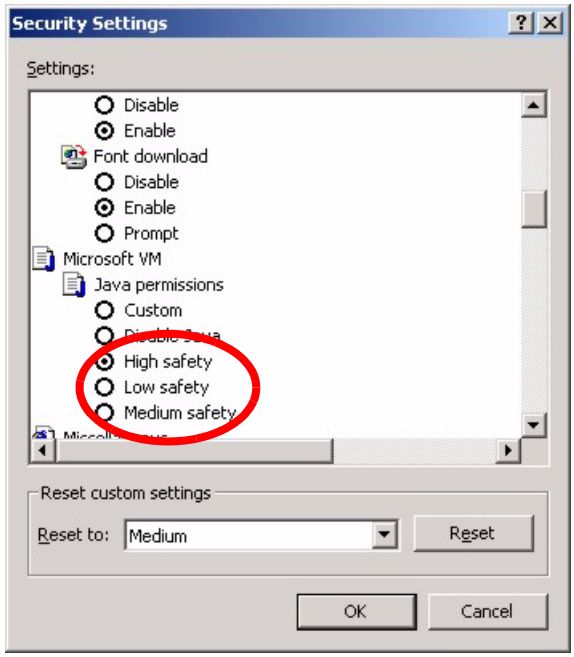
2 Click the **Custom Level...** button.

3 Scroll down to **Microsoft VM**.

4 Under **Java permissions** make sure that a safety level is selected.

5 Click **OK** to close the window.

Figure 144 Security Settings - Java



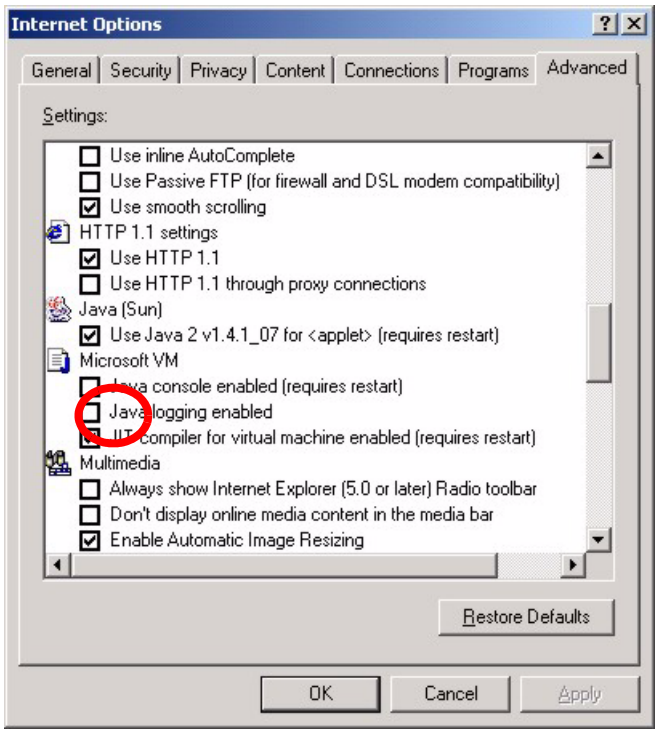
18.2.1.3.1 JAVA (Sun)

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Advanced** tab.

2 make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.

3 Click **OK** to close the window.

Figure 145 Java (Sun)



18.3 Problems with the LAN Interface

Table 99 Troubleshooting the LAN Interface

PROBLEM	CORRECTIVE ACTION
Cannot access the ZyWALL from the LAN.	Check your Ethernet cable type and connections. Refer to the Quick Start Guide for LAN connection instructions.
	Make sure the computer's Ethernet adapter is installed and functioning properly.
Cannot ping any computer on the LAN.	Check the 10M/100M LAN LEDs on the front panel. One of these LEDs should be on. If they are both off, check the cables between your ZyWALL and hub or the station.
	Verify that the IP address and the subnet mask of the ZyWALL and the computers are on the same subnet.

18.4 Problems with the WAN Interface

Table 100 Troubleshooting the WAN Interface

PROBLEM	CORRECTIVE ACTION
Cannot get WAN IP address from the ISP.	The ISP provides the WAN IP address after authentication. Authentication may be through the user name and password, the MAC address or the host name. Use the following corrective actions to make sure the ISP can authenticate your connection.
	You need a username and password if you're using PPPoE or PPTP encapsulation. Make sure that you have entered the correct **Service Type**, **User Name** and **Password** (the user name and password are case sensitive). Refer to Chapter 4 on page 65.
	If your ISP requires MAC address authentication, you should clone the MAC address from your computer on the LAN as the ZyWALL's WAN MAC address. Refer to Chapter 4 on page 65. It is recommended that you clone your computer's MAC address, even if your ISP presently does not require MAC address authentication.
	If your ISP requires host name authentication, configure your computer's name as the ZyWALL's system name. Refer to Section 2.5 on page 53.

18.5 Problems with Internet Access

Table 101 Troubleshooting Internet Access

PROBLEM	CORRECTIVE ACTION
Cannot access the Internet.	Connect your cable/DSL modem with the ZyWALL using the appropriate cable. Check with the manufacturer of your cable/DSL device about your cable requirement because some devices may require crossover cable and others a regular straight-through cable.
	Refer to Chapter 4 on page 65 and verify your settings.

18.6 Problems with the Password

Table 102 Troubleshooting the Password

PROBLEM	CORRECTIVE ACTION
Cannot access the ZyWALL.	The password field is case sensitive. Make sure that you enter the correct password using the proper casing.
	Use the Reset button to restore the factory default configuration file. This will restore all of the factory defaults including the password. See Section 2.3 on page 45 for details.

18.7 Problems with Remote Management

Table 103 Troubleshooting Telnet

PROBLEM	CORRECTIVE ACTION
Cannot access the ZyWALL from the LAN or WAN.	Refer to Section 15.1.1 on page 232 for scenarios when remote management may not be possible.
	When NAT is enabled: • Use the ZyWALL's WAN IP address when configuring from the WAN. • Use the ZyWALL's LAN IP address when configuring from the LAN.
	Refer to Section 18.3 on page 265 for instructions on checking your LAN connection.
	Refer to Section 18.4 on page 266 for instructions on checking your WAN connection.

Appendix A
Setting up Your Computer's IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

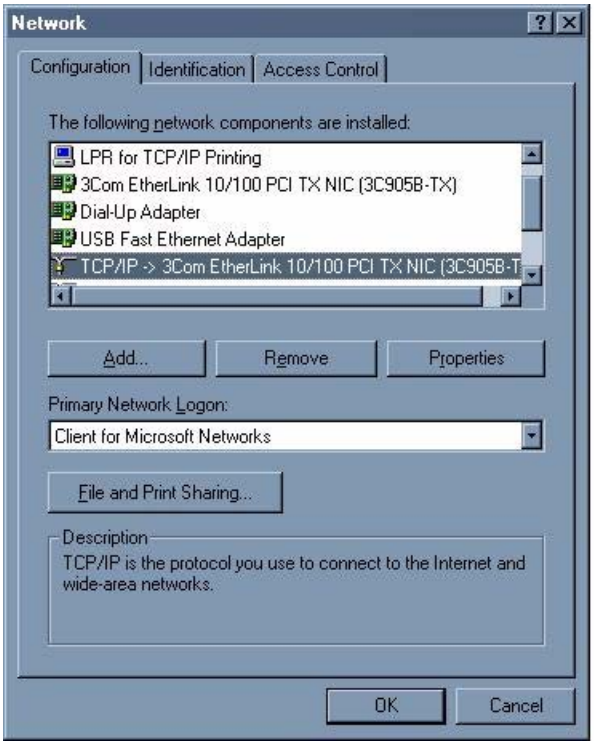
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the ZyWALL's LAN port.

Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window.

Figure 146 WIndows 95/98/Me: Network: Configuration



Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

1. In the **Network** window, click **Add**.
2. Select **Adapter** and then click **Add**.
3. Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

1. In the **Network** window, click **Add**.
2. Select **Protocol** and then click **Add**.
3. Select **Microsoft** from the list of **manufacturers**.
4. Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

1. Click **Add**.
2. Select **Client** and then click **Add**.

3 Select **Microsoft** from the list of manufacturers.

4 Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.

5 Restart your computer so the changes you made take effect.

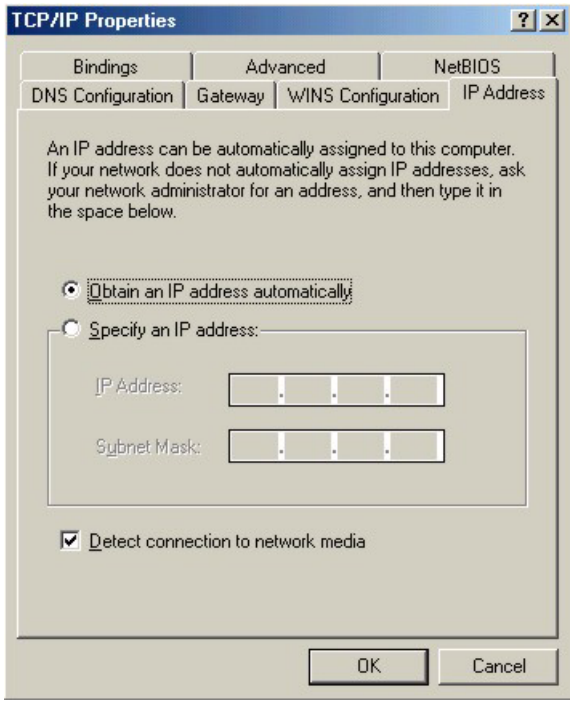
Configuring

1 In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**

2 Click the **IP Address** tab.

- If your IP address is dynamic, select **Obtain an IP address automatically**.
- If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

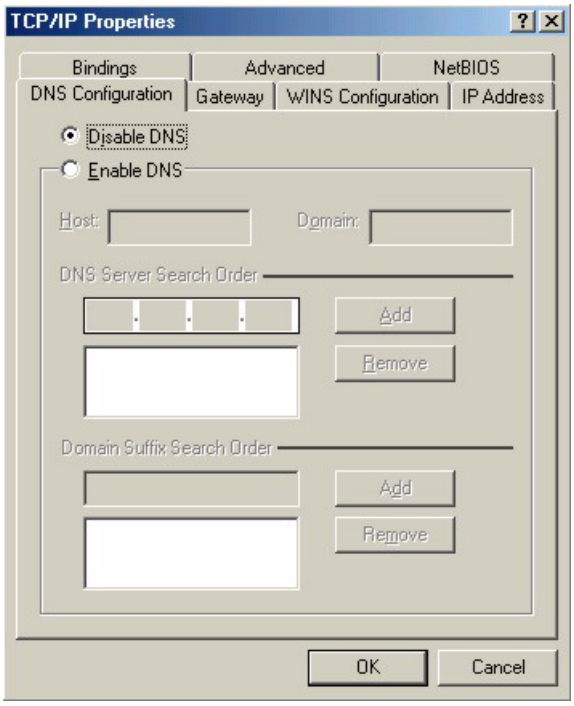
Figure 147 Windows 95/98/Me: TCP/IP Properties: IP Address



3 Click the **DNS** Configuration tab.

- If you do not know your DNS information, select **Disable DNS**.
- If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).

Figure 148 Windows 95/98/Me: TCP/IP Properties: DNS Configuration



4 Click the **Gateway** tab.

- If you do not know your gateway's IP address, remove previously installed gateways.
- If you have a gateway IP address, type it in the **New gateway field** and click **Add**.

5 Click **OK** to save and close the **TCP/IP Properties** window.

6 Click **OK** to close the **Network** window. Insert the Windows CD if prompted.

7 Turn on your ZyWALL and restart your computer when prompted.

Verifying Settings

1 Click **Start** and then **Run**.

2 In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.

3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

The following example figures use the default Windows XP GUI theme.

1 Click **start** (**Start** in Windows 2000/NT), **Settings**, **Control Panel**.

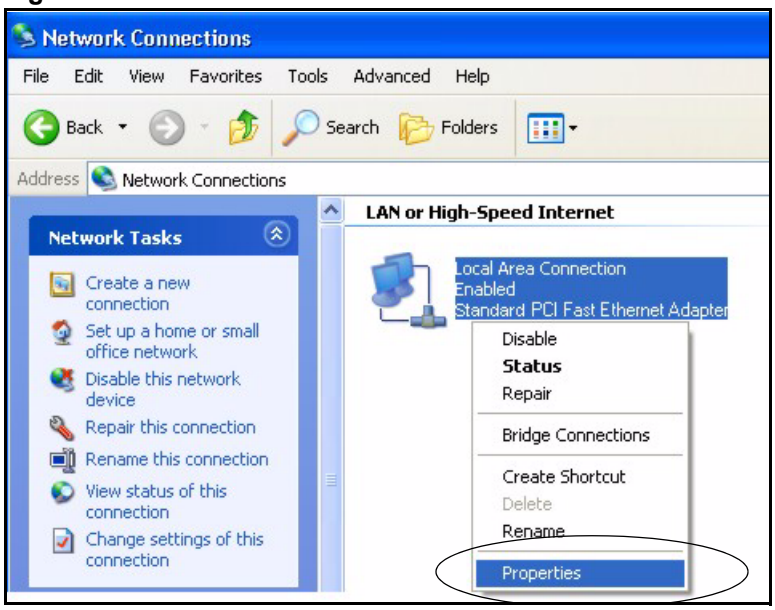
Figure 149 Windows XP: Start Menu

2 In the **Control Panel**, double-click **Network Connections** (**Network and Dial-up Connections** in Windows 2000/NT).

Figure 150 Windows XP: Control Panel

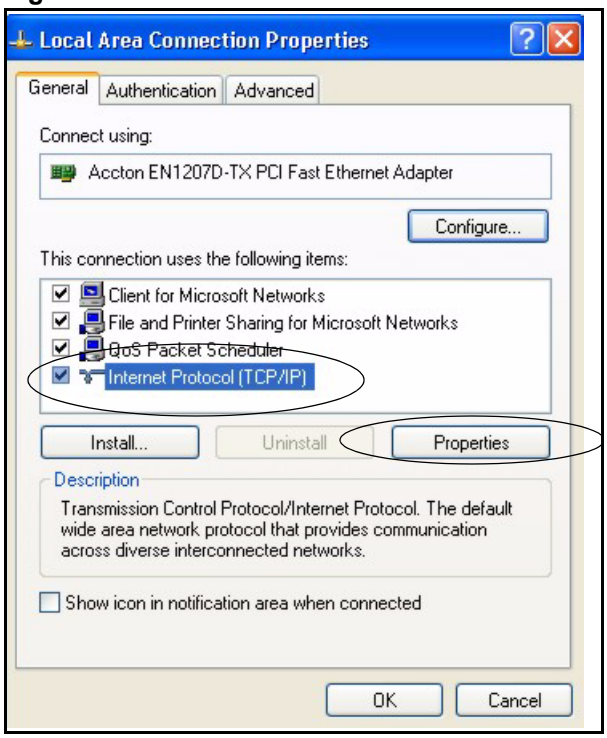
3 Right-click **Local Area Connection** and then click **Properties**.

Figure 151 Windows XP: Control Panel: Network Connections: Properties



4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and then click **Properties**.

Figure 152 Windows XP: Local Area Connection Properties

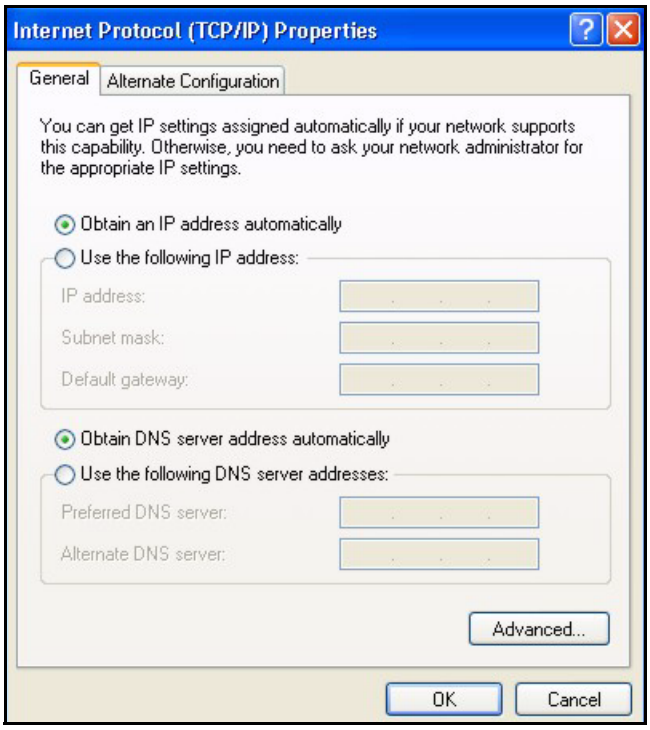


5 The **Internet Protocol TCP/IP Properties** window opens (the **General tab** in Windows XP).

- If you have a dynamic IP address click **Obtain an IP address automatically**.

- If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.
- Click **Advanced**.

Figure 153 Windows XP: Internet Protocol (TCP/IP) Properties

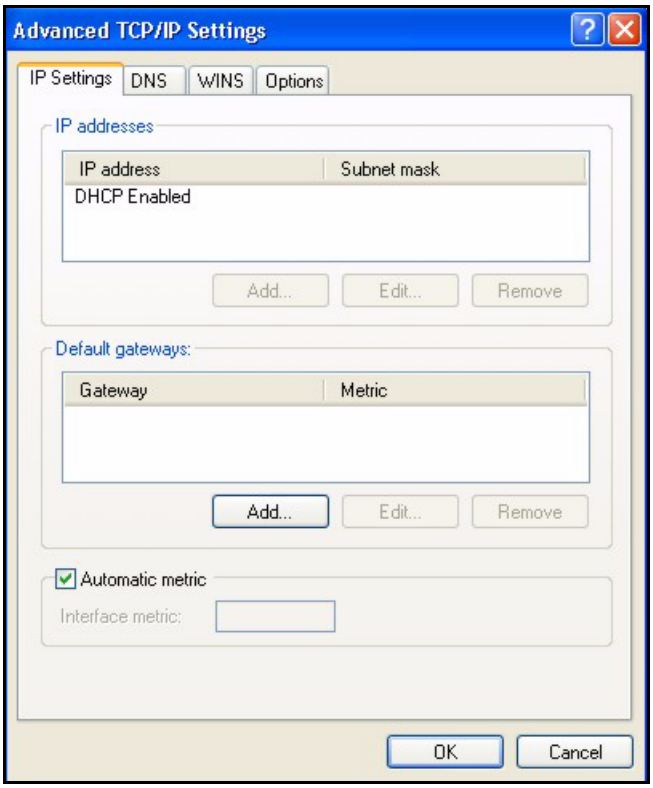


6 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.
- Click **OK** when finished.

Figure 154 Windows XP: Advanced TCP/IP Properties

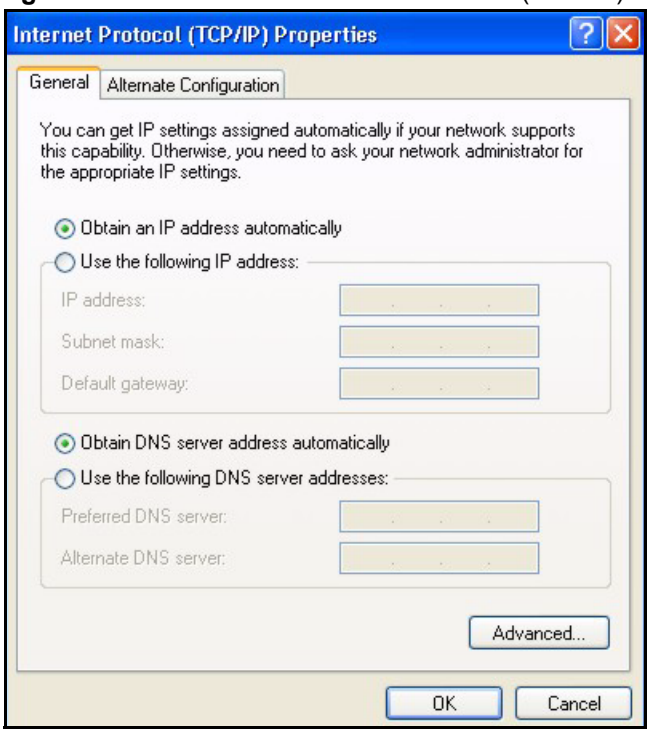


7 In the **Internet Protocol TCP/IP Properties** window (the **General tab** in Windows XP):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

  If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

Figure 155 Windows XP: Internet Protocol (TCP/IP) Properties



8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

9 Click **Close** (**OK** in Windows 2000/NT) to close the **Local Area Connection Properties** window.

10 Close the **Network Connections** window (**Network and Dial-up Connections** in Windows 2000/NT).

11 Turn on your ZyWALL and restart your computer (if prompted).

Verifying Settings

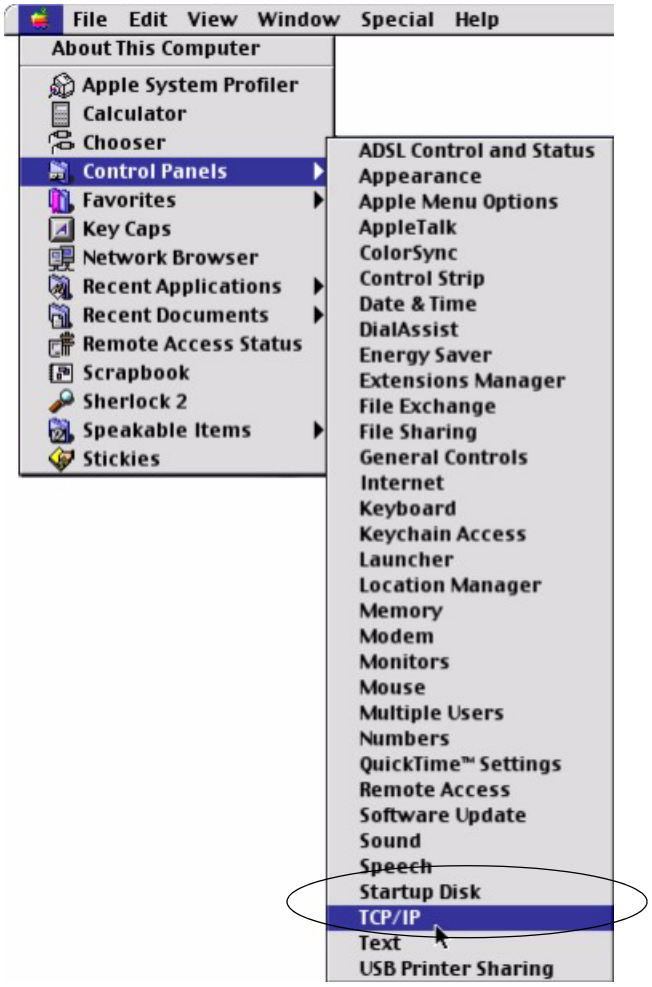
1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Macintosh OS 8/9

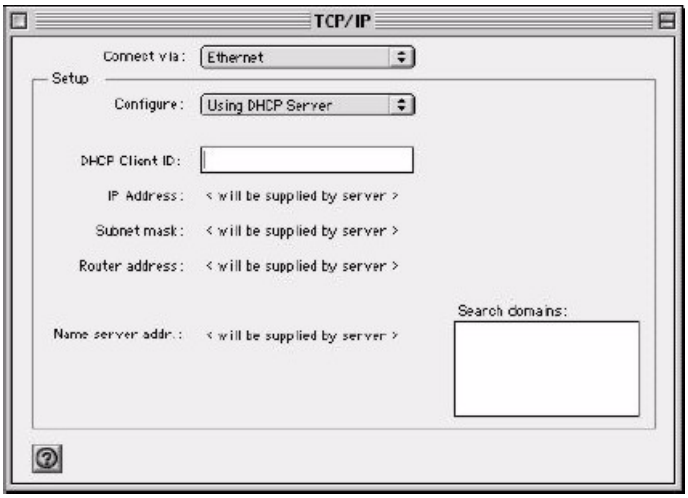
1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 156 Macintosh OS 8/9: Apple Menu



2 Select **Ethernet built-in** from the **Connect via** list.

Figure 157 Macintosh OS 8/9: TCP/IP



3 For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.

4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your ZyWALL in the **Router address** box.

5 Close the **TCP/IP Control Panel**.

6 Click **Save** if prompted, to save changes to your configuration.

7 Turn on your ZyWALL and restart your computer (if prompted).

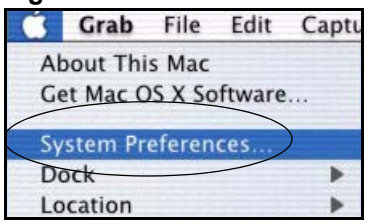
Verifying Settings

Check your TCP/IP properties in the **TCP/IP Control Panel** window.

Macintosh OS X

1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

Figure 158 Macintosh OS X: Apple Menu

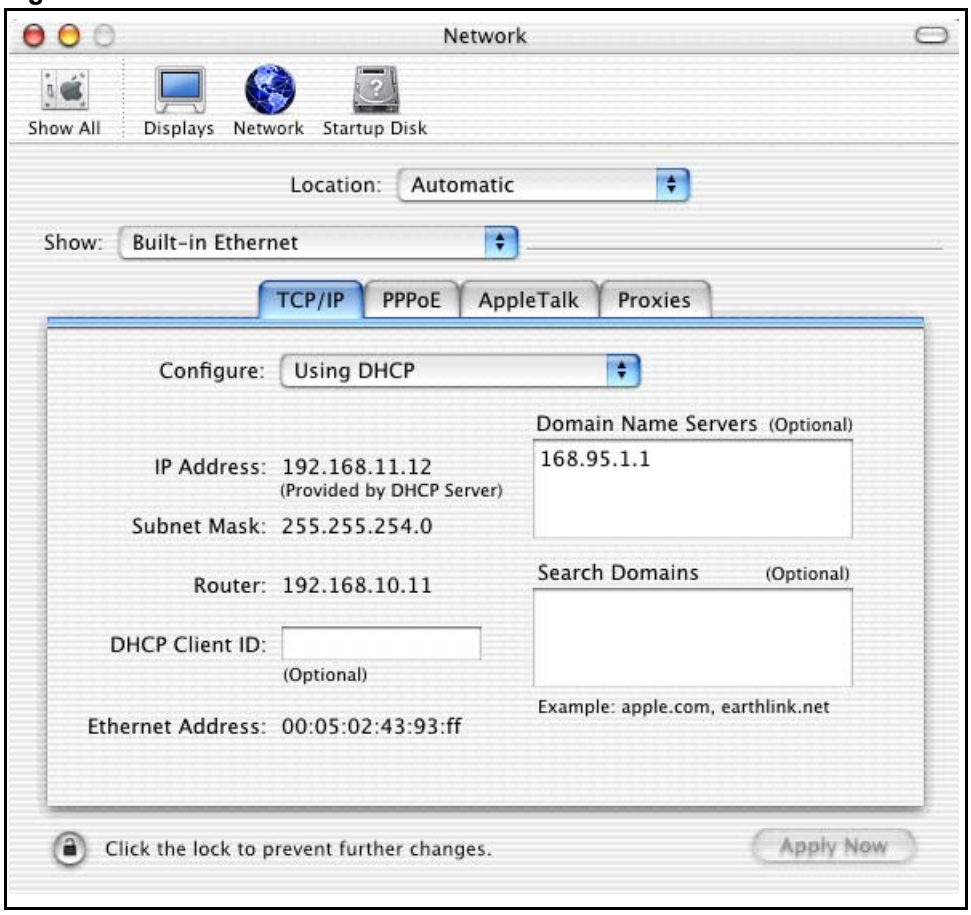


2 Click **Network** in the icon bar.

- Select **Automatic** from the **Location** list.
- Select **Built-in Ethernet** from the **Show** list.
- Click the **TCP/IP** tab.

3 For dynamically assigned settings, select **Using DHCP** from the **Configure** list.

Figure 159 Macintosh OS X: Network



4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your ZyWALL in the **Router address** box.

5 Click **Apply Now** and close the window.

6 Turn on your ZyWALL and restart your computer (if prompted).

Verifying Settings

Check your TCP/IP properties in the **Network** window.

Appendix B
IP Subnetting

IP Addressing

Routers "route" based on the network number. The router that delivers the data packet to the correct destination host uses the host ID.

IP Classes

An IP address is made up of four octets (eight bits), written in dotted decimal notation, for example, 192.168.1.1. IP addresses are categorized into different classes. The class of an address depends on the value of its first octet.

- Class "A" addresses have a 0 in the left most bit. In a class "A" address the first octet is the network number and the remaining three octets make up the host ID.
- Class "B" addresses have a 1 in the left most bit and a 0 in the next left most bit. In a class "B" address the first two octets make up the network number and the two remaining octets make up the host ID.
- Class "C" addresses begin (starting from the left) with 1 1 0. In a class "C" address the first three octets make up the network number and the last octet is the host ID.
- Class "D" addresses begin with 1 1 1 0. Class "D" addresses are used for multicasting. (There is also a class "E" address. It is reserved for future use.)

Table 104 Classes of IP Addresses

IP ADDRESS:		OCTET 1	OCTET 2	OCTET 3	OCTET 4
Class A	0	Network number	Host ID	Host ID	Host ID
Class B	10	Network number	Network number	Host ID	Host ID
Class C	110	Network number	Network number	Network number	Host ID

Note: Host IDs of all zeros or all ones are not allowed.

Therefore:

A class "C" network (8 host bits) can have 2^8 –2 or 254 hosts.

A class "B" address (16 host bits) can have 2^{16} –2 or 65534 hosts.

A class "A" address (24 host bits) can have 2^{24} –2 hosts (approximately 16 million hosts).

Since the first octet of a class "A" IP address must contain a "0", the first octet of a class "A" address can have a value of 0 to 127.

Similarly the first octet of a class "B" must begin with "10", therefore the first octet of a class "B" address has a valid range of 128 to 191. The first octet of a class "C" address begins with "110", and therefore has a range of 192 to 223.

Table 105 Allowed IP Address Range By Class

CLASS	ALLOWED RANGE OF FIRST OCTET (BINARY)	ALLOWED RANGE OF FIRST OCTET (DECIMAL)
Class A	**0**0000000 to **0**1111111	0 to 127
Class B	**10**000000 to **10**111111	128 to 191
Class C	**110**00000 to **110**11111	192 to 223
Class D	**1110**0000 to **1110**1111	224 to 239

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). A subnet mask has 32 is a "1" then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is "0" then the corresponding bit in the IP address is part of the host ID.

Subnet masks are expressed in dotted decimal notation just as IP addresses are. The "natural" masks for class A, B and C IP addresses are as follows.

Table 106 "Natural" Masks

CLASS	NATURAL MASK
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Subnetting

With subnetting, the class arrangement of an IP address is ignored. For example, a class C address no longer has to have 24 bits of network number and 8 bits of host ID. With subnetting, some of the host ID bits are converted into network number bits. By convention, subnet masks always consist of a continuous sequence of ones beginning from the left most bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a "/" followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with mask 255.255.255.128.

The following table shows all possible subnet masks for a class "C" address using both notations.

Table 107 Alternative Subnet Mask Notation

SUBNET MASK IP ADDRESS	SUBNET MASK "1" BITS	LAST OCTET BIT VALUE
255.255.255.0	/24	0000 0000
255.255.255.128	/25	1000 0000
255.255.255.192	/26	1100 0000
255.255.255.224	/27	1110 0000
255.255.255.240	/28	1111 0000
255.255.255.248	/29	1111 1000
255.255.255.252	/30	1111 1100

The first mask shown is the class "C" natural mask. Normally if no mask is specified it is understood that the natural mask is being used.

Example: Two Subnets

As an example, you have a class "C" address 192.168.1.0 with subnet mask of 255.255.255.0.

Table 108 Two Subnets Example

	NETWORK NUMBER	HOST ID
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask	255.255.255.	0
Subnet Mask (Binary)	11111111.11111111.11111111.	00000000

The first three octets of the address make up the network number (class "C"). You want to have two separate networks.

Divide the network 192.168.1.0 into two separate subnets by converting one of the host ID bits of the IP address to a network number bit. The "borrowed" host ID bit can be either "0" or "1" thus giving two subnets; 192.168.1.0 with mask 255.255.255.128 and 192.168.1.128 with mask 255.255.255.128.

Note: In the following charts, shaded/bolded last octet bit values indicate host ID bits "borrowed" to form network ID bits. The number of "borrowed" host ID bits determines the number of subnets you can have. The remaining number of host ID bits (after "borrowing") determines the number of hosts you can have on each subnet.

Table 109 Subnet 1

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**0**0000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	**1**0000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 110 Subnet 2

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**1**0000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	**1**0000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

The remaining 7 bits determine the number of hosts each subnet can have. Host IDs of all zeros represent the subnet itself and host IDs of all ones are the broadcast address for that subnet, so the actual number of hosts available on each subnet in the example above is $2^7 - 2$ or 126 hosts for each subnet.

192.168.1.0 with mask 255.255.255.128 is the subnet itself, and 192.168.1.127 with mask 255.255.255.128 is the directed broadcast address for the first subnet. Therefore, the lowest IP address that can be assigned to an actual host for the first subnet is 192.168.1.1 and the highest is 192.168.1.126. Similarly the host ID range for the second subnet is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The above example illustrated using a 25-bit subnet mask to divide a class "C" address space into two subnets. Similarly to divide a class "C" address into four subnets, you need to "borrow" two host ID bits to give four possible combinations of 00, 01, 10 and 11. The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192. Each subnet contains 6 host ID bits, giving 2^6-2 or 62 hosts for each subnet (all 0's is the subnet itself, all 1's is the broadcast address on the subnet).

Table 111 Subnet 1

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 112 Subnet 2

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 113 Subnet 3

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 114 Subnet 4

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example Eight Subnets

Similarly use a 27-bit mask to create 8 subnets (001, 010, 011, 100, 101, 110).

The following table shows class C IP address last octet values for each subnet.

Table 115 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

The following table is a summary for class "C" subnet planning.

Table 116 Class C Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

Subnetting With Class A and Class B Networks.

For class "A" and class "B" addresses the subnet mask also determines which bits are part of the network number and which are part of the host ID.

A class "B" address has two host ID octets available for subnetting and a class "A" address has three host ID octets (see Table 104 on page 281) available for subnetting.

The following table is a summary for class "B" subnet planning.

Table 117 Class B Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Appendix C PPPoE

PPPoE in Action

An ADSL modem bridges a PPP session over Ethernet (PPP over Ethernet, RFC 2516) from your computer to an ATM PVC (Permanent Virtual Circuit) which connects to a DSL Access Concentrator where the PPP session terminates (see Figure 160 on page 290). One PVC can support any number of PPP sessions from your LAN. PPPoE provides access control and billing functionality in a manner similar to dial-up services using PPP.

Benefits of PPPoE

PPPoE offers the following benefits:

It provides you with a familiar dial-up networking (DUN) user interface.

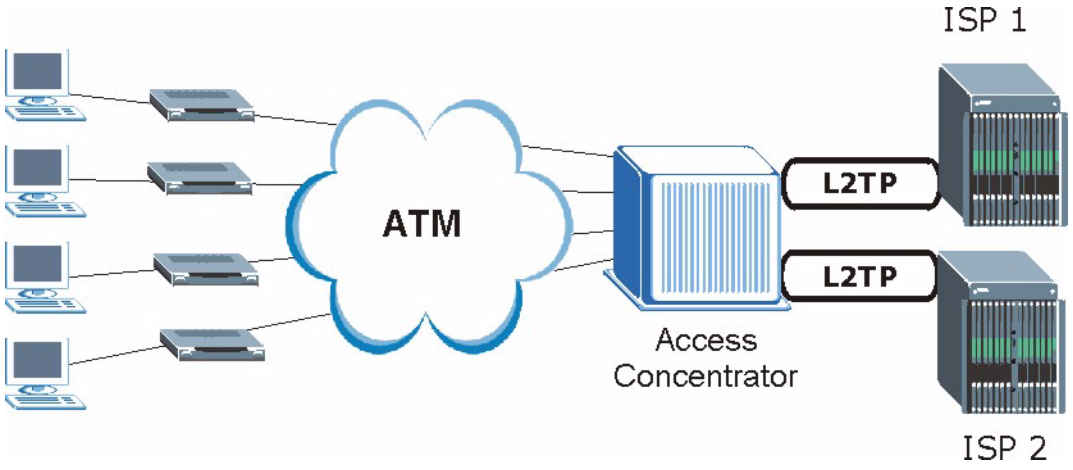
It lessens the burden on the carriers of provisioning virtual circuits all the way to the ISP on multiple switches for thousands of users. For GSTN (PSTN and ISDN), the switching fabric is already in place.

It allows the ISP to use the existing dial-up model to authenticate and (optionally) to provide differentiated services.

Traditional Dial-up Scenario

The following diagram depicts a typical hardware configuration where the computers use traditional dial-up networking.

Figure 160 Single-Computer per Router Hardware Configuration



How PPPoE Works

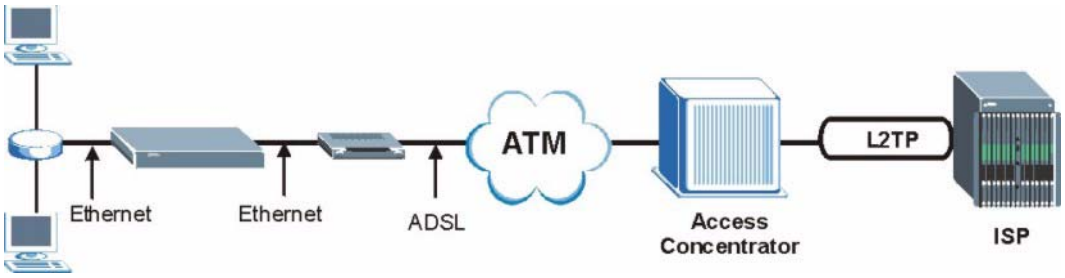
The PPPoE driver makes the Ethernet appear as a serial link to the computer and the computer runs PPP over it, while the modem bridges the Ethernet frames to the Access Concentrator (AC). Between the AC and an ISP, the AC is acting as a L2TP (Layer 2 Tunneling Protocol) LAC (L2TP Access Concentrator) and tunnels the PPP frames to the ISP. The L2TP tunnel is capable of carrying multiple PPP sessions.

With PPPoE, the VC (Virtual Circuit) is equivalent to the dial-up connection and is between the modem and the AC, as opposed to all the way to the ISP. However, the PPP negotiation is between the computer and the ISP.

ZyWALL as a PPPoE Client

When using the ZyWALL as a PPPoE client, the computers on the LAN see only Ethernet and are not aware of PPPoE. This alleviates the administrator from having to manage the PPPoE clients on the individual computers.

Figure 161 ZyWALL as a PPPoE Client



Appendix D
PPTP

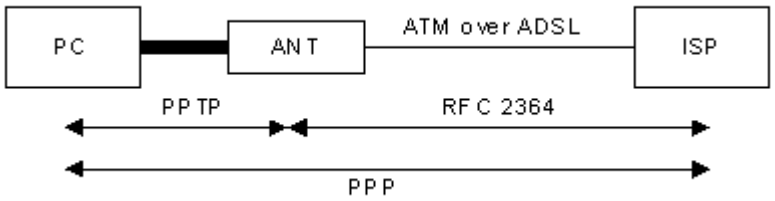
What is PPTP?

PPTP (Point-to-Point Tunneling Protocol) is a Microsoft proprietary protocol (RFC 2637 for PPTP is informational only) to tunnel PPP frames.

How can we transport PPP frames from a computer to a broadband modem over Ethernet?

A solution is to build PPTP into the ANT (ADSL Network Termination) where PPTP is used only over the short haul between the computer and the modem over Ethernet. For the rest of the connection, the PPP frames are transported with PPP over AAL5 (RFC 2364) The PPP connection, however, is still between the computer and the ISP. The various connections in this setup are depicted in the following diagram. The drawback of this solution is that it requires one separate ATM VC per destination.

Figure 162 Transport PPP frames over Ethernet



PPTP and the ZyWALL

When the ZyWALL is deployed in such a setup, it appears as a computer to the ANT.

In Windows VPN or PPTP Pass-Through feature, the PPTP tunneling is created from Windows 95, 98 and NT clients to an NT server in a remote location. The pass-through feature allows users on the network to access a different remote server using the ZyWALL's Internet connection. In SUA/NAT mode, the ZyWALL is able to pass the PPTP packets to the internal PPTP server (i.e. NT server) behind the NAT. You need to configure port forwarding for port 1723 to have the ZyWALL forward PPTP packets to the server. In the case above as the remote PPTP Client initializes the PPTP connection, the user must configure the PPTP clients. The ZyWALL initializes the PPTP connection hence; there is no need to configure the remote PPTP clients.

PPTP Protocol Overview

PPTP is very similar to L2TP, since L2TP is based on both PPTP and L2F (Cisco's Layer 2 Forwarding). Conceptually, there are three parties in PPTP, namely the PNS (PPTP Network Server), the PAC (PPTP Access Concentrator) and the PPTP user. The PNS is the box that hosts both the PPP and the PPTP stacks and forms one end of the PPTP tunnel. The PAC is the box that dials/answers the phone calls and relays the PPP frames to the PNS. The PPTP user is not necessarily a PPP client (can be a PPP server too). Both the PNS and the PAC must have IP connectivity; however, the PAC must in addition have dial-up capability. The phone call is between the user and the PAC and the PAC tunnels the PPP frames to the PNS. The PPTP user is unaware of the tunnel between the PAC and the PNS.

Figure 163 PPTP Protocol Overview

Microsoft includes PPTP as a part of the Windows OS. In Microsoft's implementation, the computer, and hence the ZyWALL, is the PNS that requests the PAC (the ANT) to place an outgoing call over AAL5 to an RFC 2364 server.

Control & PPP Connections

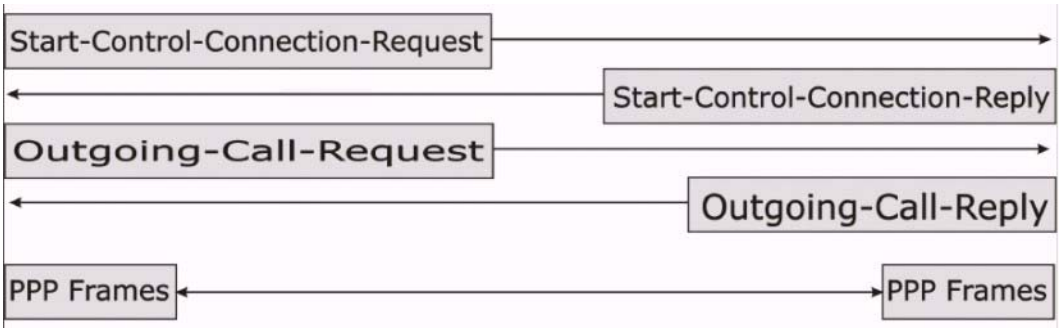
Each PPTP session has distinct control connection and PPP data connection.

Call Connection

The control connection runs over TCP. Similar to L2TP, a tunnel control connection is first established before call control messages can be exchanged. Please note that a tunnel control connection supports multiple call sessions.

The following diagram depicts the message exchange of a successful call setup between a computer and an ANT.

Figure 164 Example Message Exchange between Computer and an ANT



PPP Data Connection

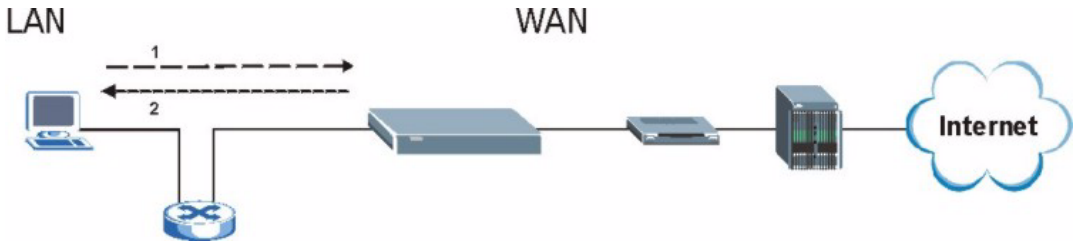
The PPP frames are tunneled between the PNS and PAC over GRE (General Routing Encapsulation, RFC 1701, 1702). The individual calls within a tunnel are distinguished using the Call ID field in the GRE header.

Appendix E
Triangle Route

The Ideal Setup

When the firewall is on, your ZyWALL acts as a secure gateway between your LAN and the Internet. In an ideal network topology, all incoming and outgoing network traffic passes through the ZyWALL to protect your LAN against attacks.

Figure 165 Ideal Setup



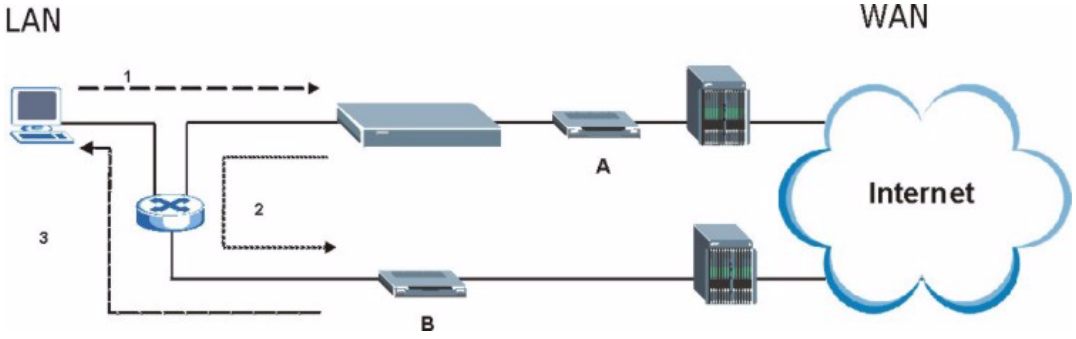
The "Triangle Route" Problem

A traffic route is a path for sending or receiving data packets between two Ethernet devices. Some companies have more than one alternate route to one or more ISPs. If the LAN and ISP(s) are in the same subnet, the "triangle route" problem may occur. The steps below describe the "triangle route" problem.

1. A computer on the LAN initiates a connection by sending out a SYN packet to a receiving server on the WAN.
2. The ZyWALL reroutes the SYN packet through Gateway **B** on the LAN to the WAN.
3. The reply from the WAN goes directly to the computer on the LAN without going through the ZyWALL.

As a result, the ZyWALL resets the connection, as the connection has not been acknowledged.

Figure 166 "Triangle Route" Problem



The "Triangle Route" Solutions

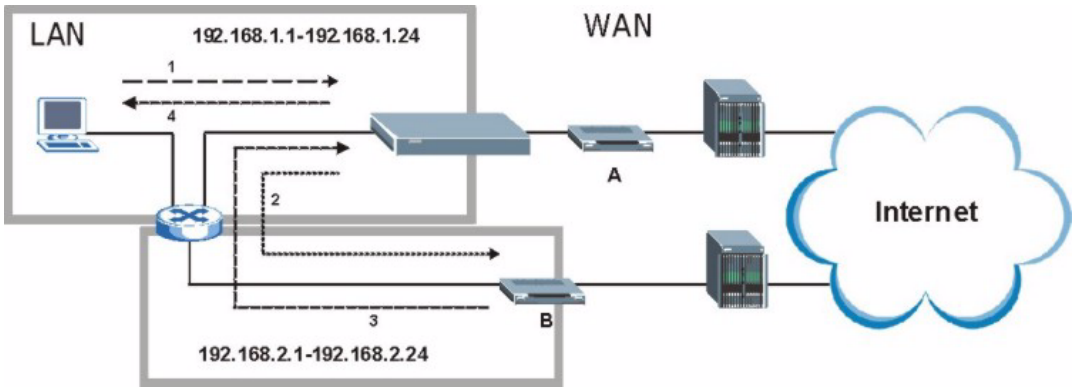
This section presents you two solutions to the "triangle route" problem.

IP Aliasing

IP alias allows you to partition your network into logical sections over the same Ethernet interface. Your ZyWALL supports up to three logical LAN interfaces with the ZyWALL being the gateway for each logical network. By putting your LAN and Gateway **B** 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 B, which is in the 192.168.2.1 to 192.168.2.24 subnet.
3. The reply from WAN goes through the ZyWALL to the computer on the LAN in the 192.168.1.1 to 192.168.1.24 subnet.

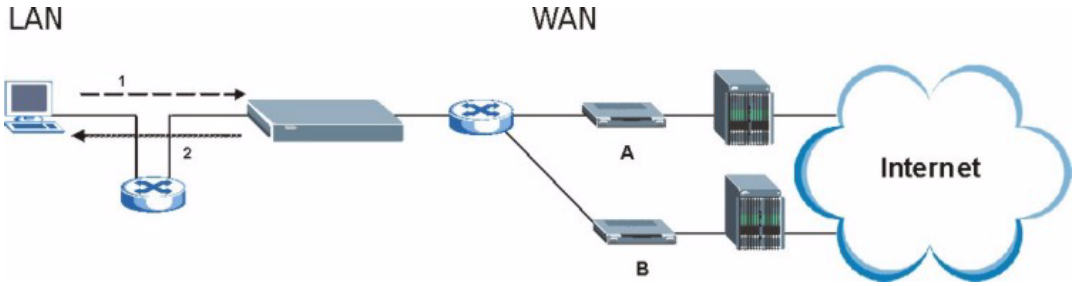
Figure 167 IP Alias



Gateways on the WAN Side

A second solution to the "triangle route" problem is to put all of your network gateways on the WAN side as the following figure shows. This ensures that all incoming network traffic passes through your ZyWALL to your LAN. Therefore your LAN is protected.

Figure 168 Gateways on the WAN Side



How To Configure Triangle Route

1. From the SMT main menu, enter 24.
2. Enter "8" in menu 24 to enter CI command mode.
3. Use the following command to allow triangle route:

```
sys firewall ignore triangle all on
```

or this command to disallow triangle route:

```
sys firewall ignore triangle all off
```

APPENDIX F
SIP Passthrough

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.

SIP Identities

A SIP account uses an identity (sometimes referred to as a SIP address). A complete SIP identity is called a SIP URI (Uniform Resource Identifier). A SIP account's URI identifies the SIP account in a way similar to the way an e-mail address identifies an e-mail account. The format of a SIP identity is SIP-Number@SIP-Service-Domain.

SIP Number

The SIP number is the part of the SIP URI that comes before the "@" symbol. A SIP number can use letters like in an e-mail address (johndoe@your-ITSP.com for example) or numbers like a telephone number (1122334455@VoIP-provider.com for example).

SIP Service Domain

The SIP service domain of the VoIP service provider is the domain name in a SIP URI. For example, if the SIP address is 1122334455@VoIP-provider.com, then "VoIP-provider.com" is the SIP service domain.

SIP Call Progression

The following figure displays the basic steps in the setup and tear down of a SIP call. A calls B.

Table 118 SIP Call Progression

A		B
1. INVITE		
		2. Ringing

Table 118 SIP Call Progression (continued)

A		B
		3. OK
4. ACK		
	5.Dialogue (voice traffic)	
6. BYE		
		7. OK

1. A sends a SIP INVITE request to B. This message is an invitation for B to participate in a SIP telephone call.
2. B sends a response indicating that the telephone is ringing.
3. B sends an OK response after the call is answered.
4. A then sends an ACK message to acknowledge that B has answered the call.
5. Now A and B exchange voice media (talk).
6. After talking, A hangs up and sends a BYE request.
7. B replies with an OK response confirming receipt of the BYE request and the call is terminated.

SIP Servers

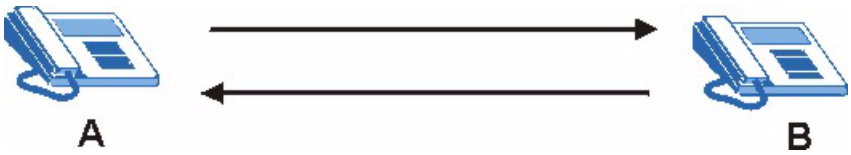
SIP is a client-server protocol. A SIP client is an application program or device that sends SIP requests. A SIP server responds to the SIP requests.

When you use SIP to make a VoIP call, it originates at a client and terminates at a server. A SIP client could be a computer or a SIP phone. One device can act as both a SIP client and a SIP server.

SIP User Agent Server

A SIP user agent server can make and receive VoIP telephone calls. This means that SIP can be used for peer-to-peer communications even though it is a client-server protocol. In the following figure, either A or B can act as a SIP user agent client to initiate a call. A and B can also both act as a SIP user agent server to receive the call.

Figure 169 SIP User Agent Server



SIP Proxy Server

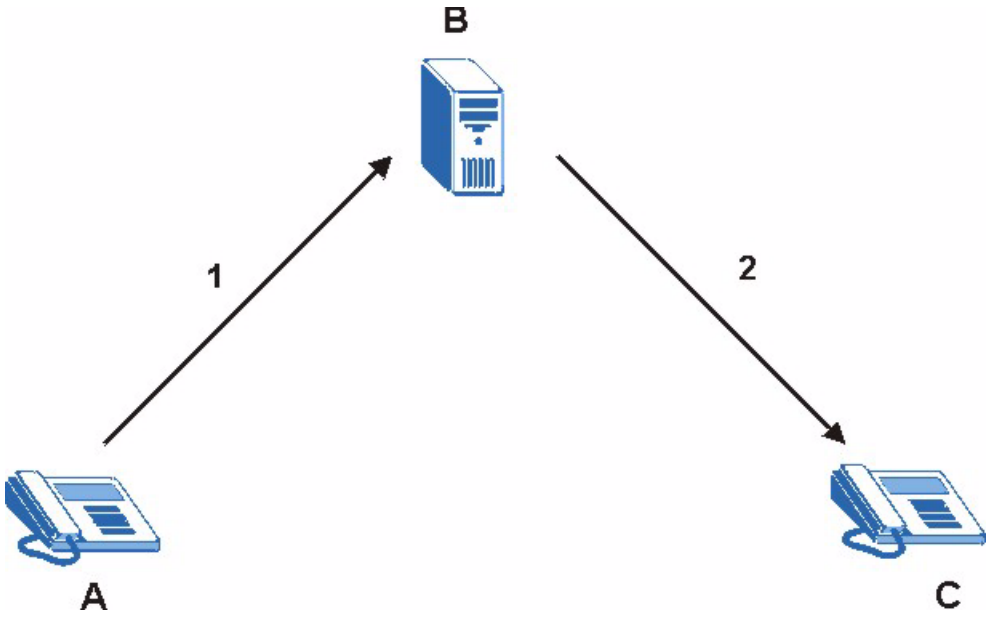
A SIP proxy server receives requests from clients and forwards them to another server.

In the following example, you want to use client device A to call someone who is using client device C.

1 The client device (A in the figure) sends a call invitation to the SIP proxy server (B).

2 The SIP proxy server forwards the call invitation to C.

Figure 170 SIP Proxy Server



SIP Redirect Server

A SIP redirect server accepts SIP requests, translates the destination address to an IP address and sends the translated IP address back to the device that sent the request. Then the client device that originally sent the request can send requests to the IP address that it received back from the redirect server. Redirect servers do not initiate SIP requests.

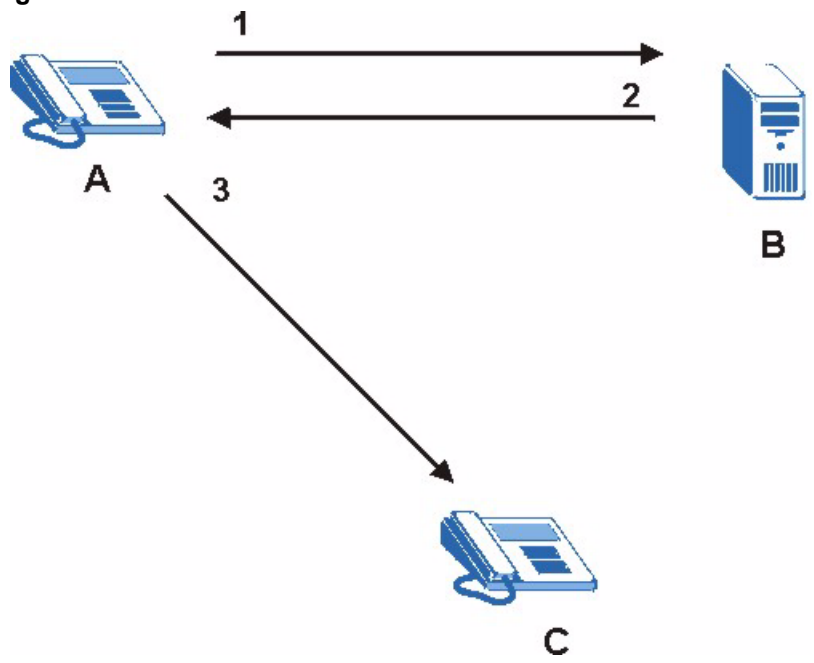
In the following example, you want to use client device A to call someone who is using client device C.

1 Client device A sends a call invitation for C to the SIP redirect server (B).

2 The SIP redirect server sends the invitation back to A with C's IP address (or domain name).

3 Client device A then sends the call invitation to client device C.

Figure 171 SIP Redirect Server



SIP Register Server

A SIP register server maintains a database of SIP identity-to-IP address (or domain name) mapping. The register server checks your user name and password when you register.

RTP

When you make a VoIP call using SIP, the RTP (Real time Transport Protocol) is used to handle voice data transfer. See RFC 1889 for details on RTP.

SIP ALG

Some NAT routers may include a SIP Application Layer Gateway (ALG). A SIP ALG allows VoIP calls to pass through NAT by examining and translating IP addresses embedded in the data stream. When a VoIP device (SIP client) behind the SIP ALG registers with the SIP register server, the SIP ALG translates the device's private IP address inside the SIP data stream to a public IP address. You do not need to use STUN if your VoIP device is behind the SIP ALG.

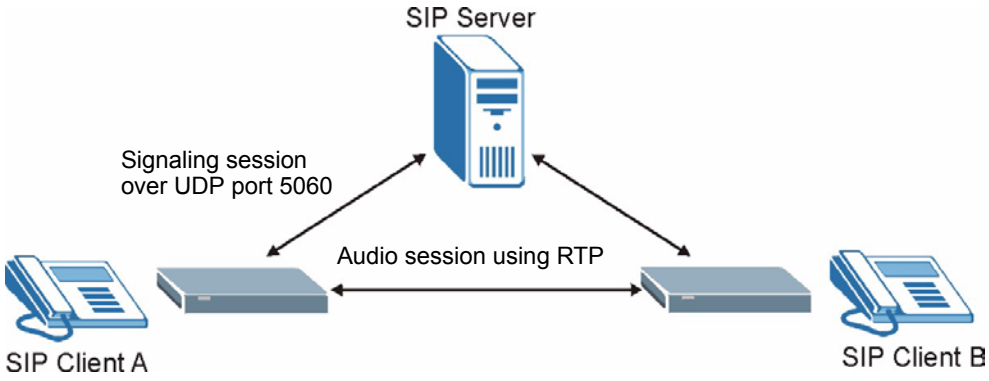
STUN

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.

ZyXEL SIP ALG

- SIP clients can be connected to the LAN, WLAN or DMZ. A SIP server must be on the WAN. The WLAN and DMZ are not available on all models.
- 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.

Figure 172 ZyWALL SIP ALG



SIP ALG and NAT

The ZyWALL dynamically creates an implicit port forwarding rule for SIP traffic from the WAN to the LAN.

The SIP 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**.

SIP ALG and Firewall

The ZyWALL creates an implicit temporary firewall rule for the dynamic RTP port on the WAN to the SIP client device on the LAN. The firewall rule is created for both directions to allow voice packets. The firewall rule is deleted when the call is terminated.

SIP ALG and Multiple WAN

When the ZyWALL has two WAN ports and uses the second highest priority WAN port as a back up, it drops SIP connections when the primary WAN port connection fails. The ZyWALL does not automatically change the SIP connection to the secondary WAN port.

If the primary WAN connection fails, the SIP client needs to re-register with the SIP server through the secondary WAN port to have the SIP connection go through the secondary WAN port.

When the ZyWALL uses both of the WAN ports at the same time, you can configure a routing policy to have the voice traffic from any IP address with UDP port 5060 and the RTP ports go over a specified WAN port.

Enabling/Disabling the SIP ALG

The ZyWALL SIP ALG is turned off by default to avoid retranslating the IP address of an existing SIP device that is using STUN. If you want to use a SIP client device (a SIP phone or IP phone for example) behind the ZyWALL without STUN, use the `ip alg enable ALG_SIP` command to activate the SIP ALG.

Signaling Session Timeout

Most SIP clients have an "expire" mechanism indicating the lifetime of signaling sessions. The SIP UA 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 call during the ZyWALL SIP timeout default (60 minutes), the ZyWALL SIP ALG drops any incoming calls after the timeout period. You can use the `ip alg siptimeout` command to change the timeout value.

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 dorp 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.

Appendix G
VPN Setup

This appendix will help you to quickly create a IPSec/VPN connection between two ZyXEL IPSec routers. It should be considered a quick reference for experienced users.

General Notes

- The private networks behind the IPSec routers must be on different subnets.

  For example, 192.168.**10**.0/24 and 192.168.**20**.0/24.
- If the sites are/were previously connected using a leased line or ISDN router, physically disconnect these devices from the network before testing your new VPN connection. The old route may have been learnt by RIP and would take priority over the new VPN connection.
- To test whether or not a tunnel is working, ping from a computer at one site to a computer at the other.
- Before doing so, ensure that both computers have Internet access (via the IPSec routers).
- You can use the "**E-MAIL**" **Peer Type** and the "**SUBNET**" **Local** and **Remote Address Type** to simplify the configuration.
- Do not manually create any static IP routes for the remote VPN site. They are not required.

Dynamic IPSec Rule

Create a dynamic rule by setting the **Secure Gateway Address** to '0.0.0.0'. A single dynamic rule can support multiple simultaneous incoming IPSec connections.

All users of a dynamic rule have the same pre-shared key. You may need to change the pre-shared key if one of the users leaves. See the support notes at http://www.zyxel.com for configuration examples for software VPN clients.

Full Feature NAT Mode

With **Full Feature** NAT mode, you must map the intended VPN rule's local policy addresses as the Inside Local Address (ILA) to a public IP address assigned by the ISP (an Inside Global Address or IGA) before you can configure the VPN rule. For example, you could create a One-to-One address mapping rule that maps the VPN rule's local policy addresses as the ILA to the VPN rule's my IP address as the IGA.

You may have to specify the public IP address in the **My IP Addr** field of the local IPSec rule. If you have not configured the address mapping properly, a "SPD doesn't match configuration of NAT" message displays when you try to save the IPSec rule.

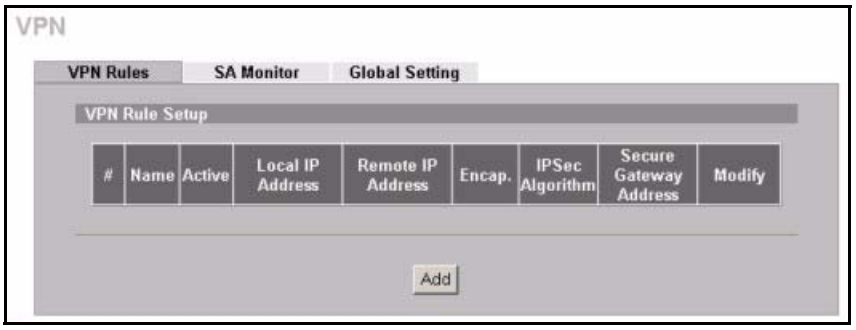
The following pages show a typical configuration that builds a tunnel between two private networks. One network is the headquarters (HQ) and the other is a branch office. Both sites have static (fixed) public addresses. Replace the **Secure Gateway Address** and **Local/ Remote IP Address Start** settings with your own values.

VPN Configuration via Web Configurator

This section gives a VPN rule configuration example using the web configurator.

1 Click **VPN** to display the following screen. Click the **Add** button.

Figure 173 VPN Rules



2 Configure the screens in the headquarters and the branch office as follows and click **Apply**.
The pre-shared key must be exactly the same on both IPSec routers. Use a simple key and/or copy and paste the setting into the other IPSec router to avoid typos.

Figure 174 Headquarters VPN Rule Edit

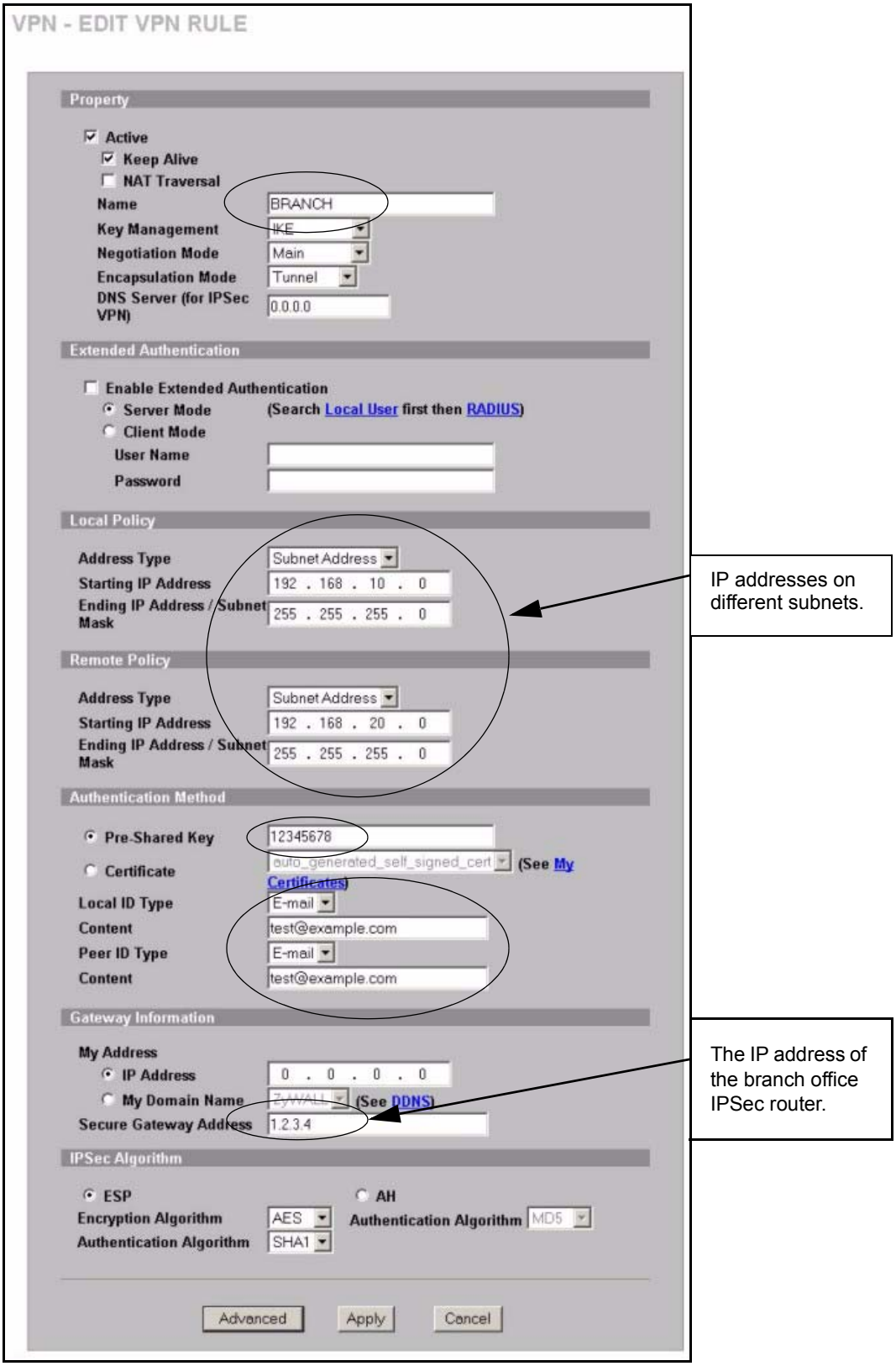
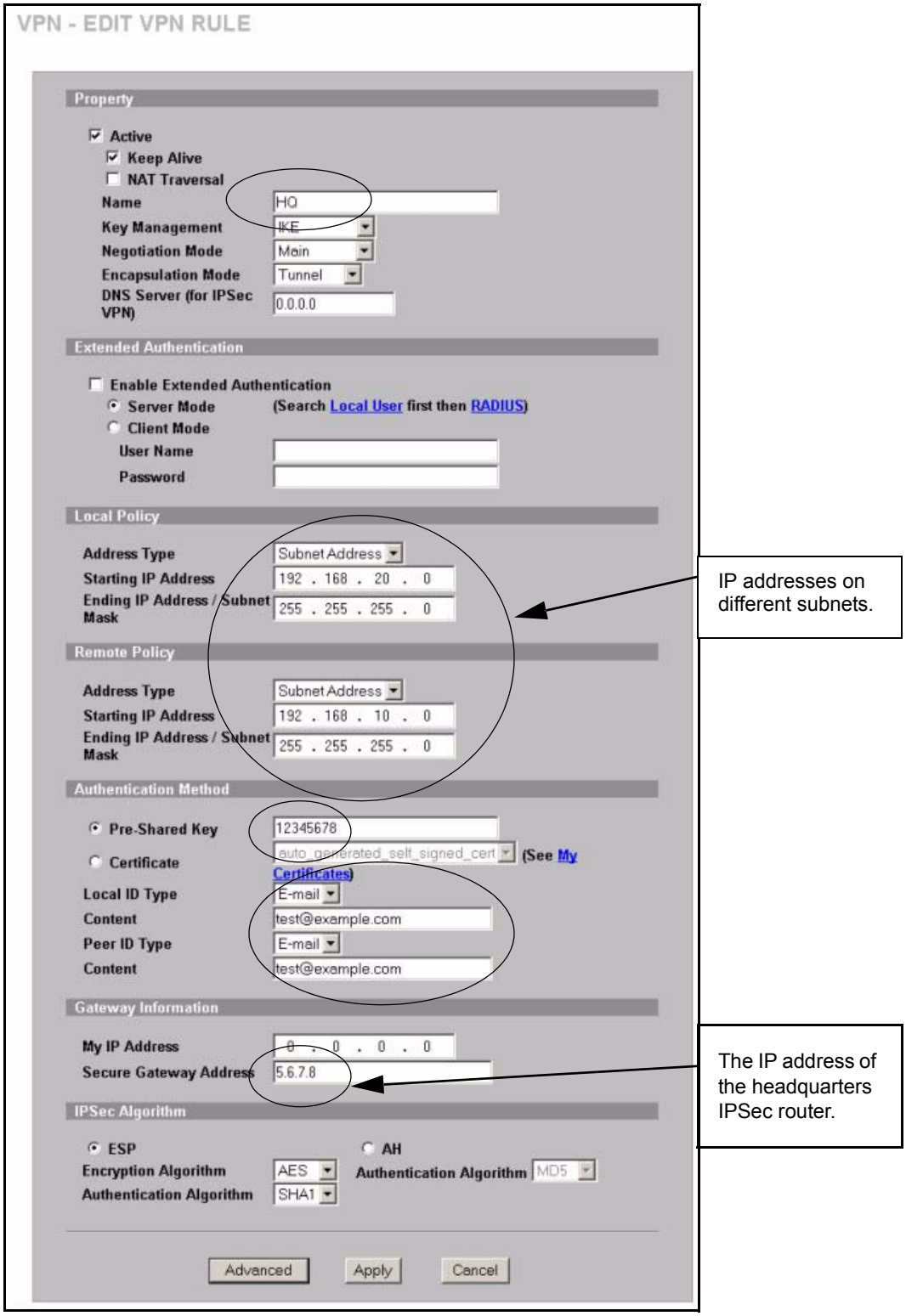


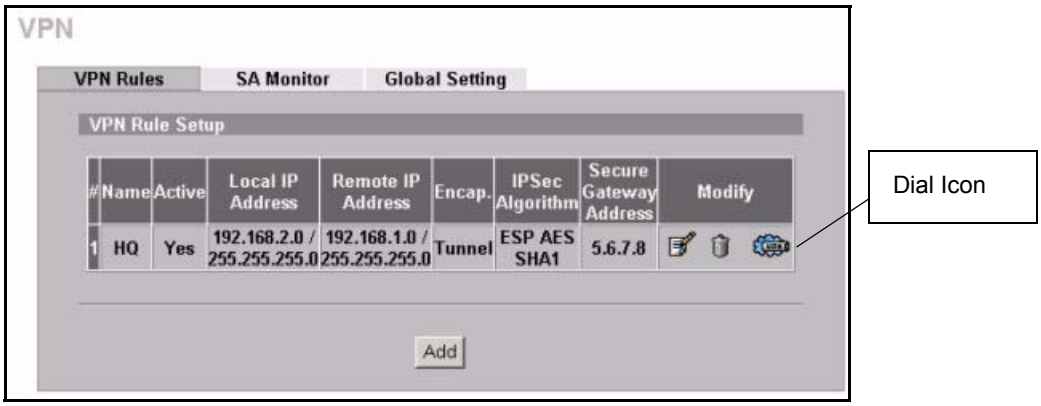
Figure 175 Branch Office VPN Rule Edit



Dialing the VPN Tunnel via Web Configurator

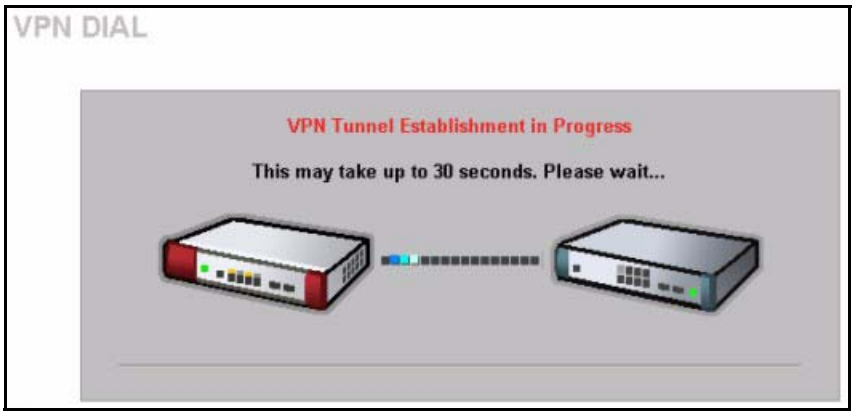
To test whether the IPSec routers can build the VPN tunnel, click the dial icon in the **VPN Rules** screen's **Modify** column to have the IPSec routers set up the tunnel.[1]

Figure 176 VPN Rule Configured



The following screen displays.

Figure 177 VPN Dial



This screen displays later if the IPSec routers can build the VPN tunnel.

1. This feature is not available on all ZyWALL models.

Figure 178 VPN Tunnel Established

VPN Configuration via SMT

This section gives a VPN rule configuration example using the SMT.

1 From the main menu, enter 27 to display the first VPN menu (shown next).

Figure 179 Menu 27: VPN/IPSec Setup

```
                Menu 27 - VPN/IPSec Setup

                          1. IPSec Summary
                          2. SA Monitor



            Enter Menu Selection Number:
```

2 Type 1 in menu 27 and then press [ENTER] to display **Menu 27.1 — IPSec Summary**. This is a summary read-only menu of your IPSec rules (tunnels). Select **Edit** in the **Select Command** field; type the index number of a rule in the **Select Rule** field and press [ENTER].

Figure 180 Menu 27.1: IPSec Summary

```
                          Menu 27.1 - IPSec Summary
 #     Name   A Local Addr Start  - Addr End / Mask   Encap  IPSec Algorithm
Key Mgt     Remote Addr Start - Addr End / Mask          Secure Gw Addr
--- ---------- - -----------------   ----------------- ------ --------------
 001

 002

 003

 004

 005


              Select Command=  None          Select Rule=  N/A

                    Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

3 Configure the rules in the headquarters and the branch office as follows.

Figure 181 Headquarters Menu 27.1.1: IPSec Setup

```
                            Menu 27.1.1 - IPSec Setup

          Index #= 1        Name= BRANCH
          Active= Yes       Keep Alive= Yes   Nat Traversal= No
          Local ID type= E-MAIL     Content= test@example.com
          My IP Addr= 0.0.0.0
          Peer ID type= E-MAIL      Content= test@example.com
          Secure Gateway Address= 1.2.3.4
          Protocol= 0       DNS Server= 0.0.0.0
          Local:  Addr Type= SUBNET
              IP Addr Start= 192.168.10.0     End/Subnet Mask= 255.255.255.0
                 Port Start= 0                End= N/A
          Remote: Addr Type= SUBNET
              IP Addr Start= 192.168.20.0     End/Subnet Mask= 255.255.255.0
                 Port Start= 0                End= N/A
          Enable Replay Detection= No
          Key Management= IKE
          Edit Key Management Setup= No

                    Press ENTER to Confirm or ESC to Cancel:
Press ENTER to Confirm or ESC to Cancel:
```

Note: Press [ENTER] at the bottom of each screen to save your configuration.

You can press the 'Up' arrow at the top of a menu to quickly reach the bottom of the menu.

Figure 182 Branch Office Menu 27.1.1: IPSec Setup

```
                            Menu 27.1.1 - IPSec Setup

          Index #= 1        Name= HQ
          Active= Yes       Keep Alive= Yes   Nat Traversal= No
          Local ID type= E-MAIL     Content= test@example.com
          My Addr Type= IP          Address= 0.0.0.0
          Peer ID type= E-MAIL      Content= test@example.com
          Secure Gateway Address= 5.6.7.8
          Protocol= 0       DNS Server= 0.0.0.0
          Local:  Addr Type= SUBNET
              IP Addr Start= 192.168.20.0     End/Subnet Mask= 255.255.255.0
                 Port Start= 0                End= N/A
          Remote: Addr Type= SUBNET
              IP Addr Start= 192.168.10.1     End/Subnet Mask= 255.255.255.0
                 Port Start= 0                End= N/A
          Enable Replay Detection= No
          Key Management= IKE
          Edit Key Management Setup= No

                    Press ENTER to Confirm or ESC to Cancel:
Press ENTER to Confirm or ESC to Cancel:
```

4 Move the cursor to the **Edit Key Management Setup** field in **Menu 27.1.1 - IPSec Setup**; press [SPACE BAR] to select **Yes** and then press [ENTER] to display **Menu 27.1.1.1 - IKE Setup**.
Only configure the pre-shared key. Leave the default settings for the other fields.

The pre-shared key must be exactly the same on both IPSec routers. Use a simple key and/or copy and paste the setting into the other IPSec router to avoid typos.

Figure 183 Menu 27.1.1.1: IKE Setup

```
                            Menu 27.1.1.1 - IKE Setup

      Phase 1
        Negotiation Mode= Main
        Authentication Method= Pre-Shared Key
        PSK= 12345678
        Certificate= N/A
        Encryption Algorithm= DES
        Authentication Algorithm= MD5
        SA Life Time (Seconds)= 28800
        Key Group= DH1
      Phase 2
        Active Protocol= ESP
        Encryption Algorithm= DES
        Authentication Algorithm= SHA1
        SA Life Time (Seconds)= 28800
        Encapsulation= Tunnel
        Perfect Forward Secrecy (PFS)= None

                     Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.
```

Dialing the VPN Tunnel via SMT

If you would like to test whether the IPSec devices can build the IPSec tunnel before trying to ping a computer, use the '**ipsec dial n**' (where "n" is the number of the VPN rule) command from the Command Interpreter - **Menu 24.8** to have the IPSec device set up the tunnel.

Here is an example.

```
Copyright (c) 1994 - 2004 ZyXEL Communications Corp.
ras> ipsec dial 1
Tunnel built successfully!
```

VPN Troubleshooting

If the IPSec tunnel does not build properly, the problem is likely a configuration error at one of the IPSec routers. The following steps will help you to rapidly identify and correct configuration problems.

Log into the SMTs of both ZyXEL IPSec routers via telnet.
Position the telnet windows side-by-side and visually compare the configuration in **Menu 27.1.1** (IPSec Rule) and **Menu 27.1.1.1** (IKE Setup). Check the settings in each field methodically and slowly.

VPN Log

The system log can often help to identify a configuration problem.
Enable IKE & IPSec logging via the web configurator at both ends, clear the log and then build the tunnel.

View the log via the web configurator or type 'sys log disp' from CLI. See Appendix N on page 347 for information on the log messages.

Figure 184 VPN Log Example

```
zw5> sys log disp ike ipsec

#  .time                 source                 destination            notes

    message
  0|09/21/2004 05:45:08 |172.21.3.43           |172.21.3.185          |IKE

    Rule [1] Tunnel built successfully
  1|09/21/2004 05:45:08 |172.21.3.43           |172.21.3.185          |IKE

    Send:[HASH]
  2|09/21/2004 05:45:08 |172.21.3.43           |172.21.3.185          |IKE

    Adjust TCP MSS to 1398
  3|09/21/2004 05:45:07 |172.21.3.185          |172.21.3.43           |IKE

    Recv:[HASH][SA][NONCE][ID][ID]
  4|09/21/2004 05:45:07 |172.21.3.43           |172.21.3.185          |IKE

    Send:[HASH][SA][NONCE][ID][ID]
  5|09/21/2004 05:45:07 |172.21.3.43           |172.21.3.185          |IKE

    Start Phase 2: Quick Mode
  6|09/21/2004 05:45:07 |172.21.3.43           |172.21.3.185          |IKE

    Phase 1 IKE SA process done
  7|09/21/2004 05:45:07 |172.21.3.185          |172.21.3.43           |IKE

    Recv:[ID][HASH][NOTFY:INIT_CONTACT]
  8|09/21/2004 05:45:07 |172.21.3.43           |172.21.3.185          |IKE

    Send:[ID][HASH][NOTFY:INIT_CONTACT]
  9|09/21/2004 05:45:07 |172.21.3.185          |172.21.3.43           |IKE

    Recv:[KE][NONCE]
 10|09/21/2004 05:45:07 |172.21.3.43           |172.21.3.185          |IKE

    Send:[KE][NONCE]
 11|09/21/2004 05:45:07 |172.21.3.185          |172.21.3.43           |IKE
```

IPSec Debug

If you are having difficulty building an IPSec tunnel to a non-ZyXEL IPSec router, advanced users may wish to examine the IPSec debug feature (**Menu 24.8**).

Figure 185 IKE/IPSec Debug Example

```
ras> ipsec debug
type            level           display
ras> ipsec debug type
<0:Disable | 1:Original on|off | 2:IKE on|off | 3: IPSec [SPI]|on|off |
4:XAUTH on|off | 5:CERT on|off | 6: All>
ras> ipsec debug level
<0:None | 1:User | 2:Low | 3:High>

ras> ipsec debug type 1 on
ras> ipsec debug type 2 on
ras> ipsec debug level 3

Copyright (c) 1994 - 2004 ZyXEL Communications Corp.
ras> ipsec dial 1
Start dialing for tunnel <rule# 1>...
ikeStartNegotiate(): saIndex<0>
peerIp<xxx.xxx.xxx.xxx> protocol: <NONE>(0)
   peer Ip <xxx.xxx.xxx.xxx> initiator(): type<IPSEC_ESP>, exch<Main>
   initiator :
   protocol: IPSEC_ESP, exchange mode: Main mode  find_ipsec_sa():
      find ipsec saNot found
      Not found  isadb_is_outstanding_req():
      Send event to LBN task for DH processLBN task proc event <DH param req>
Main Mode processing done successfully, state=MM wait DH param.
   LBN task proc event <DH param req>genDHParameters(): dh_len=96
      gen DH Parameters : dh_len=96  GenRand: A(secret_val)
      GenRand: A(secret_val) done
      done  lbnTwoExpMod(): elen=48, mlen=48

...
...

Tunnel built successfully!!!
```

Use a VPN Tunnel

A VPN tunnel gives you a secure connection to another computer or network. The **VPN Status** screen displays whether or not your VPN tunnel is connected. Example VPN tunnel uses are securely sending and retrieving files, and accessing corporate network drives, web servers and email. Services work as if you were at the office instead of connected through the Internet.

FTP Example

The following example shows a text-based login from a branch office computer to an FTP server behind the remote IPSec router at headquarters. The server's IP address (192.168.10.33) is in the subnet configured in the **Local Policy** fields in Figure 174 on page 307.

```
C:\Documents and Settings\Administrator>ftp 192.168.10.33
Connected to 192.168.109.33.
220 Serv-U FTP-Server v2.5b for WinSock ready...
User (192.168.109.33:(none)): test
331 User name okay, need password.
Password:
230 User logged in, proceed.
```

Appendix H
Importing Certificates

This appendix shows importing certificates examples using Internet Explorer 5.

Import ZyWALL Certificates into Netscape Navigator

In Netscape Navigator, you can permanently trust the ZyWALL's server certificate by importing it into your operating system as a trusted certification authority.

Select **Accept This Certificate Permanently** in the following screen to do this.

Figure 186 Security Certificate

Importing the ZyWALL's Certificate into Internet Explorer

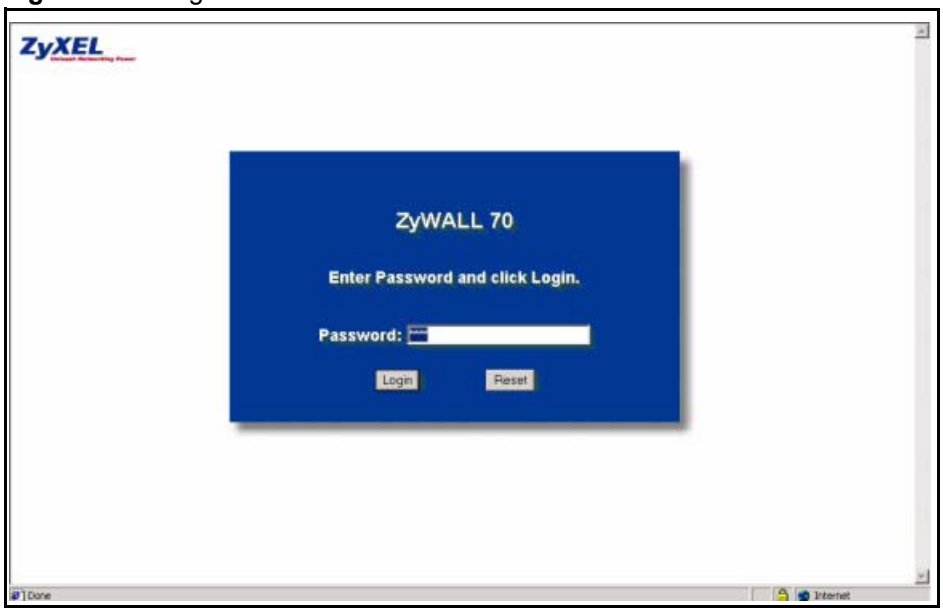
For Internet Explorer to trust a self-signed certificate from the ZyWALL, simply import the self-signed certificate into your operating system as a trusted certification authority.

To have Internet Explorer trust a ZyWALL certificate issued by a certificate authority, import the certificate authority's certificate into your operating system as a trusted certification authority.

The following example procedure shows how to import the ZyWALL's (self-signed) server certificate into your operating system as a trusted certification authority.

1 In Internet Explorer, double click the lock shown in the following screen.

Figure 187 Login Screen



2 Click **Install Certificate** to open the **Install Certificate** wizard.

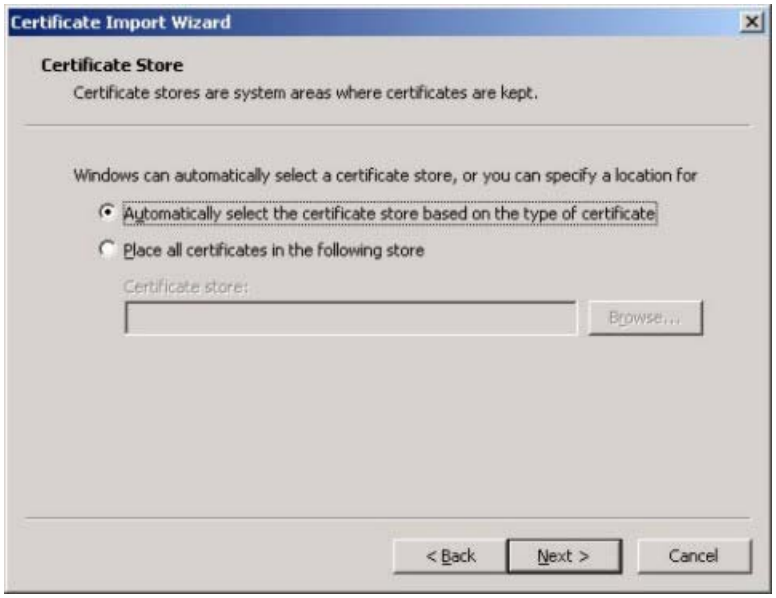
Figure 188 Certificate General Information before Import

3 Click **Next** to begin the **Install Certificate** wizard.

Figure 189 Certificate Import Wizard 1

4 Select where you would like to store the certificate and then click **Next**.

Figure 190 Certificate Import Wizard 2



5 Click **Finish** to complete the **Import Certificate** wizard.

Figure 191 Certificate Import Wizard 3

6 Click **Yes** to add the ZyWALL certificate to the root store.

Figure 192 Root Certificate Store

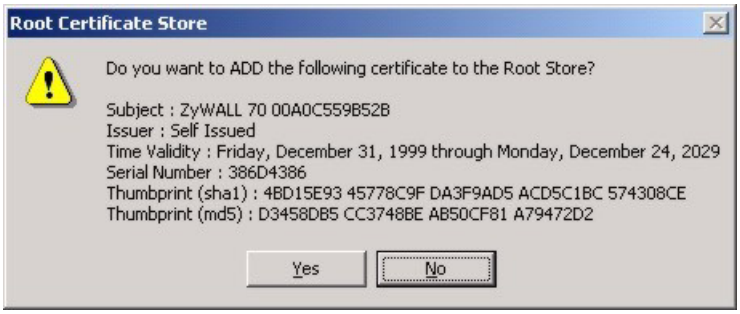
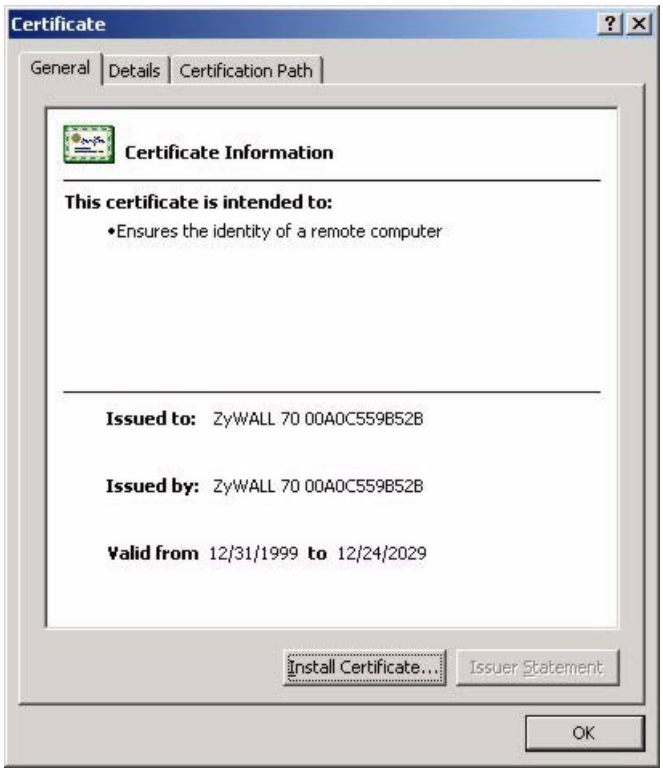


Figure 193 Certificate General Information after Import



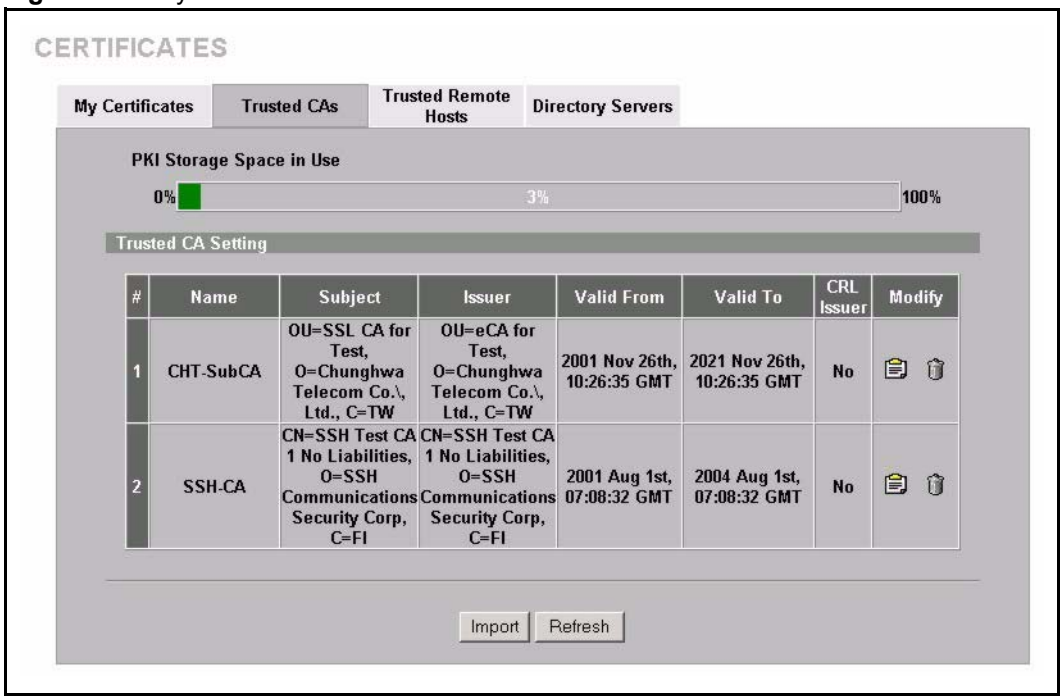
Enrolling and Importing SSL Client Certificates

The SSL client needs a certificate if **Authenticate Client Certificates** is selected on the ZyWALL.

You must have imported at least one trusted CA to the ZyWALL in order for the **Authenticate Client Certificates** to be active (see the Certificates chapter for details).

Apply for a certificate from a Certification Authority (CA) that is trusted by the ZyWALL (see the ZyWALL's **Trusted CA** web configurator screen).

Figure 194 ZyWALL Trusted CA Screen

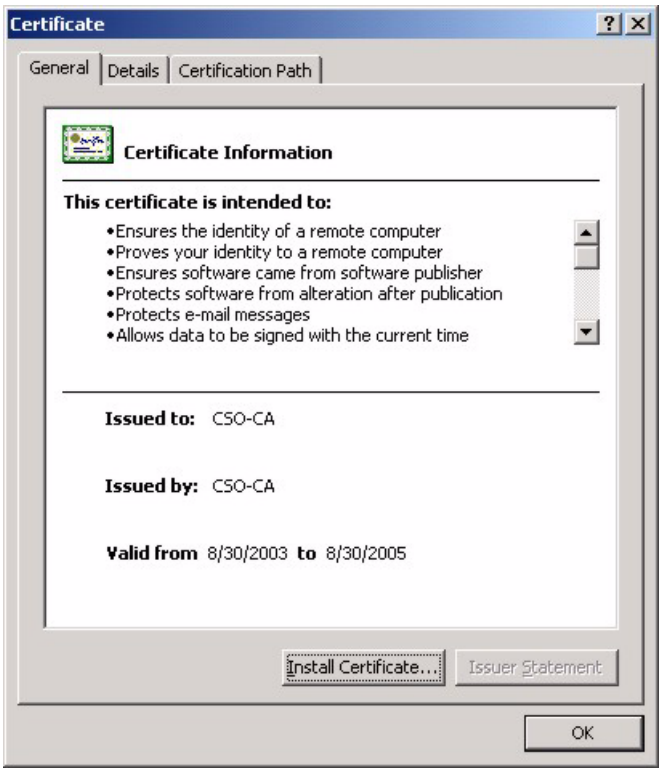


The CA sends you a package containing the CA's trusted certificate(s), your personal certificate(s) and a password to install the personal certificate(s).

Installing the CA's Certificate

1 Double click the CA's trusted certificate to produce a screen similar to the one shown next.

Figure 195 CA Certificate Example



2 Click **Install Certificate** and follow the wizard as shown earlier in this appendix.

Installing Your Personal Certificate(s)

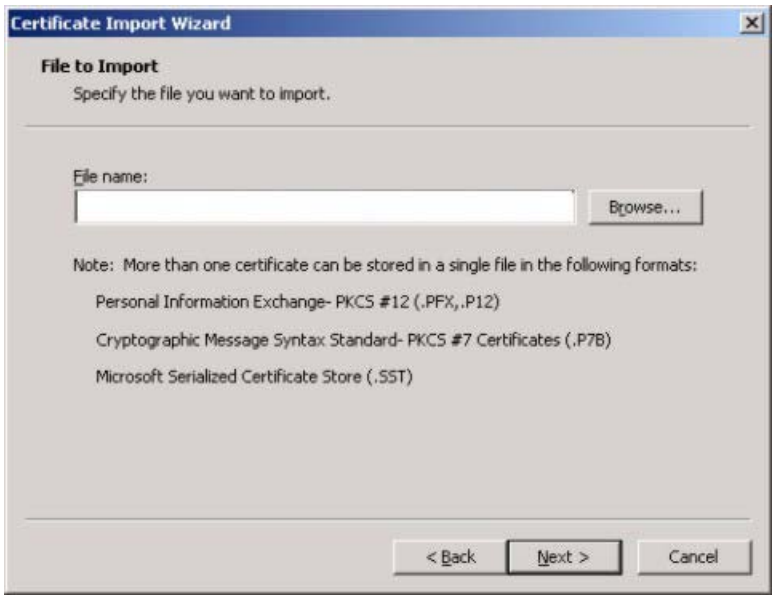
You need a password in advance. The CA may issue the password or you may have to specify it during the enrollment. Double-click the personal certificate given to you by the CA to produce a screen similar to the one shown next

1 Click **Next** to begin the wizard.

Figure 196 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 197 Personal Certificate Import Wizard 2

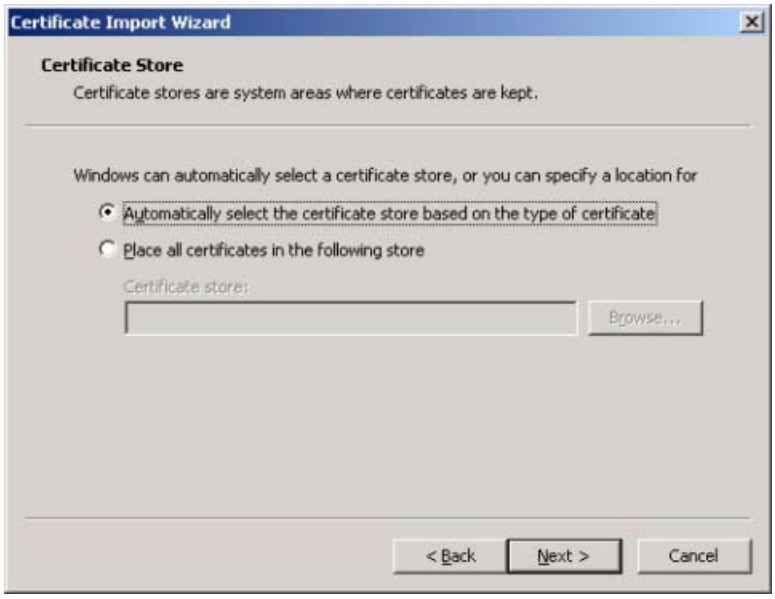


3 Enter the password given to you by the CA.

Figure 198 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 199 Personal Certificate Import Wizard 4



5 Click **Finish** to complete the wizard and begin the import process.

Figure 200 Personal Certificate Import Wizard 5

6 You should see the following screen when the certificate is correctly installed on your computer.

Figure 201 Personal Certificate Import Wizard 6

Using a Certificate When Accessing the ZyWALL Example

Use the following procedure to access the ZyWALL via HTTPS.

1 Enter 'https://ZyWALL IP Address/ in your browser's web address field.

Figure 202 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 203 SSL Client Authentication

3 You next see the ZyWALL login screen.

Figure 204 ZyWALL Secure Login Screen

Appendix I
Command Interpreter

The following describes how to use the command interpreter. Enter 24 in the main menu to bring up the system maintenance menu. Enter 8 to go to **Menu 24.8 - Command Interpreter Mode**. See the included disk or zyxel.com for more detailed information on these commands.

Note: Use of undocumented commands or misconfiguration can damage the unit and possibly render it unusable.

Command Syntax

- The command keywords are in `courier new` font.
- Enter the command keywords exactly as shown, do not abbreviate.
- The required fields in a command are enclosed in angle brackets <>.
- The optional fields in a command are enclosed in square brackets `[]`.
- The `|` symbol means or.

  For example,

  sys filter netbios config <type> <on|off>

  means that you must specify the type of netbios filter and whether to turn it on or off.

Command Usage

A list of valid commands can be found by typing `help` or `?` at the command prompt. Always type the full command. Type `exit` to return to the SMT main menu when finished.

Appendix J
Firewall Commands

The following describes the firewall commands. See Appendix I on page 329 for information on the command structure.

Table 119 Firewall Commands

FUNCTION	COMMAND	DESCRIPTION
FirewallSet-Up		
	`config edit firewall active <yes | no>`	This command turns the firewall on or off.
	`config retrieve firewall`	This command returns the previously saved firewall settings.
	`config save firewall`	This command saves the current firewall settings.
Display		
	`config display firewall`	This command shows the of all the firewall settings including e-mail, attack, and the sets/ rules.
	`config display firewall set <set #>`	This command shows the current configuration of a set; including timeout values, name, default-permit, and etc.If you don't put use a number (#) after "set", information about all of the sets/rules appears.
	`config display firewall set <set #> rule <rule #>`	This command shows the current entries of a rule in a firewall rule set.
	`config display firewall attack`	This command shows all of the attack response settings.
	`config display firewall e-mail`	This command shows all of the e-mail settings.
	`config display firewall ?`	This command shows all of the available firewall sub commands.
Edit		

Table 119 Firewall Commands (continued)

FUNCTION	COMMAND	DESCRIPTION
E-mail	`config edit firewall e-mail mail-server <ip address of mail server>`	This command sets the IP address to which the e-mail messages are sent.
	`config edit firewall e-mail return-addr <e-mail address>`	This command sets the source e-mail address of the firewall e-mails.
	`config edit firewall e-mail email-to <e-mail address>`	This command sets the e-mail address to which the firewall e-mails are sent.
	`config edit firewall e-mail policy <full | hourly | daily | weekly>`	This command sets how frequently the firewall log is sent via e-mail.
	`config edit firewall e-mail day <sunday | monday | tuesday | wednesday | thursday | friday | saturday>`	This command sets the day on which the current firewall log is sent through e-mail if the ZyWALL is set to send it on a weekly basis.
	`config edit firewall e-mail hour <0-23>`	This command sets the hour when the firewall log is sent through e- mail if the ZyWALL is set to send it on an hourly, daily or weekly basis.
	`config edit firewall e-mail minute <0-59>`	This command sets the minute of the hour for the firewall log to be sent via e- mail if the ZyWALL is set to send it on a hourly, daily or weekly basis.
Attack	`config edit firewall attack send-alert <yes | no>`	This command enables or disables the immediate sending of DOS attack notification e-mail messages.
	`config edit firewall attack block <yes | no>`	Set this command to yes to block new traffic after the tcp-max-incomplete threshold is exceeded. Set it to no to delete the oldest half-open session when traffic exceeds the tcp-max-incomplete threshold.
	`config edit firewall attack block-minute <0-255>`	This command sets the number of minutes for new sessions to be blocked when the tcp-max-incomplete threshold is reached. This command is only valid when block is set to yes.

Table 119 Firewall Commands (continued)

FUNCTION	COMMAND	DESCRIPTION
	`config edit firewall attack minute-high <0-255>`	This command sets the threshold rate of new half-open sessions per minute where the ZyWALL starts deleting old half-opened sessions until it gets them down to the minute-low threshold.
	`config edit firewall attack minute-low <0-255>`	This command sets the threshold of half-open sessions where the ZyWALL stops deleting half-opened sessions.
	`config edit firewall attack max-incomplete-high <0-255>`	This command sets the threshold of half-open sessions where the ZyWALL starts deleting old half-opened sessions until it gets them down to the max incomplete low.
	`config edit firewall attack max-incomplete-low <0-255>`	This command sets the threshold where the ZyWALL stops deleting half-opened sessions.
	`config edit firewall attack tcp-max-incomplete <0-255>`	This command sets the threshold of half-open TCP sessions with the same destination where the ZyWALL starts dropping half-open sessions to that destination.
Sets	`config edit firewall set <set #> name <desired name>`	This command sets a name to identify a specified set.
	`Config edit firewall set <set #> default-permit <forward | block>`	This command sets whether a packet is dropped or allowed through, when it does not meet a rule within the set.
	`Config edit firewall set <set #> icmp-timeout <seconds>`	This command sets the time period to allow an ICMP session to wait for the ICMP response.
	`Config edit firewall set <set #> udp-idle-timeout <seconds>`	This command sets how long a UDP connection is allowed to remain inactive before the ZyWALL considers the connection closed.
	`Config edit firewall set <set #> connection-timeout <seconds>`	This command sets how long ZyWALL waits for a TCP session to be established before dropping the session.
	`Config edit firewall set <set #> fin-wait-timeout <seconds>`	This command sets how long the ZyWALL leaves a TCP session open after the firewall detects a FIN-exchange (indicating the end of the TCP session).

Table 119 Firewall Commands (continued)

FUNCTION	COMMAND	DESCRIPTION
	`Config edit firewall set <set #> tcp-idle-timeout <seconds>`	This command sets how long ZyWALL lets an inactive TCP connection remain open before considering it closed.
	`Config edit firewall set <set #> log <yes | no>`	This command sets whether or not the ZyWALL creates logs for packets that match the firewall's default rule set.
Rules	`Config edit firewall set <set #> rule <rule #> permit <forward | block>`	This command sets whether packets that match this rule are dropped or allowed through.
	`Config edit firewall set <set #> rule <rule #> active <yes | no>`	This command sets whether a rule is enabled or not.
	`Config edit firewall set <set #> rule <rule #> protocol <integer protocol value >`	This command sets the protocol specification number made in this rule for ICMP.
	`Config edit firewall set <set #> rule <rule #> log <none | match | not-match | both>`	This command sets the ZyWALL to log traffic that matches the rule, doesn't match, both or neither.
	`Config edit firewall set <set #> rule <rule #> alert <yes | no>`	This command sets whether or not the ZyWALL sends an alert e-mail when a DOS attack or a violation of a particular rule occurs.
	`config edit firewall set <set #> rule <rule #> srcaddr-single <ip address>`	This command sets the rule to have the ZyWALL check for traffic with this individual source address.
	`config edit firewall set <set #> rule <rule #> srcaddr-subnet <ip address> <subnet mask>`	This command sets a rule to have the ZyWALL check for traffic from a particular subnet (defined by IP address and subnet mask).
	`config edit firewall set <set #> rule <rule #> srcaddr-range <start ip address> <end ip address>`	This command sets a rule to have the ZyWALL check for traffic from this range of addresses.
	`config edit firewall set <set #> rule <rule #> destaddr-single <ip address>`	This command sets the rule to have the ZyWALL check for traffic with this individual destination address.

Table 119 Firewall Commands (continued)

FUNCTION	COMMAND	DESCRIPTION
	`config edit firewall set <set #> rule <rule #> destaddr-subnet <ip address> <subnet mask>`	This command sets a rule to have the ZyWALL check for traffic with a particular subnet destination (defined by IP address and subnet mask).
	`config edit firewall set <set #> rule <rule #> destaddr-range <start ip address> <end ip address>`	This command sets a rule to have the ZyWALL check for traffic going to this range of addresses.
	`config edit firewall set <set #> rule <rule #> TCP destport-single  <port #>`	This command sets a rule to have the ZyWALL check for TCP traffic with this destination address. You may repeat this command to enter various, non-consecutive port numbers.
	`config edit firewall set <set #> rule <rule #> TCP destport-range <start port #> <end port #>`	This command sets a rule to have the ZyWALL check for TCP traffic with a destination port in this range.
	`config edit firewall set <set #> rule <rule #> UDP destport-single  <port #>`	This command sets a rule to have the ZyWALL check for UDP traffic with this destination address. You may repeat this command to enter various, non-consecutive port numbers.
	`config edit firewall set <set #> rule <rule #> UDP destport-range <start port #> <end port #>`	This command sets a rule to have the ZyWALL check for UDP traffic with a destination port in this range.
Delete		
	`config delete firewall e-mail`	This command removes all of the settings for e-mail alert.
	`config delete firewall attack`	This command resets all of the attack response settings to their defaults.
	`config delete firewall set <set #>`	This command removes the specified set from the firewall configuration.
	`config delete firewall set <set #> rule<rule #>`	This command removes the specified rule in a firewall configuration set.

Appendix K
NetBIOS Filter Commands

The following describes the NetBIOS packet filter commands. See Appendix I on page 329 for information on the command structure.

Introduction

NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast 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.

You can configure NetBIOS filters to do the following :

- Allow or disallow the sending of NetBIOS packets from the LAN to the WAN and from the WAN to the LAN.
- Allow or disallow the sending of NetBIOS packets from the LAN to the DMZ and from the DMZ to the LAN.
- Allow or disallow the sending of NetBIOS packets from the WAN to the DMZ and from the DMZ to the WAN.
- Allow or disallow the sending of NetBIOS packets through VPN connections.
- Allow or disallow NetBIOS packets to initiate calls.

Display NetBIOS Filter Settings

Syntax: `sys filter netbios disp`

This command gives a read-only list of the current NetBIOS filter modes for The ZyWALL.

NetBIOS Display Filter Settings Command Example

```
=========== NetBIOS Filter Status ===========
        Between LAN and WAN: Block
        Between LAN and DMZ: Block
        Between WAN and DMZ: Block
        IPSec Packets: Forward
        Trigger Dial: Disabled
```

The filter types and their default settings are as follows.

Table 120 NetBIOS Filter Default Settings

NAME	DESCRIPTION	EXAMPLE
Between LAN and WAN	This field displays whether NetBIOS packets are blocked or forwarded between the LAN and the WAN.	Block
Between LAN and DMZ	This field displays whether NetBIOS packets are blocked or forwarded between the LAN and the DMZ.	Block
Between WAN and DMZ	This field displays whether NetBIOS packets are blocked or forwarded between the WAN and the DMZ.	Block
IPSec Packets	This field displays whether NetBIOS packets sent through a VPN connection are blocked or forwarded.	Forward
Trigger dial	This field displays whether NetBIOS packets are allowed to initiate calls. Disabled means that NetBIOS packets are blocked from initiating calls.	Disabled

NetBIOS Filter Configuration

```
Syntax:sys filter netbios config <type> <on|off>
```

where

`<type>` =	Identify which NetBIOS filter (numbered 0-3) to configure. 0 = Between LAN and WAN 1 = Between LAN and DMZ 2 = Between WAN and DMZ 3 = IPSec packet pass through 4 = Trigger Dial
`<on|off>` =	For type 0 and 1, use on to enable the filter and block NetBIOS packets. Use off to disable the filter and forward NetBIOS packets. For type 3, use on to block NetBIOS packets from being sent through a VPN connection. Use off to allow NetBIOS packets to be sent through a VPN connection. For type 4, use on to allow NetBIOS packets to initiate dial backup calls. Use off to block NetBIOS packets from initiating dial backup calls.

Example commands

`sys filter netbios config 0 on`	This command blocks LAN to WAN and WAN to LAN NetBIOS packets.
`sys filter netbios config 1 off`	This command forwards LAN to DMZ and DMZ to LAN NetBIOS packets.

`sys filter netbios config 3 on`	This command blocks IPSec NetBIOS packets.
`sys filter netbios config 4 off`	This command stops NetBIOS commands from initiating calls.

Appendix L
Certificates Commands

The following describes the certificate commands. See Appendix I on page 329 for information on the command structure.

All of these commands start with certificates.

Table 121 Certificates Commands

COMMAND	DESCRIPTION		
my_cert			
	create		
	create	selfsigned <name> <subject> [key size]	Create a self-signed local host certificate. <name> specifies a descriptive name for the generated certificate. <subject> specifies a subject name (required) and alternative name (required). The format is "subject-name-dn;{ip,dns,email}=value". If the name contains spaces, please put it in quotes. [key size] specifies the key size. It has to be an integer from 512 to 2048. The default is 1024 bits.
	create	request <name> <subject> [key size]	Create a certificate request and save it to the router for later manual enrollment. <name> specifies a descriptive name for the generated certification request. <subject> specifies a subject name (required) and alternative name (required). The format is "subject-name-dn;{ip,dns,email}=value". If the name contains spaces, please put it in quotes. [key size] specifies the key size. It has to be an integer from 512 to 2048. The default is 1024 bits.
	create	scep_enroll <name> <CA addr> <CA cert> <auth key> <subject> [key size]	Create a certificate request and enroll for a certificate immediately online using SCEP protocol. <name> specifies a descriptive name for the enrolled certificate. <CA addr> specifies the CA server address. <CA cert> specifies the name of the CA certificate. <auth key> specifies the key used for user authentication. If the key contains spaces, please put it in quotes. To leave it blank, type "". <subject> specifies a subject name (required) and alternative name (required). The format is "subject-name-dn;{ip,dns,email}=value". If the name contains spaces, please put it in quotes. [key size] specifies the key size. It has to be an integer from 512 to 2048. The default is 1024 bits.

Table 121 Certificates Commands (continued)

COMMAND	DESCRIPTION		
	create	cmp_enroll <name> <CA addr> <CA cert> <auth key> <subject> [key size]	Create a certificate request and enroll for a certificate immediately online using CMP protocol. <name> specifies a descriptive name for the enrolled certificate. <CA addr> specifies the CA server address. <CA cert> specifies the name of the CA certificate. <auth key> specifies the id and key used for user authentication. The format is "id:key". To leave the id and key blank, type ":". <subject> specifies a subject name (required) and alternative name (required). The format is "subject-name-dn;{ip,dns,email}=value". If the name contains spaces, please put it in quotes. [key size] specifies the key size. It has to be an integer from 512 to 2048. The default is 1024 bits.
	import	[name]	Import the PEM-encoded certificate from stdin. [name] specifies the descriptive name (optional) as which the imported certificate is to be saved. For my certificate importation to be successful, a certification request corresponding to the imported certificate must already exist on ZyWALL. After the importation, the certification request will automatically be deleted. If a descriptive name is not specified for the imported certificate, the certificate will adopt the descriptive name of the certification request.
	export	<name>	Export the PEM-encoded certificate to stdout for user to copy and paste. <name> specifies the name of the certificate to be exported.
	view	<name>	View the information of the specified local host certificate. <name> specifies the name of the certificate to be viewed.
	verify	<name> [timeout]	Verify the certification path of the specified local host certificate. <name> specifies the name of the certificate to be verified. [timeout] specifies the timeout value in seconds (optional). The default timeout value is 20 seconds.
	delete	<name>	Delete the specified local host certificate. <name> specifies the name of the certificate to be deleted.
	list		List all my certificate names and basic information.
	rename	<old name> <new name>	Rename the specified my certificate. <old name> specifies the name of the certificate to be renamed. <new name> specifies the new name as which the certificate is to be saved.
	def_self_signed	[name]	Set the specified self-signed certificate as the default self-signed certificate. [name] specifies the name of the certificate to be set as the default self-signed certificate. If [name] is not specified, the name of the current self-signed certificate is displayed.

Table 121 Certificates Commands (continued)

COMMAND	DESCRIPTION		
	replace_factory		Create a certificate using your device MAC address that will be specific to this device. The factory default certificate is a common default certificate for all ZyWALL models.
ca_trusted			
	import	<name>	Import the PEM-encoded certificate from stdin. <name> specifies the name as which the imported CA certificate is to be saved.
	export	<name>	Export the PEM-encoded certificate to stdout for user to copy and paste. <name> specifies the name of the certificate to be exported.
	view	<name>	View the information of the specified trusted CA certificate. <name> specifies the name of the certificate to be viewed.
	verify	<name> [timeout]	Verify the certification path of the specified trusted CA certificate. <name> specifies the name of the certificate to be verified. [timeout] specifies the timeout value in seconds (optional). The default timeout value is 20 seconds.
	delete	<name>	Delete the specified trusted CA certificate. <name> specifies the name of the certificate to be deleted.
	list		List all trusted CA certificate names and basic information.
	rename	<old name> <new name>	Rename the specified trusted CA certificate. <old name> specifies the name of the certificate to be renamed. <new name> specifies the new name as which the certificate is to be saved.
	crl_issuer	<name> [on|off]	Specify whether or not the specified CA issues CRL. <name> specifies the name of the CA certificate. [on|off] specifies whether or not the CA issues CRL. If [on|off] is not specified, the current crl_issuer status of the CA.
remote_trusted			
	import	<name>	Import the PEM-encoded certificate from stdin. <name> specifies the name as which the imported remote host certificate is to be saved.
	export	<name>	Export the PEM-encoded certificate to stdout for user to copy and paste. <name> specifies the name of the certificate to be exported.
	view	<name>	View the information of the specified trusted remote host certificate. <name> specifies the name of the certificate to be viewed.
	verify	<name> [timeout]	Verify the certification path of the specified trusted remote host certificate. <name> specifies the name of the certificate to be verified. [timeout] specifies the timeout value in seconds (optional). The default timeout value is 20 seconds.

Table 121 Certificates Commands (continued)

COMMAND	DESCRIPTION		
	delete	<name>	Delete the specified trusted remote host certificate. <name> specifies the name of the certificate to be deleted.
	list		List all trusted remote host certificate names and basic information.
	rename	<old name> <new name>	Rename the specified trusted remote host certificate. <old name> specifies the name of the certificate to be renamed. <new name> specifies the new name as which the certificate is to be saved.
dir_server			
	add	<name> <addr[:port]> [login:pswd]	Add a new directory service. <name> specifies a descriptive name as which the added directory server is to be saved. <addr[:port]> specifies the server address (required) and port (optional). The format is "server-address[:port]". The default port is 389. [login:pswd] specifies the login name and password, if required. The format is "[login:password]".
	delete	<name>	Delete the specified directory service. <name> specifies the name of the directory server to be deleted.
	view	<name>	View the specified directory service. <name> specifies the name of the directory server to be viewed.
	edit	<name> <addr[:port]> [login:pswd]	Edit the specified directory service. <name> specifies the name of the directory server to be edited. <addr[:port]> specifies the server address (required) and port (optional). The format is "server-address[:port]". The default port is 389. [login:pswd] specifies the login name and password, if required. The format is "[login:password]".
	list		List all directory service names and basic information.
	rename	<old name> <new name>	Rename the specified directory service. <old name> specifies the name of the directory server to be renamed. <new name> specifies the new name as which the directory server is to be saved.
cert_manager			
	reinit		Reinitialize the certificate manager.

Appendix M Brute-Force Password Guessing Protection

Brute-force password guessing protection allows you to specify a wait-time that must expire before entering a fourth password after three incorrect passwords have been entered.

The following describes the commands for enabling, disabling and configuring the brute-force password guessing protection mechanism for the password. See Appendix I on page 329 for information on the command structure.

Table 122 Brute-Force Password Guessing Protection Commands

COMMAND	DESCRIPTION
sys pwderrtm	This command displays the brute-force guessing password protection settings.
sys pwderrtm 0	This command turns off the password's protection from brute-force guessing. The brute-force password guessing protection is turned off by default.
sys pwderrtm N	This command sets the password protection to block all access attempts for N (a number from 1 to 60) minutes after the third time an incorrect password is entered.

Example

```
sys pwderrtm 5
```

This command sets the password protection to block all access attempts for five minutes after the third time an incorrect password is entered.

Appendix N
Log Descriptions

This appendix provides descriptions of example log messages.

Table 123 System Maintenance Logs

LOG MESSAGE	DESCRIPTION
`Time calibration is successful`	The router has adjusted its time based on information from the time server.
`Time calibration failed`	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.
`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.

Table 123 System Maintenance Logs (continued)

LOG MESSAGE	DESCRIPTION
`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.

Table 124 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 connection is down.`	A WAN connection is down. You cannot access the network through this interface.

Table 125 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.
`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.

Table 126 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.
`Firewall session time out, sent TCP RST`	The router sent a TCP reset packet when a dynamic firewall session timed out. The default timeout values are as follows: ICMP idle timeout: 3 minutes UDP idle timeout: 3 minutes TCP connection (three way handshaking) timeout: 270 seconds TCP FIN-wait timeout: 2 MSL (Maximum Segment Lifetime set in the TCP header). TCP idle (established) timeout (s): 150 minutes 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 127 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.

Table 128 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. For type and code details, see Table 140 on page 359.
`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. For type and code details, see Table 140 on page 359.
`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 129 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 130 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.

Table 130 PPP Logs (continued)

LOG MESSAGE	DESCRIPTION
`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 131 UPnP Logs

LOG MESSAGE	DESCRIPTION
`UPnP pass through Firewall`	UPnP packets can pass through the firewall.

Table 132 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" checkbox, 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.

Table 132 Content Filtering Logs (continued)

LOG MESSAGE	DESCRIPTION
`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.

Table 133 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. For type and code details, see Table 140 on page 359.
`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. For type and code details, see Table 140 on page 359.
`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. For type and code details, see Table 140 on page 359.
`icmp echo : ICMP (type:%d, code:%d)`	The firewall detected an ICMP echo attack. For type and code details, see Table 140 on page 359.
`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. For type and code details, see Table 140 on page 359.
`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. For type and code details, see Table 140 on page 359.
`traceroute ICMP (type:%d, code:%d)`	The firewall detected an ICMP traceroute attack. For type and code details, see Table 140 on page 359.

Table 134 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.

Table 135 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.
`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.

Table 135 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
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.
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! Username: <Username>	The router used extended authentication to authenticate the listed username.

Table 135 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
`XAUTH fail! Username: <Username>`	The router was not able to use extended authentication to authenticate the listed username.
`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.
`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.

Table 135 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
`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.

Table 136 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.
`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.

Table 136 PKI Logs (continued)

LOG MESSAGE	DESCRIPTION
`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 137 on page 357 for the corresponding descriptions of the codes.

Table 137 Certificate Path Verification Failure Reason 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.
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.

Table 137 Certificate Path Verification Failure Reason Codes (continued)

CODE	DESCRIPTION
26	Database method failed.
27	Path was not verified.
28	Maximum path length reached.

Table 138 802.1X 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.
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.

Table 139 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.

Table 140 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

Table 140 ICMP Notes (continued)

TYPE	CODE	DESCRIPTION
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
16		Information Reply
	0	Information reply message

Table 141 Syslog Logs

LOG MESSAGE	DESCRIPTION
<Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="<msg>" note="<note>" devID="<mac address last three numbers>" 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 various log charts throughout this appendix. The "devID" is the last three characters of the MAC address of the router's LAN port. The "cat" is the same as the category in the router's logs.

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 142 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

Table 142 RFC-2408 ISAKMP Payload Types (continued)

LOG DISPLAY	PAYLOAD TYPE
SIG	Signature
NONCE	Nonce
NOTFY	Notification
DEL	Delete
VID	Vendor ID

Log Commands

Go to the command interpreter interface. Appendix I on page 329 explains how to access and use the commands.

Configuring What You Want the ZyWALL to Log

1. Use the `sys logs load` command to load the log setting buffer that allows you to configure which logs the ZyWALL is to record.
2. Use `sys logs category` to view a list of the log categories (this display varies by model).

Figure 205 Displaying Log Categories Example

```
ras> sys logs category
8021x          access         attack         display
error          icmp           ike            ipsec
javablocked    mten           packetfilter   ppp
cdr            pki            tls            remote
tcpreset       traffic        upnp           urlblocked
urlforward     wireless
```

3. Use `sys logs category` followed by a log category to display the parameters that are available for the category.

Figure 206 Displaying Log Parameters Example

```
ras> sys logs category access
Usage: [0:none/1:log/2:alert/3:both] [0:don't show debug type/
1:show debug type]
```

4. Use `sys logs category` followed by a log category and a parameter to decide what to record.

Use 0 to not record logs for that category, 1 to record only logs for that category, 2 to record only alerts for that category, and 3 to record both logs and alerts for that category. Not every parameter is available with every category.

5 Use the `sys logs save` command to store the settings in the ZyWALL (you must do this in order to record logs).

Displaying Logs

- Use the `sys logs display` command to show all of the logs in the ZyWALL's log.
- Use the `sys logs category display` command to show the log settings for all of the log categories.
- Use the `sys logs display [log category]` command to show the logs in an individual ZyWALL log category.
- Use the `sys logs clear` command to erase all of the ZyWALL's logs.

Log Command Example

This example shows how to set the ZyWALL to record the access logs and alerts and then view the results.

```
ras> sys logs load
ras> sys logs category access 3
ras> sys logs save
ras> sys logs display access

#  .time                 source                 destination            notes

    message
  0|06/08/2004 05:58:21 |172.21.4.154         |224.0.1.24           |ACCESS
BLOCK
    Firewall default policy: IGMP (W to W/ZW)
  1|06/08/2004 05:58:20 |172.21.3.56          |239.255.255.250      |ACCESS
BLOCK
    Firewall default policy: IGMP (W to W/ZW)
  2|06/08/2004 05:58:20 |172.21.0.2           |239.255.255.254      |ACCESS
BLOCK
    Firewall default policy: IGMP (W to W/ZW)
  3|06/08/2004 05:58:20 |172.21.3.191         |224.0.1.22           |ACCESS
BLOCK
    Firewall default policy: IGMP (W to W/ZW)
  4|06/08/2004 05:58:20 |172.21.0.254         |224.0.0.1            |ACCESS
BLOCK
    Firewall default policy: IGMP (W to W/ZW)
  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)
```

Index

Numerics

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z