ZyWALL 35

Internet Security Appliance

User's Guide

Version 3.63
November 2004

ZyXEL
Unleash Networking Power

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

Go to www.zyxel.com

1 Select your product from the drop-down list box on the ZyXEL home page to go to that product's page.

2 Select the certification you wish to view from this page

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal 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

1 To reduce the risk of fire, use only No. 26 AWG or larger telephone wire.

2 Do not use this product near water, for example, in a wet basement or near a swimming pool.

3 Avoid using this product during an electrical storm. There may be a remote risk of electric shock from lightening.

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	SUPPORT E-MAIL	TELEPHONE[A]	WEB SITE	REGULAR MAIL
LOCATION	SALES E-MAIL	FAX	FTP SITE	
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	
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	
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		
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		
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		
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		
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		
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		
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		

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 35.

> **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. The web configurator parts of this guide contain background information on features configurable by web configurator. The SMT parts of this guide contain background information solely on features not configurable by web configurator.

> **Note:** Use the web configurator, System Management Terminal (SMT) or command interpreter interface 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.
- The SMT menu titles and labels are in **Bold Times New Roman** font. Predefined field choices are in **Bold Arial** font. Command and arrow keys are enclosed in square brackets. [ENTER] means the Enter, or carriage return key; [ESC] means the Escape key and [SPACE BAR] means the Space Bar.
- 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.

Graphics Icons Key

ZyWALL	Computer	Notebook computer
Server	DSLAM	Firewall
Telephone	Switch	Router
Wireless Signal		

Note: The following section offers some background information on DSL. Skip to *Chapter 1* if you wish to begin working with your router right away.

CHAPTER 1
Getting to Know Your ZyWALL

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

1.1 ZyWALL 35 Internet Security Appliance Overview

The ZyWALL 35 is the ideal secure gateway for all data passing between the Internet and the LAN.

By integrating NAT, firewall, content filtering, certificates and VPN capability, ZyXEL's ZyWALL is a complete security solution that protects your Intranet and efficiently manages data traffic on your network. Dual WAN ports, dial backup and traffic redirect enhance reliability. You can deploy the ZyWALL as a transparent firewall in an existing network with minimal configuration.

The ZyWALL allows you to manage the bandwidth usage of your network's traffic. It also has two WAN interfaces and can balance the traffic load between them. You can control which IP addresses and applications get how much bandwidth. You can set priority for different types of traffic and/or IP addresses. You can also allot bandwidth to specific traffic types to guarantee delivery.

The PCMCIA/CardBus slot allows you to add a 802.11b/g-compliant wireless LAN. The ZyWALL offers highly secured wireless connectivity to your wired network with IEEE 802.1x, WEP data encryption, WPA (Wi-Fi Protected Access) and MAC address filtering. The ZyWALL increases network security by adding the option to change port roles from LAN to DMZ (De-Militarized Zone) for use with publicly accessible servers.

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	50
Number of Policy Routes	48
Number of NAT Sessions	10,000
Number of Port Forwarding Rules	50

Table 1 Feature Specifications

FEATURE	SPECIFICATION
Number of Address Mapping Rules	50
Number of IPSec VPN Tunnels/Security Associations	35

1.2.1 Physical Features

1.2.1.1 Auto-negotiating 10/100 Mbps Ethernet LAN

The LAN interface automatically detects if it's on a 10 or a 100 Mbps Ethernet.

1.2.1.2 Auto-crossover 10/100 Mbps Ethernet LAN

The LAN interface automatically adjusts to either a crossover or straight-through Ethernet cable.

1.2.1.3 Auto-negotiating 10/100 Mbps Ethernet DMZ

Public servers (Web, FTP, etc.) attached to a DeMilitarized Zone (DMZ) port are visible to the outside world (while still being protected from DoS (Denial of Service) attacks such as SYN flooding and Ping of Death) and can also be accessed from the secure LAN.

1.2.1.4 Auto-crossover 10/100 Mbps Ethernet DMZ

The DMZ interface automatically adjusts to either a crossover or straight-through Ethernet cable.

1.2.1.5 LAN/DMZ Interface

The ZyWALL provides four LAN ports that can also function as virtual DMZ ports. You can configure the ports as LAN or DMZ ports by changing the port role settings in the **LAN** or **DMZ** screen through the Web configurator.

1.2.1.6 Dual Auto-negotiating 10/100 Mbps Ethernet WAN

The 10/100 Mbps Ethernet WAN ports attach to the Internet via broadband modem or router. You can use a second connection for load sharing to increase overall network throughput or as a backup to enhance network reliability.

1.2.1.7 Dual Auto-crossover 10/100 Mbps Ethernet WAN

The WAN interface automatically adjusts to either a crossover or straight-through Ethernet cable.

1.2.1.8 Dial Backup WAN

The dial backup port can be used in reserve as a traditional dial-up connection when/if ever the WAN 1, 2 and traffic redirect connections fail.

1.2.1.9 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.

1.2.1.10 Reset Button

Use the reset button to restore the factory default password to 1234; IP address to 192.168.1.1, subnet mask to 255.255.255.0 and DHCP server enabled with a pool of 32 IP addresses starting at 192.168.1.33.

1.2.1.11 Dual PCMCIA and CardBus Slot

The dual PCMCIA and Card Bus slot provides the option of a wireless LAN.

1.2.1.12 IEEE 802.11 b/g Wireless LAN

The optional wireless LAN card provides mobility and a fast network environment for small and home offices. Users can connect to the local area network without any wiring efforts and enjoy reliable high-speed connectivity.

1.2.2 Non-Physical Features

1.2.2.1 Load Balancing

The ZyWALL improves quality of service and maximizes bandwidth utilization by dividing traffic loads between the two WAN interfaces (or ports).

1.2.2.2 SIP Passthrough

The ZyWALL includes a SIP Application Layer Gateway (ALG). It allows VoIP calls to pass through NAT by examining and translating IP addresses embedded in the data stream.

1.2.2.3 Transparent Firewall

Transparent firewall is also known as a bridge firewall. The ZyWALL can act as a bridge and still have the capability of filtering and inspecting the packets between a router and the LAN, or two routers. You do not need to do any other changes to your existing network. By deploying a ZyWALL in each segment, you can prevent the virus from spreading to the whole company network.

1.2.2.4 STP (Spanning Tree Protocol) / RSTP (Rapid STP)

When the ZyWALL is set to bridge mode, (R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a bridge to interact with other (R)STP -compliant bridges in your network to ensure that only one path exists between any two stations on the network.

1.2.2.5 Bandwidth Management

Bandwidth management allows you to allocate network resources according to defined policies. This policy-based bandwidth allocation helps your network to better handle real-time applications such as Voice-over-IP (VoIP).

1.2.2.6 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.

1.2.2.7 X-Auth (Extended Authentication)

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

1.2.2.8 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.

1.2.2.9 SSH

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

1.2.2.10 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

1.2.2.11 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.

1.2.2.12 Content Filtering

The ZyWALL can block web features such as ActiveX controls, Java applets and cookies, as well as disable web proxies. The ZyWALL can block or allow access to web sites that you specify. The ZyWALL can also block access to web sites containing keywords that you specify. You can define time periods and days during which content filtering is enabled and include or exclude a range of users on the LAN from content filtering.

You can also subscribe to category-based content filtering that allows your ZyWALL to check web sites against an external database of dynamically updated ratings of millions of web sites.

1.2.2.13 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.

1.2.2.14 RADIUS (RFC2138, 2139)

RADIUS (Remote Authentication Dial In User Service) server enables authentication, authorization and accounting for your wireless network.

1.2.2.15 IEEE 802.1x for Network Security

The ZyWALL supports the IEEE 802.1x standard that works with the IEEE 802.11 to enhance user authentication. With the local user profile, the ZyWALL allows you to configure up 32 user profiles without a network authentication server. In addition, centralized user and accounting management is possible on an optional network authentication server.

1.2.2.16 Wi-Fi Protected Access

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

1.2.2.17 Wireless LAN MAC Address Filtering

Your ZyWALL can check the MAC addresses of wireless stations against a list of allowed or denied MAC addresses.

1.2.2.18 WEP Encryption

WEP (Wired Equivalent Privacy) encrypts data frames before transmitting over the wireless network to help keep network communications private.

1.2.2.19 Packet Filtering

The packet filtering mechanism blocks unwanted traffic from entering/leaving your network.

1.2.2.20 Call Scheduling

Configure call time periods to restrict and allow access for users on remote nodes.

1.2.2.21 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.

1.2.2.22 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.

1.2.2.23 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.

1.2.2.24 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.

1.2.2.25 IP Alias

IP Alias allows you to partition a physical network into logical networks over the same Ethernet interface. The ZyWALL supports three logical LAN and/or DMZ interfaces via its single physical Ethernet LAN and/or DMZ interface with the ZyWALL itself as the gateway for each network.

1.2.2.26 IP Policy Routing

IP Policy Routing provides a mechanism to override the default routing behavior and alter packet forwarding based on the policies defined by the network administrator.

1.2.2.27 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.

1.2.2.28 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).

1.2.2.29 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).

1.2.2.30 Traffic Redirect

Traffic Redirect forwards WAN traffic to a backup gateway on the LAN when the ZyWALL cannot connect to the Internet, thus acting as an auxiliary backup when your regular WAN connection fails.

1.2.2.31 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.

1.2.2.32 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. The ZyWALL can also act as a surrogate DHCP server (**DHCP Relay**) where it relays IP address assignment from the actual real DHCP server to the clients.

1.2.2.33 Full Network Management

The embedded web configurator is an all-platform web-based utility that allows you to easily access the ZyWALL's management interface. Most functions of the ZyWALL are also software configurable via the SMT (System Management Terminal) interface. The SMT is a menu-driven interface that you can access from a terminal emulator through the console port or over a telnet connection.

1.2.2.34 RoadRunner Support

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

1.2.2.35 Logging and Tracing

Built-in message logging and packet tracing.

Unix syslog facility support.

Firewall logs.

Content filtering logs.

1.2.2.36 Upgrade ZyWALL Firmware via LAN

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

1.2.2.37 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 for the ZyWALL

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

1.3.1 Secure Broadband Internet Access via Cable or DSL Modem

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

Figure 1 Secure Internet Access via Cable, DSL or Wireless Modem
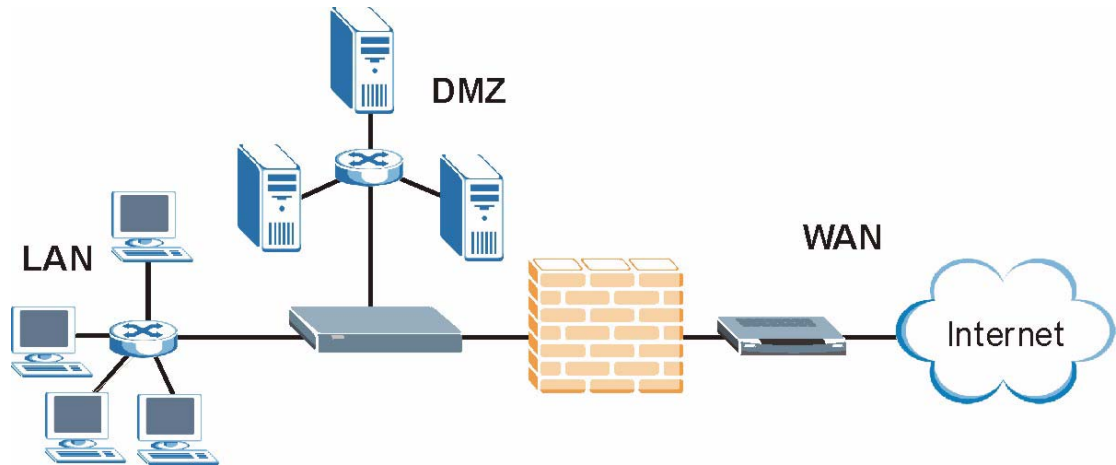
1.3.2 VPN Application

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

Figure 2   VPN Application
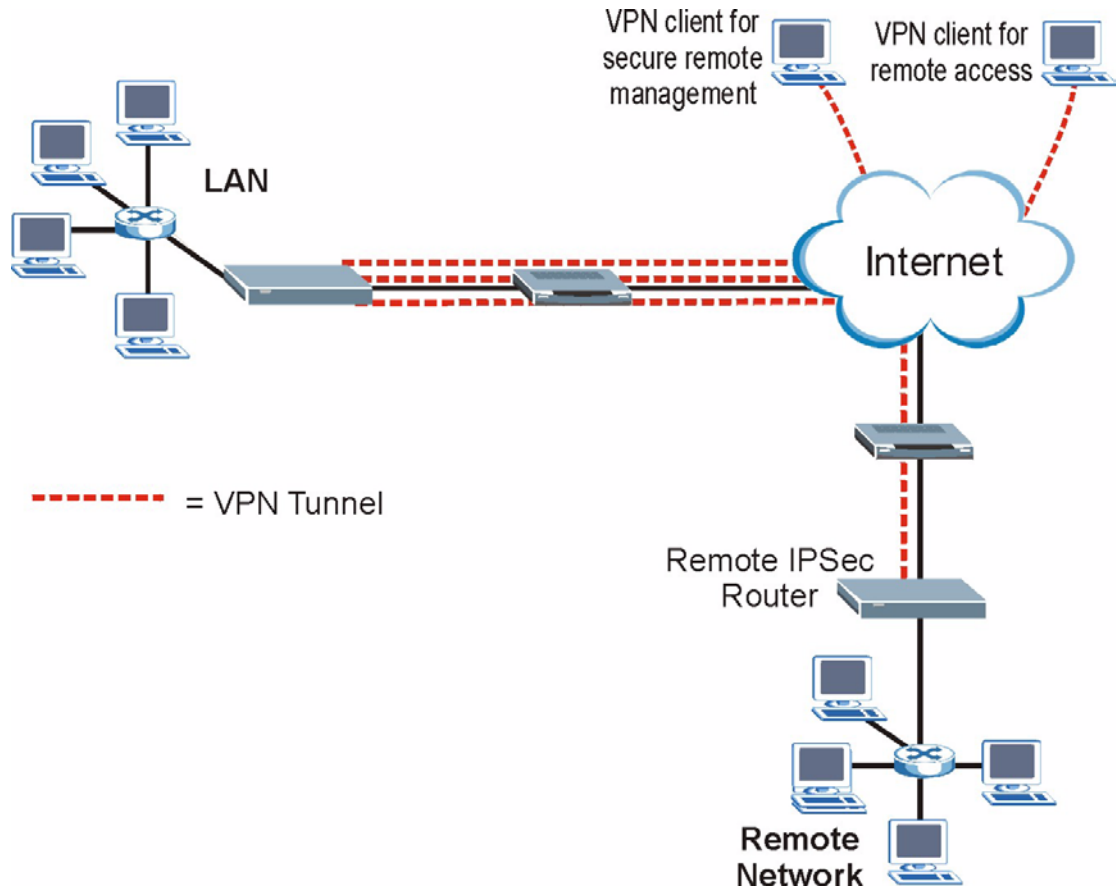
CHAPTER 2
Introducing the Web Configurator

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

2.1 Web Configurator Overview

The embedded web configurator allows you to manage the ZyWALL from anywhere through a browser such as Microsoft Internet Explorer or Netscape Navigator. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions with JavaScript enabled. It is recommended that you set your screen resolution to 1024 by 768 pixels. The screens you see in the web configurator may vary somewhat from the ones shown in this document due to differences between individual firmware versions.
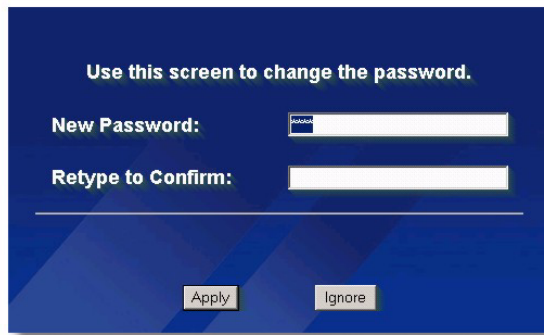
2.2 Accessing the ZyWALL Web Configurator

1 Make sure your ZyWALL hardware is properly connected and prepare your computer/computer network to connect to the ZyWALL (refer to the *Quick Start Guide*).

2 Launch your web browser.

3 Type "192.168.1.1" as the URL.

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

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

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

Figure 3 Change Password Screen

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

> **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 4 Replace Certificate Screen

7 You should now see the **HOME** screen (see Figure 6).

> **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 back of the ZyWALL. Uploading this configuration file replaces the current configuration file with the factory-default configuration file. This means that you will lose all configurations that you had previously and the speed of the console port will be reset to the default of 9600bps with 8 data bit, no parity, one stop bit and flow control set to none. The password will be reset to 1234, also.

2.3.1 Procedure To Use The Reset Button

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

1 Press the **RESET** button for ten seconds, and then release it. If the **SYS** LED begins to blink, the defaults have been restored and the ZyWALL restarts. Otherwise, go to step 2.

2 Turn the ZyWALL off.

3 While pressing the **RESET** button, turn the ZyWALL on.

4 Continue to hold the **RESET** button. The **SYS** LED will begin to blink and flicker very quickly after about 20 seconds. This indicates that the defaults have been restored and the ZyWALL is now restarting.

5 Release the **RESET** button and wait for the ZyWALL to finish restarting.

2.3.2 Uploading a Configuration File Via Console Port

1 Download the default configuration file from the ZyXEL FTP site, unzip it and save it in a folder.

2 Turn off the ZyWALL, begin a terminal emulation software session and turn on the ZyWALL again. When you see the message "Press Any key to enter Debug Mode within 3 seconds", press any key to enter debug mode.

3 Enter "y" at the prompt below to go into debug mode.

4 Enter "atlc" after "Enter Debug Mode" message.

5 Wait for "Starting XMODEM upload" message before activating Xmodem upload on your terminal. This is an example Xmodem configuration upload using HyperTerminal.

Figure 5   Example Xmodem Upload
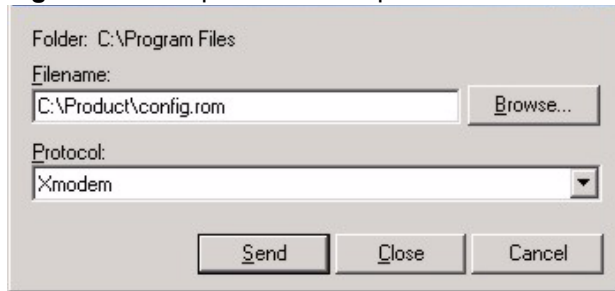
Type the configuration file's location, or click **Browse** to search for it.
Choose the **Xmodem** protocol.
Then click **Send**.

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

2.4 Navigating the ZyWALL 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 ⬛ icon (located in the top right corner of most screens) to view online help.

The screen varies according to the device mode you select in the **MAINTENANCE Device Mode** screen.

2.4.1 Router Mode

The following screen displays when the ZyWALL is set to router mode. The ZyWALL is set to router mode by default.

Figure 6 Web Configurator HOME Screen in Router Mode
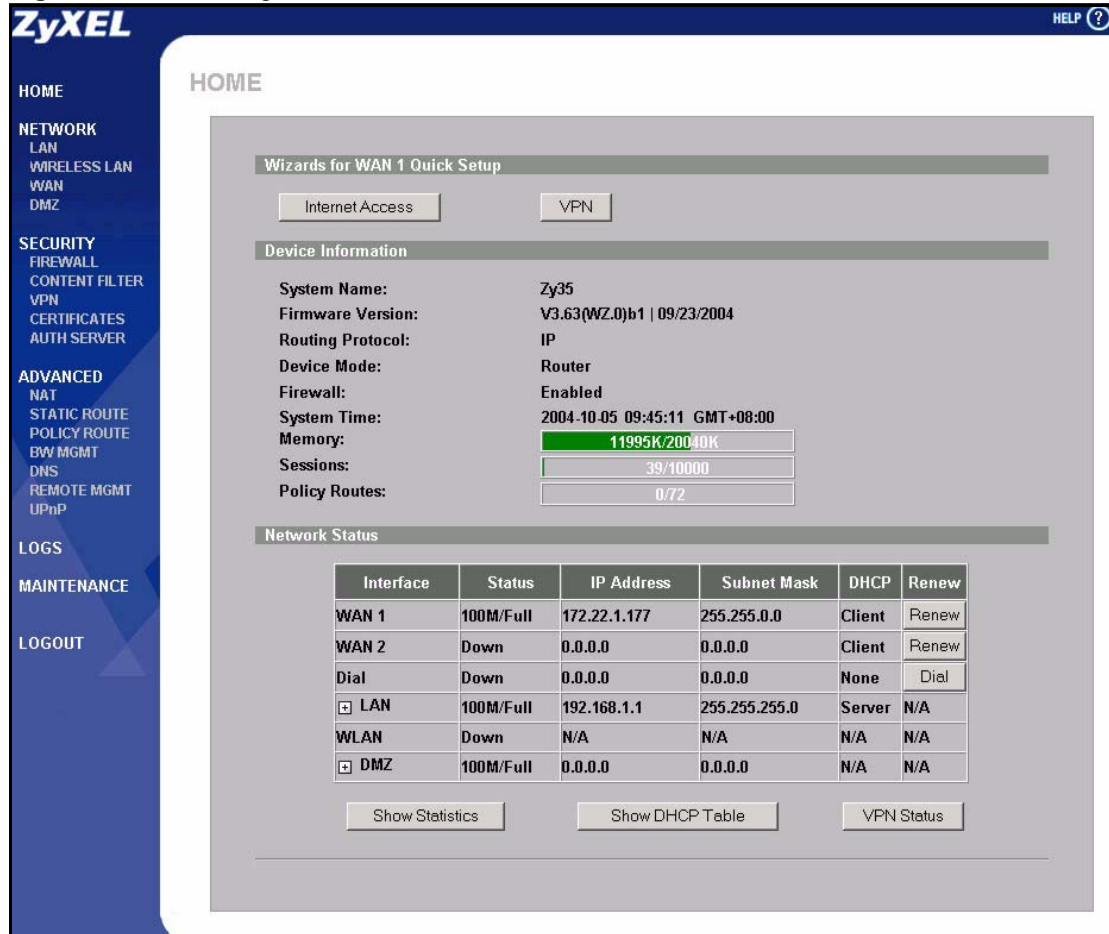
Use submenus to configure ZyWALL features.

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**, **Device Mode**, **F/W** (firmware) **Upload**, **Configuration** (Backup, Restore, Default), and **Restart**.

The following table describes the labels in this screen.

Table 2 Web Configurator HOME Screen in Router Mode

LABEL	DESCRIPTION
Wizards for WAN1 Quick Setup	
Internet Access	Click **Internet Access** to use the initial configuration wizard. This configures WAN1.
VPN Wizard	Click **VPN Wizard** to create VPN policies.
Device Information	

Table 2   Web Configurator HOME Screen in Router Mode (continued)

LABEL	DESCRIPTION
System Name	This is the **System Name** you enter in the **MAINTENANCE General** screen. It is for identification purposes.
Firmware Version	This is the ZyNOS Firmware version and the date created. ZyNOS is ZyXEL's proprietary Network Operating System design.
Routing Protocol	This shows the routing protocol - **IP** for which the ZyWALL is configured. This field is not configurable.
Device Mode	This displays whether the ZyWALL is functioning as a router or a bridge.
Firewall	This displays whether or not the ZyWALL's firewall is activated.
System Time	This field displays your ZyWALL's present date and time.
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.
Policy Routes	The first number shows how many policy routes you have configured. The second number shows the maximum number of policy routes that you can configure on the ZyWALL. The bar displays what percent of the ZyWALL's possible policy routes are configured. The bar turns from green to red when the maximum is being approached.
Network Status	
Interface	This is the port type. Port types are: WAN1, WAN2, Dial, LAN, WLAN and DMZ. Click "+" to expand or "-" to collapse the LAN and DMZ IP alias drop-down lists.
Status	For the LAN and DMZ ports, this displays the port speed and duplex setting. For the WAN and Dial Backup 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), **Dial** (starting to trigger a call) or **Drop** (dropping a call) if you're using PPPoE encapsulation. For the WLAN port, it displays **Active** when WLAN is enabled or **Inactive** when WLAN is disabled.
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**, **Relay** 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, PPPoE or dial backup connection.

Table 2 Web Configurator HOME Screen in Router Mode (continued)

LABEL	DESCRIPTION
Show Statistics	Click **Show Statistics** to see router performance statistics such as the number of packets sent and number of packets received for each port, including WAN1, WAN2, Dial Backup, LAN, WLAN and DMZ.
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 Bridge Mode

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

The ZyWALL bridges traffic traveling between the ZyWALL's interfaces.

You can use the firewall in bridge mode (refer to the firewall chapters for details on configuring the firewall).

Figure 7 Web Configurator HOME Screen in Bridge Mode
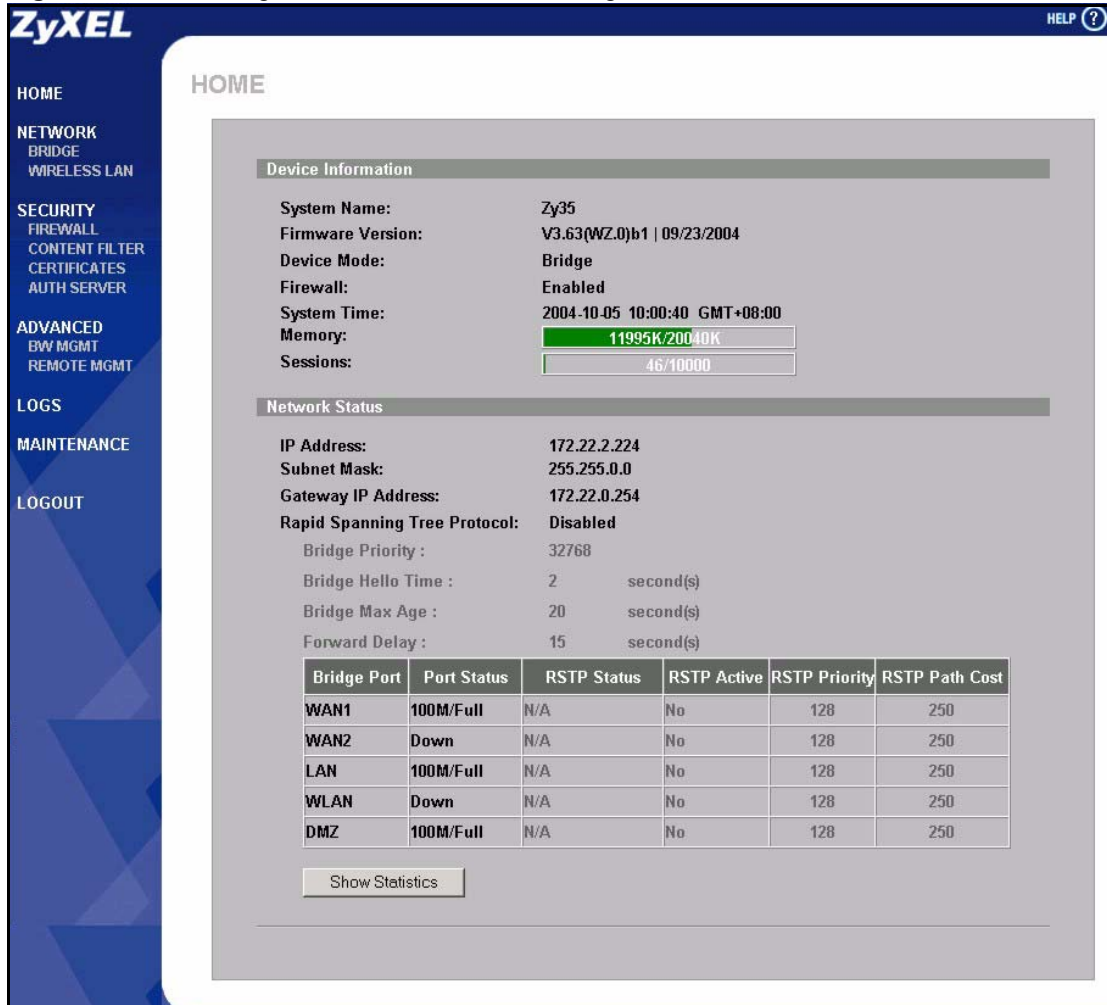
The following table describes the labels not previously discussed (see Table 2).

Table 3 Web Configurator HOME Screen in Bridge Mode

LABEL	DESCRIPTION
Network Status	
IP Address	This is the IP address of your ZyWALL in dotted decimal notation.
Subnet Mask	This is the IP subnet mask of the ZyWALL.
Gateway IP Address	This is the gateway IP address.
Rapid Spanning Tree Protocol	This shows whether RSTP (Rapid Spanning Tree Protocol) is active or not. The following labels or values relative to RSTP do not apply when RSTP is disabled.
Bridge Priority	This is the bridge priority of the ZyWALL.
Bridge Hello Time	This is the interval of BPDUs (Bridge Protocol Data Units) from the root bridge.
Bridge Max Age	This is the predefined interval that a bridge waits to get a Hello message (BPDU) from the root bridge.
Forward Delay	This is the forward delay interval.

Table 3   Web Configurator HOME Screen in Bridge Mode (continued)

LABEL	DESCRIPTION
Bridge Port	This is the port type. Port types are: WAN1, WAN2, LAN, WLAN and DMZ.
Port Status	For the WAN, LAN, and DMZ ports, this displays the port speed and duplex setting. For the WAN port, it displays **Down** when the link is not ready or has failed. For the WLAN port, it displays **Active** when WLAN is enabled or **Inactive** when WLAN is disabled.
RSTP Status	This is the RSTP status of the corresponding port.
RSTP Active	This shows whether or not RSTP is active on the corresponding port.
RSTP Priority	This is the RSTP priority of the corresponding port.
RSTP Path Cost	This is the cost of transmitting a frame from the root bridge to the corresponding port.
Show Statistics	Click **Show Statistics** to see bridge performance statistics such as the number of packets sent and number of packets received for each port, including WAN1, WAN2, LAN, DMZ and WLAN.

2.4.3 Navigation Panel

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

The following table lists the features available for each mode.

Table 4   Feature Comparison

FEATURE	BRIDGE MODE	ROUTER MODE
Internet Access Wizard		O
VPN Wizard		O
DHCP Table		O
System Statistics	O	O
LAN		O
Bridge	O	
Wireless LAN	O	O
WAN		O
DMZ		O
Firewall	O	O
Content Filter	O	O
VPN		O
Certificates	O	O
Authentication Server	O	O
NAT		O
Static Route		O
Bandwidth Management	O	O
DNS		O

Table 4   Feature Comparison

FEATURE	BRIDGE MODE	ROUTER MODE
Remote Management	O	O
UPnP		O
Logs	O	O
Maintenance	O	O

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

The following table describes the sub-menus.

Table 5   Screens Summary

LINK	TAB	FUNCTION
HOME		This screen shows the ZyWALL's general device and network status information. Use this screen to access the wizards, statistics and DHCP table.
LAN	LAN	Use this screen to configure LAN DHCP and TCP/IP settings.
	Static DHCP	Use this screen to assign fixed IP addresses on the LAN.
	IP Alias	Use this screen to partition your LAN interface into subnets.
BRIDGE	Bridge	Use this screen to change the bridge settings on the ZyWALL.
	Port Roles	Use this screen to change the LAN/DMZ port roles
WIRELESS LAN	Wireless	Use this screen to configure the wireless LAN settings and WLAN authentication/security settings.
	MAC Filter	Use this screen to change MAC filter settings on the ZyWALL
WAN	General	This screen allows you to configure load balancing, route priority and traffic redirect properties.
	WAN1	Use this screen to configure ZyWALL WAN1 port for internet access.
	WAN2	Use this screen to change your WAN2 port settings.
	Traffic Redirect	Use this screen to configure your traffic redirect properties and parameters.
	Dial Backup	Use this screen to configure the backup WAN dial-up connection
DMZ	DMZ	Use this screen to configure your DMZ connection.
	IP Alias	Use this screen to partition your DMZ interface into subnets
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.
CONTENT FILTER	General	This screen allows you to enable content filtering and block certain web features.

Table 5 Screens Summary (continued)

LINK	TAB	FUNCTION
	Categories	Use this screen to select which categories of web pages to filter out, as well as to register for external database content filtering and view reports.
	Customization	Use this screen to customize the content filter list.
VPN	VPN Rules	Use this screen to configure VPN connections and view the rule summary.
	SA Monitor	Use this screen to display and manage active VPN connections.
	Global Setting	Use this screen to allow NetBIOS packets through the VPN connections.
CERTIFICATES	My Certificates	Use this screen to view a summary list of certificates and manage certificates and certification requests.
	Trusted CAs	Use this screen to view and manage the list of the trusted CAs.
	Trusted Remote Hosts	Use this screen to view and manage the certificates belonging to the trusted remote hosts.
	Directory Servers	Use this screen to view and manage the list of the directory servers.
AUTH SERVER	Local User Database	Use this screen to configure the local user account(s) on the ZyWALL.
	RADIUS	Configure this screen to use an external server to authenticate wireless and/or VPN users.
NAT	NAT Overview	Use this screen to enable NAT.
	Address Mapping	Use this screen to configure network address translation mapping rules.
	Port Forwarding	Use this screen to configure servers behind the ZyWALL.
	Port Triggering	Use this screen to change your ZyWALL's port triggering settings.
STATIC ROUTE	IP Static Route	Use this screen to configure IP static routes.
POLICY ROUTE	Policy Rout Summary	Use this screen to view a summary list of all the policies and configure policies for use in IP policy routing.
BW MGMT	Summary	Use this screen to enable bandwidth management on an interface.
	Class Setup	Use this screen to set up the bandwidth classes.
	Monitor	Use this screen to view the ZyWALL's bandwidth usage and allotments.
DNS	System	Use this screen to configure the address and name server records.
	Cache	Use this screen to configure the DNS resolution cache.
	LAN	Use this screen to configure LAN DNS information.
	DDNS	Use this screen to set up dynamic DNS.
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.

Table 5 Screens Summary (continued)

LINK	TAB	FUNCTION
	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.
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.
	Device Mode	Use this screen to configure and have your ZyWALL work as a router or a bridge.
	F/W Upload	Use this screen to upload firmware to your ZyWALL
	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.

2.4.4 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 8   Home : Show Statistics

The following table describes the labels in this screen.

Table 6   Home : Show Statistics

LABEL	DESCRIPTION
	Click the icon to display the chart of throughput statistics.
Port	This is the WAN1, WAN2, Dial Backup, LAN, DMZ or WLAN 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.
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.

2.4.4.1 Show Statistics: Line Chart

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

Figure 9   Home : Show Statistics: Line Chart
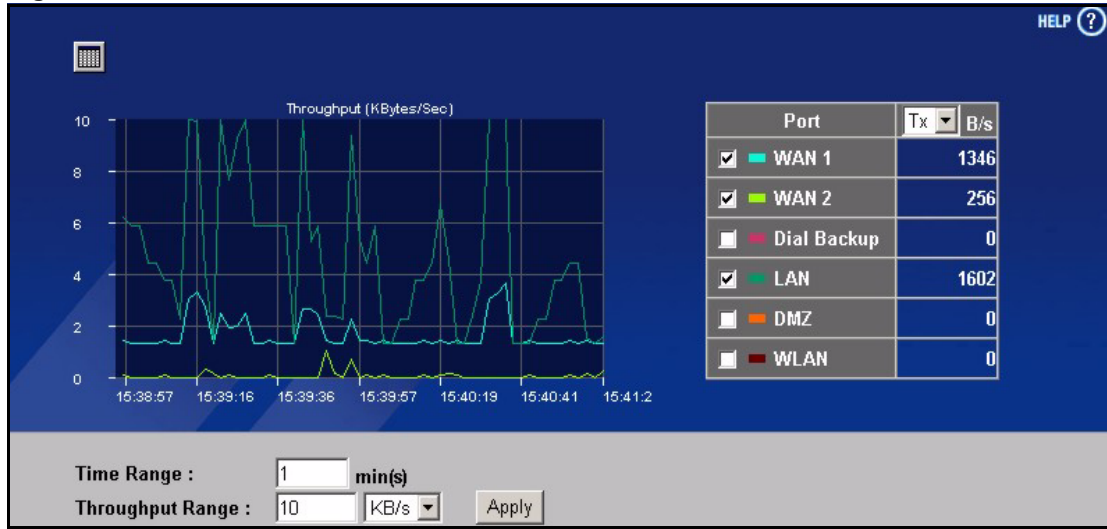
The following table describes the labels in this screen.

Table 7   Home : Show Statistics: Line Chart

LABEL	DESCRIPTION
	Click the icon to go back to the **Show Statistics** screen.
Port	Select the check box(es) to display the throughput statistics of the corresponding port(s).
B/s	Specify the direction of the traffic for which you want to show throughput statistics in this table. Select **Tx** to display transmitted traffic throughput statistics and the amount of traffic (in bytes). Select **Rx** to display received traffic throughput statistics and the amount of traffic (in bytes).
Time Range	Set the range of time (in minute) over which to display the throughput.
Throughput Range	Set the range of the throughput (in **B/s**, **KB/s** or **MB/s**) to display.
Apply	Click **Apply** to save these settings back to the ZyWALL temporarily.

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

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

Figure 10 Home : DHCP Table

The following table describes the labels in this screen.

Table 8 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.

2.4.6 VPN Status

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

Figure 11 Home : VPN Status
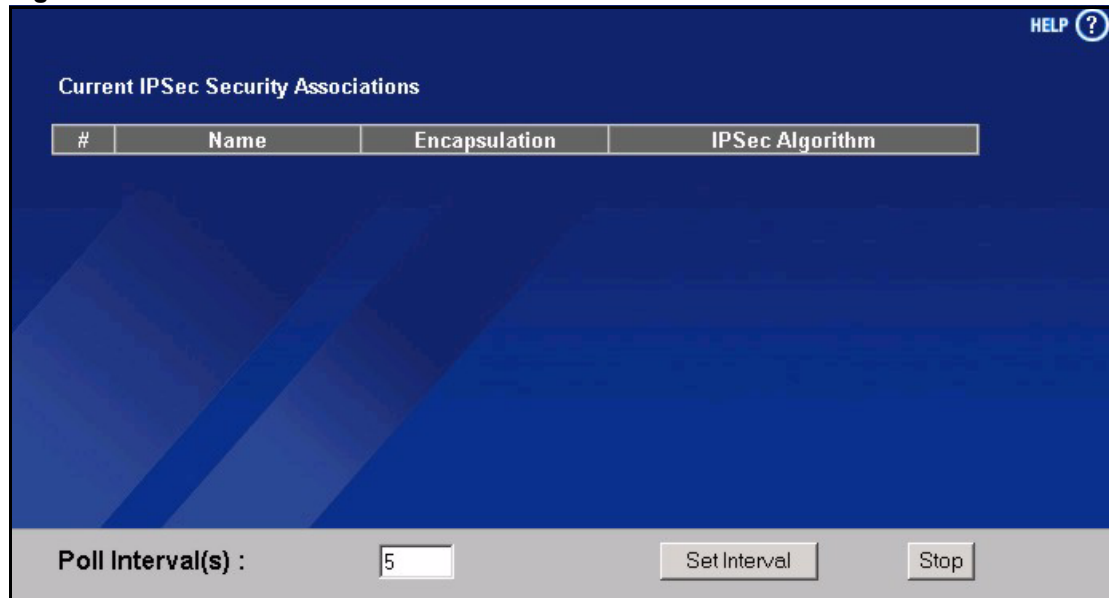
The following table describes the labels in this screen.

Table 9 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 web configurator. This chapter is only applicable when the ZyWALL is in router mode.

3.1 Wizard Setup Overview

The web configurator's setup wizards help you configure WAN1 on the ZyWALL to access the Internet and edit VPN policies and configure IKE settings to establish a VPN tunnel.

3.2 Internet Access

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.**

3.2.1.1 Ethernet

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

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

Figure 12 ISP Parameters : Ethernet Encapsulation

The following table describes the labels in this screen.

Table 10 ISP Parameters : Ethernet Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	You must choose the **Ethernet** option when the WAN port is used as a regular Ethernet. Otherwise, choose **PPPoE** or **PPTP** for a dial-up connection.
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 are not applicable (**N/A**) for 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 Password	Type your password again for confirmation.
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. Alternatively, click the right mouse button to copy and/or paste the IP address.
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.
Next	Click **Next** to continue.

3.2.1.2 PPPoE Encapsulation

Point-to-Point Protocol over Ethernet (PPPoE) functions as a dial-up connection. PPPoE is an IETF (Internet Engineering Task Force) 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 D PPPoE for more information on PPPoE.

Figure 13 ISP Parameters : PPPoE Encapsulation

The following table describes the labels in this screen.

Table 11 ISP Parameters : PPPoE Encapsulation

LABEL	DESCRIPTION
ISP Parameter for Internet Access	
Encapsulation	Choose an encapsulation method from the pull-down list box. **PPP over Ethernet** forms a dial-up connection.
Service Name	Type the name of your service provider.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Retype 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 PPPoE server. The default time is **100** seconds.
Next	Click **Next** to continue.

3.2.1.3 PPTP Encapsulation

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

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

Refer to Appendix E PPTP for more information on PPTP.

> **Note:** The ZYWALL supports one PPTP server connection at any given time.

Figure 14 ISP Parameters : PPTP Encapsulation

The following table describes the labels in this screen.

Table 12 ISP Parameters : 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	

Table 12 ISP Parameters : PPTP Encapsulation

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

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 13 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, 192.168.1.1, for your ZyWALL, but make sure that no other device on your network is using that IP address.

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

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 (see the Private DNS Server section in Chapter 20 DNS).

3.2.2.4 WAN MAC Address

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

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

> **Note:** ZyXEL recommends you clone the MAC address from a computer on your LAN even if your ISP does not require MAC address authentication.

Table 14 Example of Network Properties for LAN Servers with Fixed IP Addresses

Choose an IP address	192.168.1.2-192.168.1.32; 192.168.1.65-192.168.1.254.
Subnet mask	255.255.255.0
Gateway (or default route)	192.168.1.1(ZyWALL LAN IP)

The second wizard screen varies according to the type of encapsulation that you select in the second wizard screen.

Figure 15 WAN and DNS

The following table describes the labels in this screen.

Table 15 WAN and DNS

LABEL	DESCRIPTION
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 in this field if you selected **Use fixed IP address**. This field is available when you select Ethernet encapsulation in the previous wizard screen.
Remote IP Subnet Mask	Enter the gateway IP subnet mask (if your ISP gave you one) in this field if you selected **Use fixed IP address**. This field is not available when you select Ethernet encapsulation in the previous wizard screen.
Remote/Gateway IP Address	Enter the gateway IP address in this field if you selected **Use fixed IP address**.
System DNS Servers	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.
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). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. 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. Select **None** if you do not want to configure DNS servers. If you do not configure a system DNS server, you must use IP addresses when configuring VPN, DDNS and the time server.
WAN MAC Address	The MAC address field allows you to configure the WAN port's MAC Address by either using the factory default or cloning the MAC address from a computer on your LAN.
Factory Default	Select this option to use the factory assigned default MAC Address.
Spoof this Computer's MAC Address - IP Address	Select this option and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different rom file. It is advisable to clone the MAC address from a computer on your LAN even if your ISP does not presently require MAC address authentication.
Back	Click **Back** to return to the previous screen.
Finish	Click **Finish** to complete and save the wizard setup.

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 16 Internet Access Wizard Setup Complete
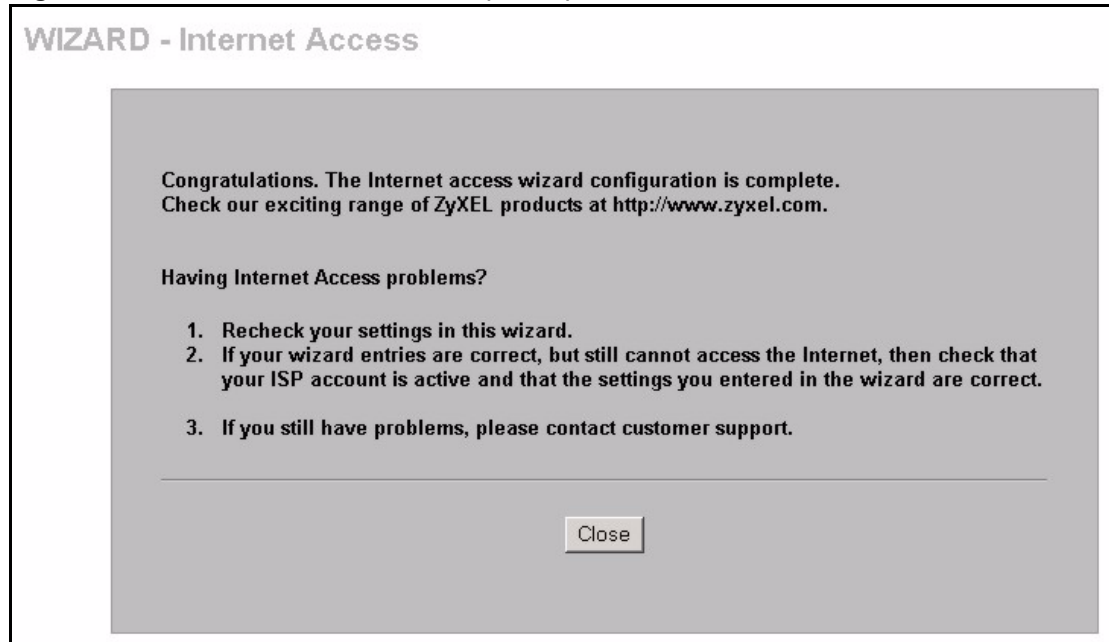
3.3 VPN Overview

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.

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.

3.4 VPN Wizard

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 VPN screens for configuration.

3.4.1 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.

3.4.2 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).

3.4.2.1 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.

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

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

Figure 17 VPN Wizard : Gateway Setting
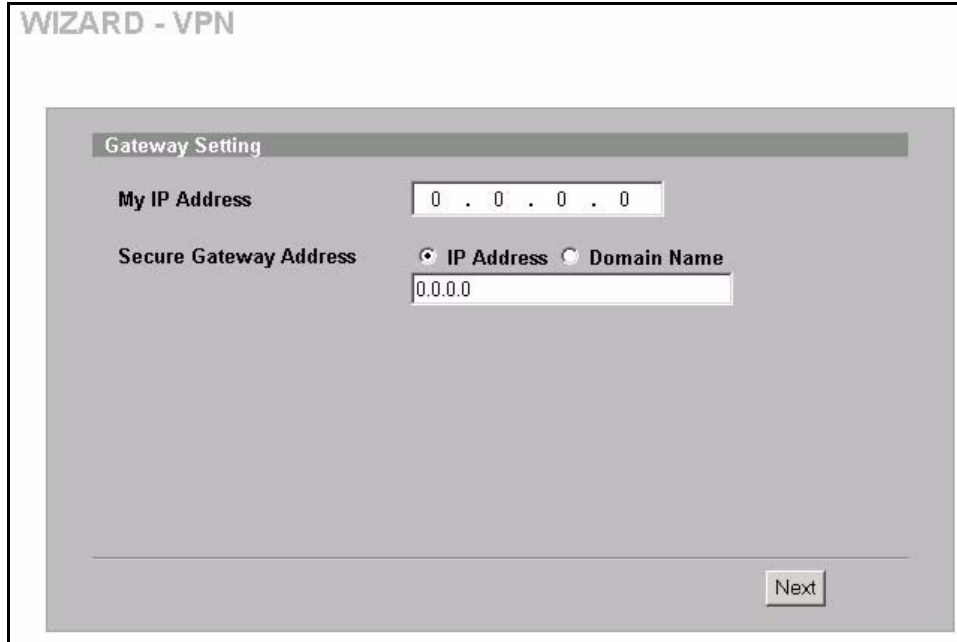
The following table describes the labels in this screen.

Table 16 VPN Wizard : Gateway Setting

LABEL	DESCRIPTION
My IP Address	Enter the WAN IP address of your ZyWALL or leave the field set to **0.0.0.0**. The following applies if the **My IP Address** field is configured as **0.0.0.0**: • When the WAN port operation mode is set to Active/Passive, the ZyWALL uses the IP address (static or dynamic) of the WAN port that is in use. • When the WAN port operation mode is set to Active/Active, the ZyWALL uses the IP address (static or dynamic) of the primary (highest priority) WAN port to set up the VPN tunnel as long as the corresponding WAN1 or WAN2 connection is up. If the corresponding WAN1 or WAN2 connection goes down, the ZyWALL uses the IP address of the other WAN port. • If both WAN connections go down, the ZyWALL uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect. See the chapter on WAN for details on dial backup and traffic redirect. The VPN tunnel has to be rebuilt if this IP address changes.
Secure Gateway Address	
IP Address	Select **IP Address** and enter the WAN IP address of the remote IPSec router (secure gateway) in the field below to identify the remote IPSec router by its IP address.
Domain Name	Select **Domain Name** and enter the domain name of the remote IPSec router (secure gateway) in the field below to identify the remote IPSec router by a domain name.
Next	Click **Next** to continue.

3.4.3 Network Setting

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 18   VPN Wizard : Network Setting

The following table describes the labels in this screen.

Table 17   VPN Wizard : Network Setting

LABEL	DESCRIPTION
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 17   VPN Wizard : Network Setting

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

3.4.4 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 19   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 the IKE Phases section. 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.

3.4.4.1 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.

3.4.4.2 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.

3.4.4.3 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.

3.4.4.4 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).

3.5 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.

3.5.1 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.

3.5.2 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 18 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.	

3.5.3 IKE Tunnel Setting (IKE Phase 1)

Figure 20   VPN Wizard : IKE Tunnel Setting

The following table describes the labels in this screen.

Table 19   VPN Wizard : IKE Tunnel Setting

LABEL	DESCRIPTION
Negotiation Mode	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 19 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.

3.5.4 IPSec Setting (IKE Phase 2)

Figure 21   VPN Wizard : IPSec Setting

The following table describes the labels in this screen.

Table 20 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).
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.

3.5.5 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 22 VPN Wizard : VPN Status

The following table describes the labels in this screen.

Table 21 VPN Wizard : VPN Status

LABEL	DESCRIPTION
Gateway Setting	
My IP Address	This is the WAN IP address of your ZyWALL.
Secure 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 N/A. When the local network is configured for a range IP address, this is the end (static) IP address, in a range of computers on the LAN behind your ZyWALL. When the local network is configured for a subnet, this is a subnet mask on the LAN behind your ZyWALL.
Remote Network	

Table 21 VPN Wizard : VPN Status (continued)

LABEL	DESCRIPTION
Starting IP Address	This is a (static) IP address on the network behind the remote IPSec router.
Ending IP Address/ Subnet Mask	When the remote network is configured for a single IP address, this field is N/A. When the remote network is configured for a range IP address, this is the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the remote network is configured for a subnet, this is a subnet mask on the network behind the remote IPSec router.
IKE Tunnel Setting (IKE Phase 1)	
Negotiation Mode	This shows **Main Mode** or **Aggressive Mode**. Multiple SAs connecting through a secure gateway must have the same negotiation mode.
Encryption Algorithm	This is the method of data encryption. Options can be **DES**, **3DES** or **AES**.
Authentication Algorithm	**MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data.
Key Group	This is the key group you chose for phase 1 IKE setup.
SA Life Time (Seconds)	This is the length of time before an IKE SA automatically renegotiates.
Pre-Shared Key	This is a pre-shared key identifying a communicating party during a phase 1 IKE negotiation.
IPSec Setting (IKE Phase 2)	
Encapsulation Mode	This shows **Tunnel** mode or **Transport** mode.
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.

3.5.6 VPN Wizard Setup Complete

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

Figure 23   VPN Wizard Setup Complete
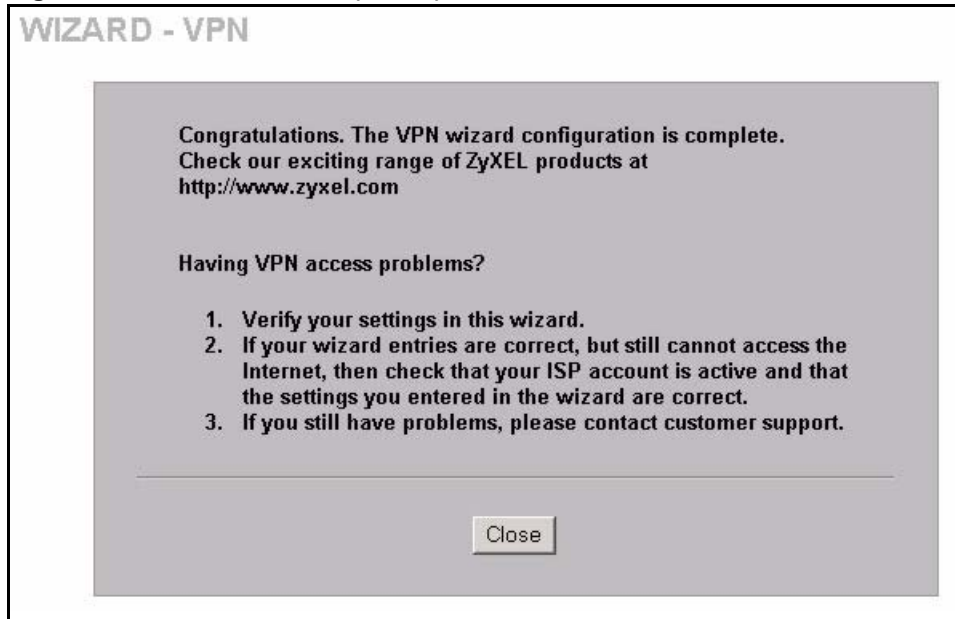
CHAPTER 4
LAN Screens

This chapter describes how to configure LAN settings. This chapter is only applicable when the ZyWALL is in router mode.

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, manage IP addresses, and partition your physical network into logical networks.

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 clients. 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 with a pool of 128 IP addresses starting from 192.168.1.33 to 192.168.1.160. This configuration leaves 127 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 **DNS System** 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 **DNS LAN** screen to configure the DNS server information that the ZyWALL sends to the DHCP client devices on the LAN.

3 Use the **REMOTE MGMT DNS** screen to configure the ZyWALL (in router mode) to accept or discard DNS queries.

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 192.168.1.1 with subnet mask of 255.255.255.0 (24 bits)
- DHCP server enabled with 128 client IP addresses starting from 192.168.1.33.

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

See the IP Address and Subnet Mask section in the **Wizard Setup** chapter 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 24 LAN
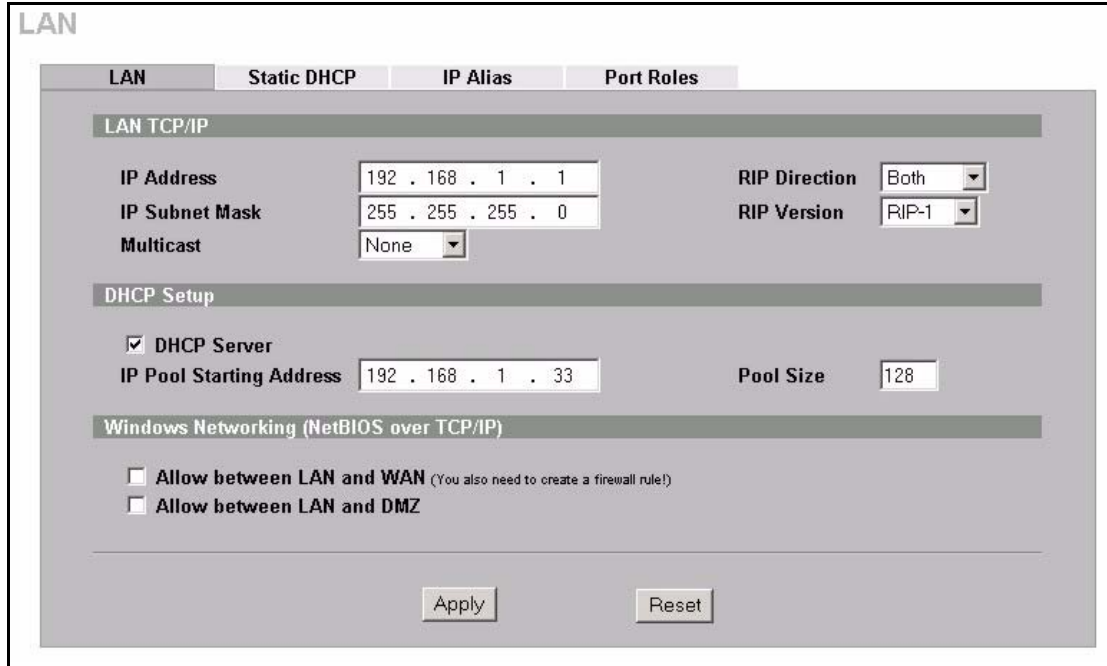
The following table describes the labels in this screen.

Table 22 LAN

LABEL	DESCRIPTION
LAN TCP/IP	
IP Address	Type the IP address of your ZyWALL in dotted decimal notation. 192.168.1.1 is the factory default. Alternatively, click the right mouse button to copy and/or paste the IP address.
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your ZyWALL automatically 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**.

Table 22 LAN (continued)

LABEL	DESCRIPTION
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 Server	DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (workstations) to obtain TCP/IP configuration at startup from a server. Unless you are instructed by your ISP, leave the **DHCP Server** check box selected. Clear it to stop the ZyWALL from acting as a DHCP server. When configured as a server, the ZyWALL provides TCP/IP configuration for the clients. If not, DHCP service is disabled and you must have another DHCP server on your LAN, or else the computers must be manually configured. When set as a server, fill in the rest of the DHCP setup fields.
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Pool Size	This field specifies the size, or count of the IP address pool.
Windows Networking (NetBIOS over TCP/IP)	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. 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.
Allow between LAN and DMZ	Select this check box to forward NetBIOS packets from the LAN to the DMZ and from the DMZ to the LAN. (Not all ZyWALL models have a DMZ port.) If your firewall is enabled with the default policy set to block DMZ to LAN traffic, you also need to enable the default DMZ to LAN firewall rule that forwards NetBIOS traffic. Clear this check box to block all NetBIOS packets going from the LAN to the DMZ and from the DMZ 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 IP addresses on the LAN to specific individual computers based on their MAC Addresses.

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 25 Static DHCP
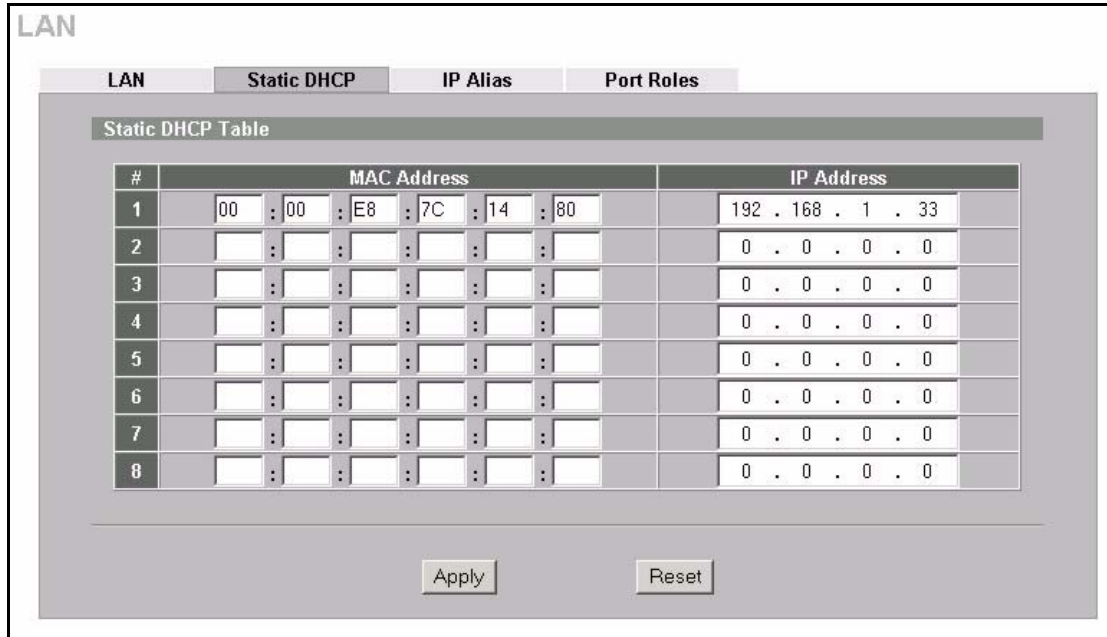
The following table describes the labels in this screen.

Table 23 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.
	The IP address can be in the same subnet as the LAN IP address or the LAN IP alias 1 or 2.
	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.

4.6 Configuring IP Alias

IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The ZyWALL supports three logical LAN interfaces via its single physical Ethernet interface with the ZyWALL itself as the gateway for each LAN network.

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

> **Note:** Make sure that the subnets of the logical networks do not overlap.

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

Figure 26 Physical Network & Partitioned Logical Networks
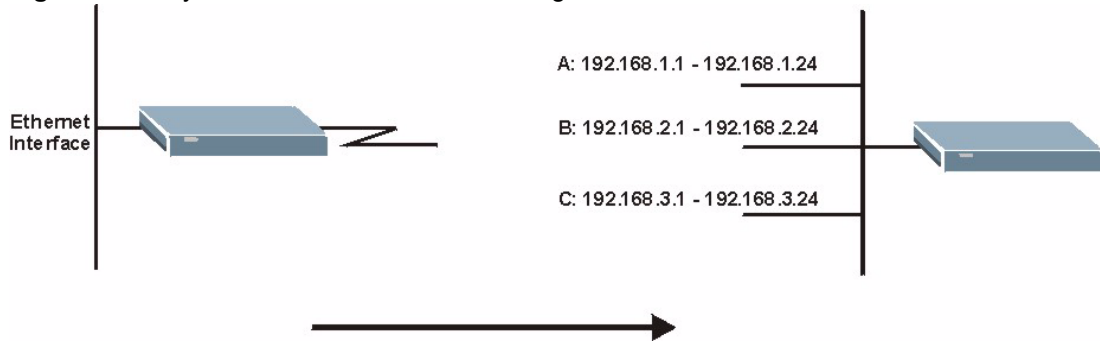
To change your ZyWALL's IP alias settings, click **LAN**, then the **IP Alias** tab. The screen appears as shown.

Figure 27 IP Alias
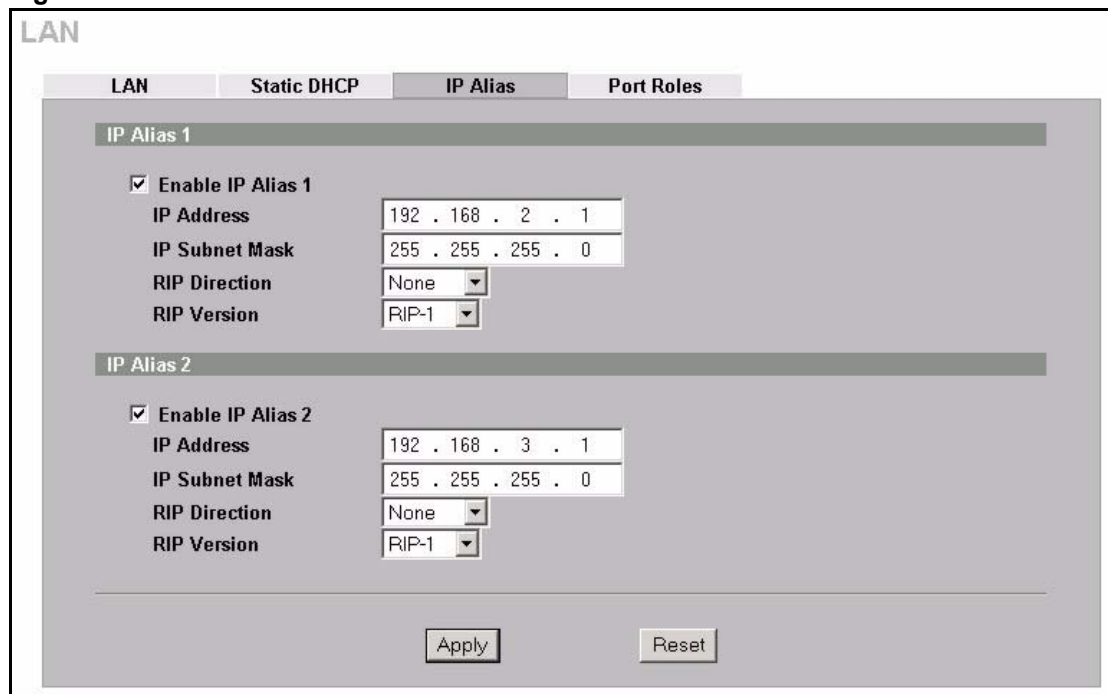
The following table describes the labels in this screen.

Table 24 IP Alias

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

4.7 Configuring Port Roles

To configure a LAN/DMZ port as a LAN or DMZ port, select its radio button next to **LAN** or **DMZ** and click **Apply**. Otherwise, click **Reset** to restore the previous configuration. The radio buttons correspond to Ethernet ports on the front panel of the ZyWALL. By default, ports 1 to 4 are all LAN ports.

> **Note:** Do the following if you are configuring from a computer connected to a LAN or DMZ port and changing the port's role:
> 1. Make sure your computer's IP address is in the same subnet as the ZyWALL's LAN or DMZ IP address.
> 2. A port's IP address varies as its role changes, use the appropriate LAN or DMZ IP address to access the ZyWALL.

Click **LAN**, then **Port Roles**. The screen appears as shown.

Figure 28 Port Roles
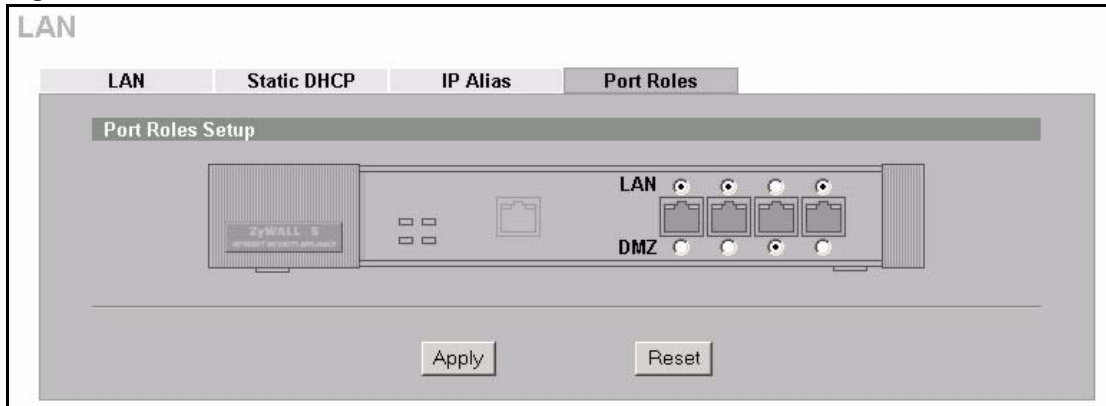
After you change the LAN/DMZ port roles and click **Apply**, please wait for few seconds until the following screen appears. Click **Return** to go back to the **Port Roles** screen.

Figure 29 Port Roles Change Complete

Chapter 4 LAN Screens

C H A P T E R 5
Bridge Screens

This chapter describes how to configure bridge settings. This chapter is only applicable when the ZyWALL is in bridge mode.

5.1 Bridge Loop

The ZyWALL can act as a bridge between a switch and a wired LAN or between two routers.

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

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

Figure 30   Bridge Loop: Bridge Connected to Wired LAN
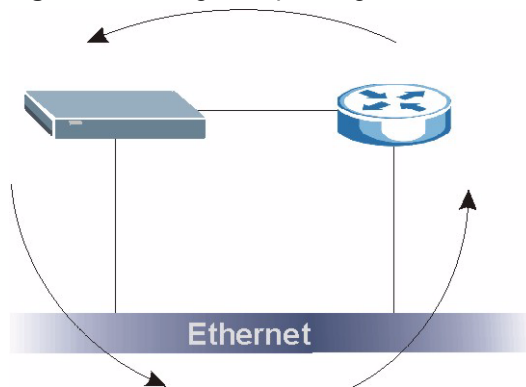
To prevent bridge loops, ensure that your ZyWALL is not set to bridge mode while connected to two wired segments of the same LAN or you enable RSTP in the **Bridge** screen.

5.2 Spanning Tree Protocol (STP)

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

5.2.1 Rapid STP

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

5.2.2 STP Terminology

The root bridge is the base of the spanning tree; it is the bridge with the lowest identifier value (MAC address).

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

Table 25   STP Path Costs

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

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

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

5.2.3 How STP Works

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

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

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

5.2.4 STP Port States

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

Table 26 STP Port States

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

5.3 Configuring Bridge

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

To change your ZyWALL's bridge settings, click **BRIDGE**. The screen appears as shown.

Figure 31 Bridge

The following table describes the labels in this screen.

Table 27 Bridge

LABEL	DESCRIPTION
Bridge Setup	
IP Address	Type the IP address of your ZyWALL in dotted decimal notation.
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address.
Gateway IP Address	Enter the gateway IP address.
First/Second/Third DNS Server	DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it. The ZyWALL uses a system DNS server (in the order you specify here) to resolve domain names for content filtering, the time server, etc. If you have the IP address(es) of the DNS server(s), enter the DNS server's IP address(es) in the field(s) to the right.

Table 27 Bridge (continued)

LABEL	DESCRIPTION
Rapid Spanning Tree Protocol Setup	
Enable Rapid Spanning Tree Protocol	Select the check box to activate RSTP on the ZyWALL.
Bridge Priority	Enter a number between 0 and 61440 as bridge priority of the ZyWALL. 0 is the highest.
Bridge Hello Time	Enter an interval (between 1 and 10) in seconds that the root bridge waits before sending a hello packet.
Bridge Max Age	Enter an interval (between 6 and 40) in seconds that a bridge waits to get a Hello BPDU from the root bridge.
Forward Delay	Enter the length of time (between 4 and 30) in seconds that a bridge remains in the listening and learning port states. The default is 15 seconds.
Bridge Port	This is the bridge port type. Port types are: WAN, LAN, WLAN and DMZ.
RSTP Active	Select the check box to enable RSTP on the corresponding port.
RSTP Priority 0(Highest)~240(Lowest)	Enter a number between 0 and 240 as RSTP priority for the corresponding port. 0 is the highest.
RSTP Path Cost 1(Lowest)~65535(Highest)	Enter a number between 1 and 65535 as RSTP path cost for the corresponding port. 65535 is the highest.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

5.4 Configuring Port Roles

Click **BRIDGE**, then **Port Roles** to configure a LAN/DMZ port as a LAN or DMZ port.

To configure a LAN/DMZ port as a LAN or DMZ port, select its radio button next to **LAN** or **DMZ** and click **Apply**. Otherwise, click **Reset** to restore the previous configuration. The radio buttons correspond to Ethernet ports on the front panel of the ZyWALL. By default, ports 1 to 4 are all LAN ports.

CHAPTER 6
Wireless LAN and Authentication Server

This chapter discusses how to configure Wireless LAN and Auth Server on the ZyWALL.

6.1 Wireless LAN Overview

This section introduces the wireless LAN (WLAN) and some basic scenarios.

6.1.1 Additional Installation Requirements for Using 802.1x

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

6.2 Wireless LAN Basics

This section provides background information on WLAN.

6.2.1 Channel

A channel is the radio frequency(ies) used by IEEE 802.11b wireless devices. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a different channel than an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

6.2.2 ESS ID

An Extended Service Set (ESS) is a group of access points or wireless gateways connected to a wired LAN on the same subnet. An ESS ID uniquely identifies each set. All access points or wireless gateways and their associated wireless stations in the same set must have the same ESSID.

6.2.3 RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they cannot hear each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

Figure 32 RTS Threshold
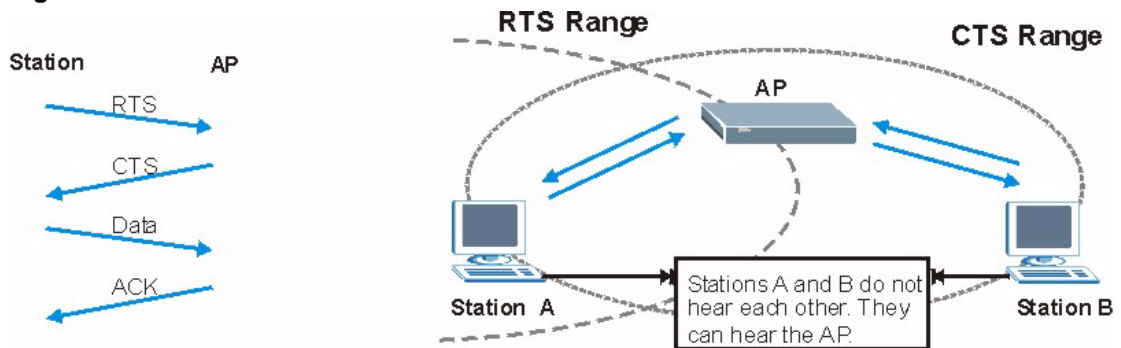
When station **A** sends data to the ZyWALL, it might not know that the station **B** is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

RTS/CTS is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the cost of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

6.2.4 Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the ZyWALL will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS Threshold** size.

6.3 Wireless Security

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

The figure below shows the possible wireless security levels on your ZyWALL. EAP (Extensible Authentication Protocol) is used for authentication and utilizes dynamic WEP key exchange. It requires interaction with a RADIUS (Remote Authentication Dial-In User Service) server either on the WAN or your LAN to provide authentication service for wireless stations.

Figure 33   ZyWALL Wireless Security Levels
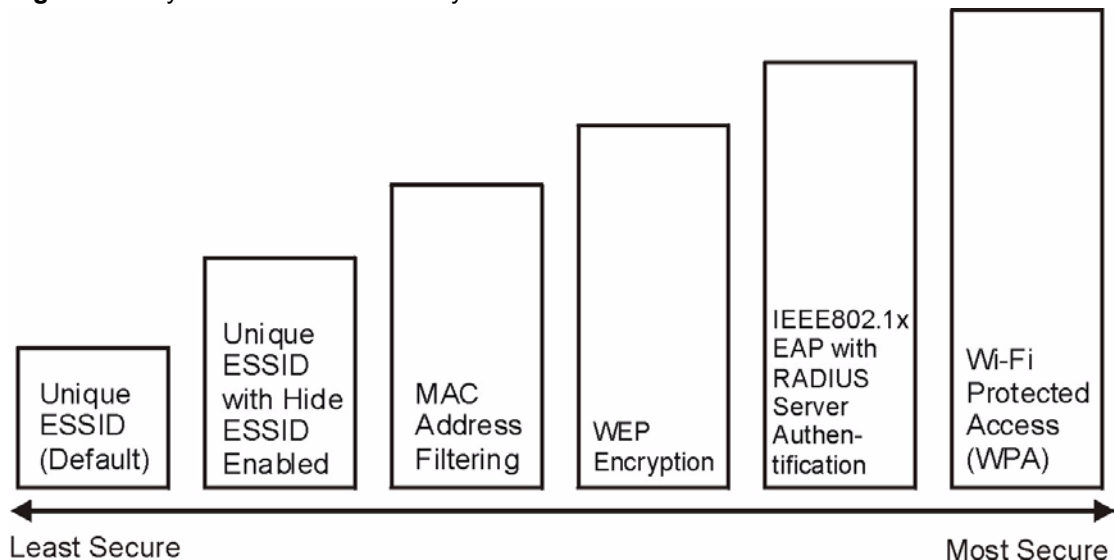
If you do not enable any wireless security on your ZyWALL, your network is accessible to any wireless networking device that is within range.

Use the ZyWALL web configurator to configurator to set up your wireless LAN security settings. Refer to the chapter on using the ZyWALL web configurator to see how to access the web configurator.

6.4 Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each Authentication Method/ key management protocol type. You enter manual keys by first selecting **64-bit WEP** or **128-bit WEP** from the **WEP Encryption** field and then typing the keys (in ASCII or hexadecimal format) in the key text boxes. MAC address filters are not dependent on how you configure these security features.

Table 28   Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	WEP	No	Enable
WPA	TKIP	No	Enable
WPA-PSK	WEP	Yes	Enable
WPA-PSK	TKIP	Yes	Enable

6.5 WEP Encrytion

WEP (Wired Equivalent Privacy) as specified in the IEEE 802.11 standard provides methods for both data encryption and wireless station authentication. WEP provides a mechanism for encrypting data using encryption keys. Both the AP and the wireless stations must use the same WEP key to encrypt and decrypt data. Your ZyWALL allows you to configure up to four 64-bit or 128-bit WEP keys, but only one key can be used at any one time.

6.6 802.1x Overview

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

6.7 Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the Wireless screen. You may still configure and store keys here, but they will not be used while Dynamic WEP is enabled.

To use Dynamic WEP, enable and configure the RADIUS server (see the Introduction to RADIUS section) and enable Dynamic WEP Key Exchange in the 802.1x screen. Ensure that the wireless station's EAP type is configured to one of the following:

- EAP-TLS
- EAP-TTLS
- PEAP

> **Note:** EAP-MD5 cannot be used with Dynamic WEP Key Exchange.

6.8 Introduction to WPA

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

6.8.1 User Authentication

WPA applies IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. You can't use the ZyWALL's Local User Database for WPA authentication purposes since the Local User Database uses EAP-MD5 which cannot be used to generate keys. See later in this chapter and the appendices for more information on IEEE 802.1x, RADIUS and EAP.

Therefore, if you don't have an external RADIUS server you should use WPA-PSK (WPA - Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a client will be granted access to a WLAN.

6.8.2 Encryption

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

Temporal Key Integrity Protocol (TKIP) uses 128-bit keys that are dynamically generated and distributed by the authentication server. It includes a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

TKIP regularly changes and rotates the encryption keys so that the same encryption key is never used twice. The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), TKIP makes it much more difficult to decode data on a Wi-Fi network than WEP, making it difficult for an intruder to break into the network.

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

6.9 WPA-PSK Application Example

A WPA-PSK application looks as follows.

1 First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters (including spaces and symbols).

2 The AP checks each client's password and (only) allows it to join the network if it matches its password.

3 The AP derives and distributes keys to the wireless clients.

4 The AP and wireless clients use the TKIP encryption process to encrypt data exchanged between them.

Figure 34 WPA-PSK Authentication
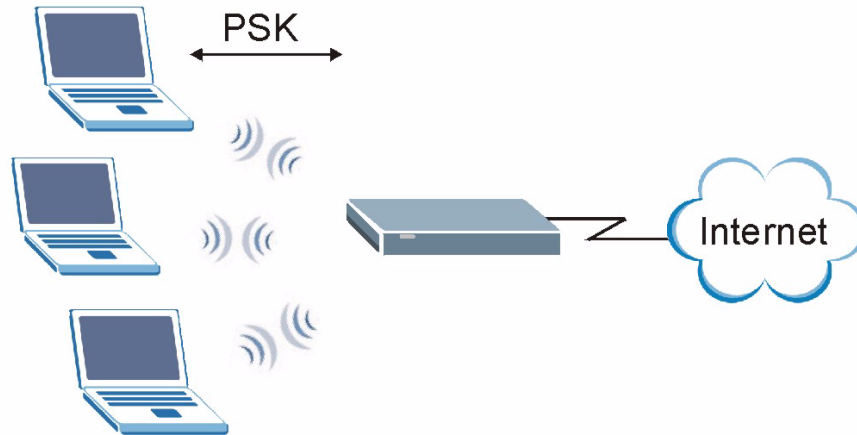
6.10 WPA with RADIUS Application Example

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

1 The AP passes the wireless client's authentication request to the RADIUS server.

2 The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.

3 The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

Figure 35   WPA with RADIUS Application Example
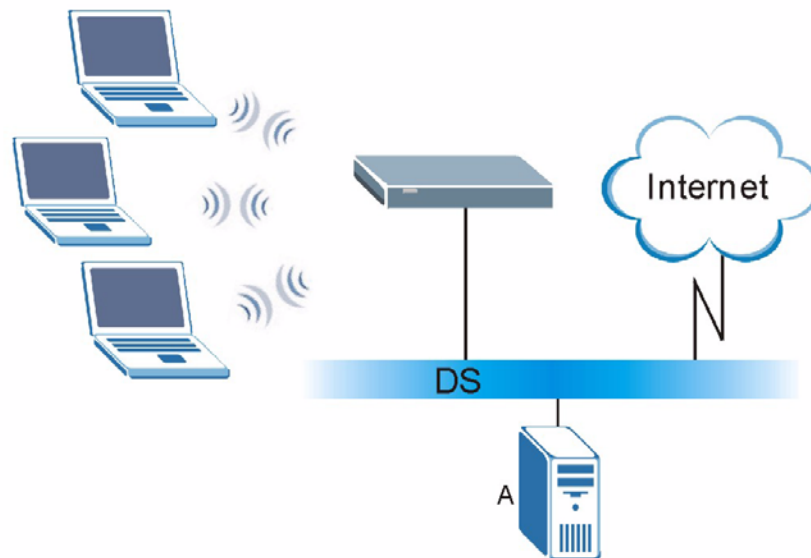
6.11 Wireless Client WPA Supplicants

A wireless client supplicant is the software that runs on an operating system instructing the wireless client how to use WPA. At the time of writing, the most widely available supplicants are the WPA patch for Windows XP, Funk Software's Odyssey client, and Meetinghouse Data Communications' AEGIS client.

The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

6.12 Inserting a PCMCIA/CardBus Wireless LAN Card

Use a ZyAIR series wireless LAN PCMCIA/CardBus card to add optional wireless LAN capabilities.

1 Turn off the ZyWALL.

> **Note:** Never insert or remove a wireless LAN card when the ZyWALL is turned on.

2 Locate the slot labeled **Wireless LAN** on the ZyWALL.

3 With its pin connector facing the slot and the LED side facing upwards, slide the ZyAIR wireless LAN card into the slot.

> **Note:** Never force, bend or twist the wireless LAN card into the slot.

4 Turn on the ZyWALL. The **WLAN** LED should turn on.

6.13 Configuring Wireless LAN

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

Click **WIRELESS LAN** to open the **Wireless** screen. The screen varies according to the security features you select.

Figure 36   Wireless: No Security

The following table describes the labels in this screen.

Table 29   Wireless: No Security

LABEL	DESCRIPTION
Enable Wireless LAN	The wireless LAN is turned off by default, before you enable the wireless LAN you should configure some security by setting MAC filters and/or 802.1x security; otherwise your wireless LAN will be vulnerable upon enabling it. Select the check box to enable the wireless LAN.
ESSID	(Extended Service Set IDentity) The ESSID identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same ESSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN.
Hide ESSID	Select to hide the ESSID in the outgoing beacon frame so a station cannot obtain the ESSID through passive scanning.
Channel ID	This allows you to set the operating frequency/channel depending on your particular region. Select a channel from the drop-down list box.
RTS/CTS Threshold	(Request To Send) The threshold (number of bytes) for enabling RTS/CTS handshake. Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this attribute to be larger than the maximum MSDU (MAC service data unit) size turns off the RTS/CTS handshake. Setting this attribute to zero turns on the RTS/CTS handshake. Enter a value between **0** and **2432**.
Fragmentation Threshold	The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter a value between **256** and **2432**.
Security	Choose from one of the security settings listed in the drop-down box. • No Security • Static WEP • WPA-PSK • WPA • 802.1x + Dynamic WEP • 802.1x + Static WEP • 802.1x + No WEP • No Access 802.1x + Static WEP • No Access 802.1x + No WEP Select **No Security** to allow wireless stations to communicate with the access points without any data encryption. Otherwise, select the security you need and see the following sections for more information.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

6.13.1 Static WEP

Static WEP provides a mechanism for encrypting data using encryption keys. Both the AP and the wireless stations must use the same WEP key to encrypt and decrypt data. Your ZyWALL allows you to configure up to four 64-bit or 128-bit WEP keys, but only one key can be used at any one time.

In order to configure and enable WEP encryption, click the **WIRELESS LAN** link to display the **Wireless** screen. Select **Static WEP** from the **Security** list.

Figure 37 Wireless: Static WEP

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

Table 30 Wireless: Static WEP

LABEL	DESCRIPTION
Security	Select **Static WEP** from the drop-down list.
WEP Encryption	WEP (Wired Equivalent Privacy) provides data encryption to prevent unauthorized wireless stations from accessing data transmitted over the wireless network. Select **64-bit WEP** or **128-bit WEP** to enable data encryption.
Key 1 to Key 4	If you chose **64-bit WEP** in the **WEP Encryption** field, then enter any 5 characters (ASCII string) or 10 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key. If you chose **128-bit WEP** in the **WEP Encryption** field, then enter 13 characters (ASCII string) or 26 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key. There are four data encryption keys to secure your data from eavesdropping by unauthorized wireless users. The values for the keys must be set up exactly the same on the access points as they are on the wireless stations.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

6.13.2 WPA-PSK

Select **WPA-PSK** from the **Security** list.

Figure 38 Wireless: WPA-PSK
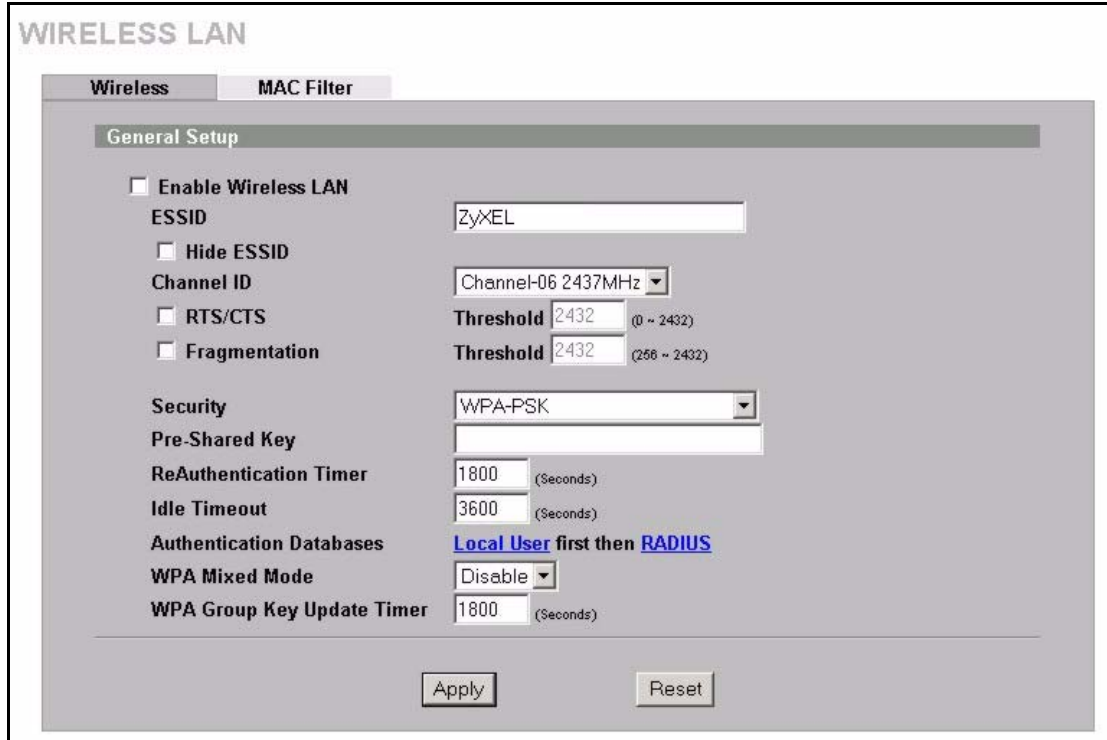
The following fields are only available when you select **WPA-PSK** in the **Security** drop down list-box.

Table 31 Wireless: WPA-PSK

LABEL	DESCRIPTION
Security	Select **WPA-PSK** from the drop-down list.
Pre-Shared Key	The encryption mechanisms used for **WPA** and **WPA-PSK** are the same. The only difference between the two is that **WPA-PSK** uses a simple common password, instead of user-specific credentials.
	Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).
ReAuthentication Timer (Seconds)	Specify how often wireless stations have to reenter usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds.
	If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout (Seconds)	The ZyWALL automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed.
Authentication Databases	Click **Local User** to go to the **Local User Database** screen where you can view and/or edit the list of users and passwords. Click **RADIUS** to go to the **RADIUS** screen where you can configure the ZyWALL to check an external RADIUS server
WPA Mixed Mode	The ZyWALL can operate in WPA Mixed Mode, which supports both clients running WPA and clients running WEP security in the same Wi-Fi network.
	Select **Enable** to activate WPA mixed mode. Otherwise, select **Disable**.

Table 31 Wireless: WPA-PSK (continued)

LABEL	DESCRIPTION
WPA Group Key Update Timer (Seconds)	The **WPA Group Key Update Timer** is the rate at which the AP (if using **WPA-PSK** key management) or RADIUS server (if using **WPA** key management) sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the **WPA Group Key Update Timer** is also supported in **WPA-PSK** mode.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

6.13.3 WPA

Select **WPA** from the **Security** list.

Figure 39   Wireless: WPA

The following fields are only available when you select **WPA-PSK** in the **Security** drop down list-box.

Table 32   Wireless: WPA

LABEL	DESCRIPTION
Security	Select **WPA** from the drop-down list.
ReAuthentication Timer (Seconds)	Specify how often wireless stations have to reenter usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.

Table 32 Wireless: WPA (continued)

LABEL	DESCRIPTION
Idle Timeout (Seconds)	The ZyWALL automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed.
Authentication Databases	Click **Local User** to go to the **Local User Database** screen where you can view and/or edit the list of users and passwords. Click **RADIUS** to go to the **RADIUS** screen where you can configure the ZyWALL to check an external RADIUS server
WPA Mixed Mode	The ZyWALL can operate in WPA Mixed Mode, which supports both clients running WPA and clients running WEP security in the same Wi-Fi network. Select **Enable** to activate WPA mixed mode. Otherwise, select **Disable**.
WPA Group Key Update Timer (Seconds)	The **WPA Group Key Update Timer** is the rate at which the AP (if using **WPA-PSK** key management) or RADIUS server (if using **WPA** key management) sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the **WPA Group Key Update Timer** is also supported in **WPA-PSK** mode.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

6.13.4 802.1x + Dynamic WEP

Select **802.1x + Dynamic WEP** from the **Security** list.

Figure 40 Wireless: 802.1x + Dynamic WEP

The following fields are only available when you select **802.1x + Dynamic WEP** in the **Security** drop down list-box.

Table 33 Wireless: 802.1x + Dynamic WEP

LABEL	DESCRIPTION
Security	Select **WPA** from the drop-down list.
ReAuthentication Timer (Seconds)	Specify how often wireless stations have to reenter usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout (Seconds)	The ZyWALL automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed.
Authentication Databases	Click **Local User** to go to the **Local User Database** screen where you can view and/or edit the list of users and passwords. Click **RADIUS** to go to the **RADIUS** screen where you can configure the ZyWALL to check an external RADIUS server
Dynamic WEP Key Exchange	Select **64-bit WEP** or **128-bit WEP** to enable data encryption. Up to 32 stations can access the ZyWALL when you configure dynamic WEP key exchange.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

6.13.5 802.1x + Static WEP

Select **802.1x + Static WEP** from the **Security** list.

Figure 41 Wireless: 802.1x + Static WEP
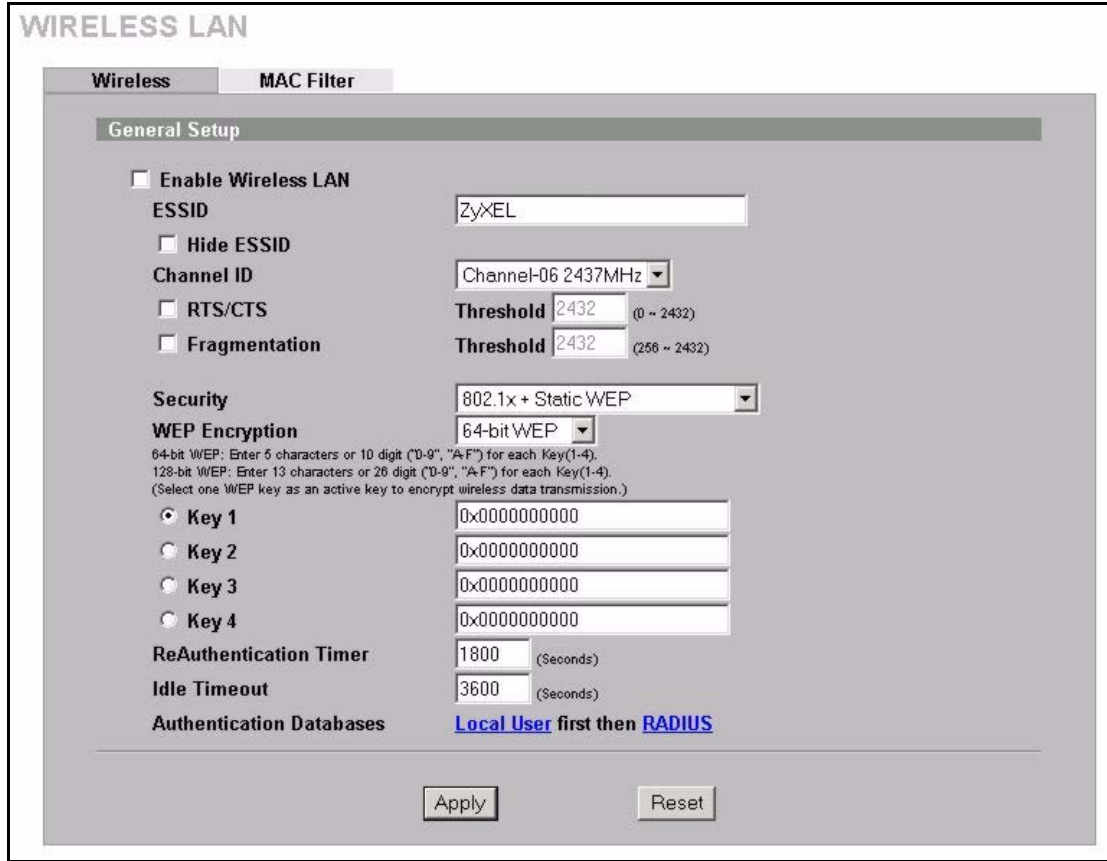
The following table describes the wireless LAN security labels in this screen.

Table 34 Wireless: 802.1x + Static WEP

LABEL	DESCRIPTION
Security	Select **802.1x + Static WEP** from the drop-down list.
WEP Encryption	WEP (Wired Equivalent Privacy) provides data encryption to prevent unauthorized wireless stations from accessing data transmitted over the wireless network. Select **64-bit WEP** or **128-bit WEP** to enable data encryption.
Key 1 to Key 4	If you chose **64-bit WEP** in the **WEP Encryption** field, then enter any 5 characters (ASCII string) or 10 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key. If you chose **128-bit WEP** in the **WEP Encryption** field, then enter 13 characters (ASCII string) or 26 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key. There are four data encryption keys to secure your data from eavesdropping by unauthorized wireless users. The values for the keys must be set up exactly the same on the access points as they are on the wireless stations.
ReAuthentication Timer (Seconds)	Specify how often wireless stations have to reenter usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout (Seconds)	The ZyWALL automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed.

Table 34 Wireless: 802.1x + Static WEP (continued)

LABEL	DESCRIPTION
Authentication Databases	Click **Local User** to go to the **Local User Database** screen where you can view and/or edit the list of users and passwords. Click **RADIUS** to go to the **RADIUS** screen where you can configure the ZyWALL to check an external RADIUS server
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

6.13.6 802.1x + No WEP

Select **802.1x + No WEP** from the **Security** list.

Figure 42 Wireless: 802.1x + No WEP

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

Table 35 Wireless: 802.1x + No WEP

LABEL	DESCRIPTION
Security	Select **802.1x + No WEP** from the drop-down list.
ReAuthenticati on Timer (Seconds)	Specify how often wireless stations have to reenter usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout (Seconds)	The ZyWALL automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed.
Authentication Databases	Click **Local User** to go to the **Local User Database** screen where you can view and/or edit the list of users and passwords. Click **RADIUS** to go to the **RADIUS** screen where you can configure the ZyWALL to check an external RADIUS server

Table 35   Wireless: 802.1x + No WEP (continued)

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

6.13.7 No Access 802.1x + Static WEP

Select **No Access 802.1x + Static WEP** to deny all wireless stations access to your wired network and allow wireless stations to communicate with the ZyWALL using static WEP keys for data encryption.

Figure 43   Wireless: No Access 802.1x + Static WEP
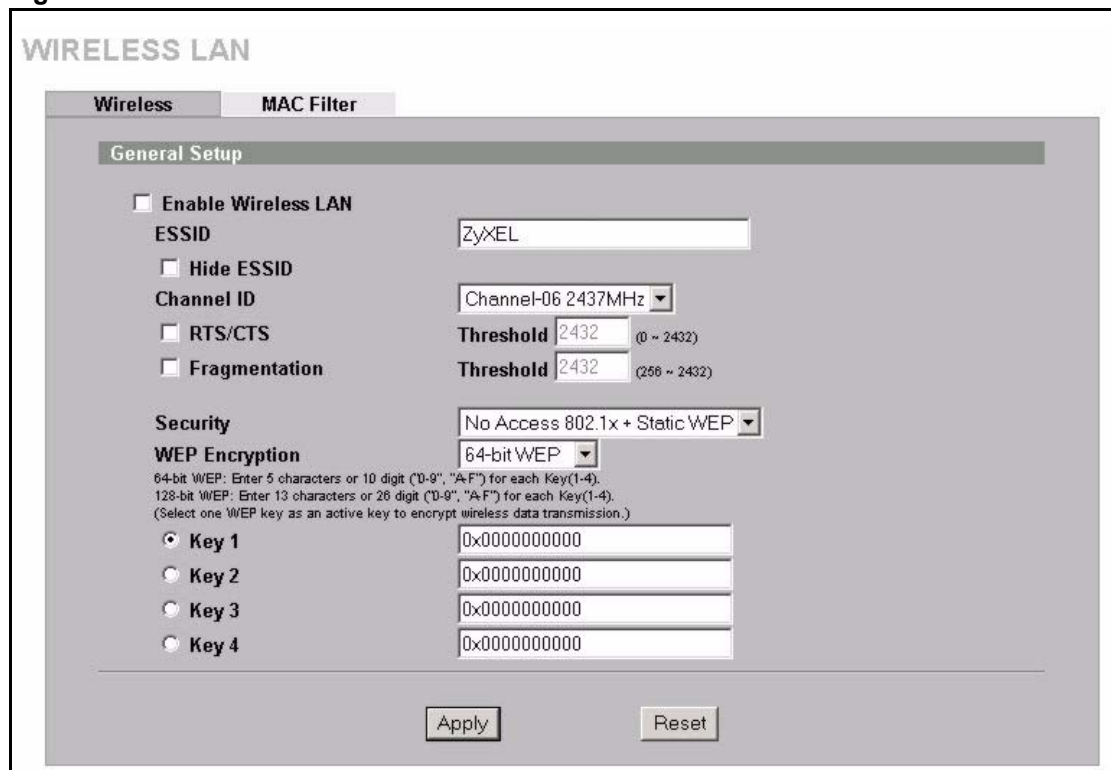
The following table describes the wireless LAN security labels in this screen.

Table 36   Wireless: No Access 802.1x + Static WEP

LABEL	DESCRIPTION
Security	Select **No Access 802.1x + Static WEP** from the drop-down list.
WEP Encryption	WEP (Wired Equivalent Privacy) provides data encryption to prevent unauthorized wireless stations from accessing data transmitted over the wireless network. Select **64-bit WEP** or **128-bit WEP** to enable data encryption.

Table 36   Wireless: No Access 802.1x + Static WEP (continued)

LABEL	DESCRIPTION
Key 1 to Key 4	If you chose **64-bit WEP** in the **WEP Encryption** field, then enter any 5 characters (ASCII string) or 10 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key. If you chose **128-bit WEP** in the **WEP Encryption** field, then enter 13 characters (ASCII string) or 26 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key. There are four data encryption keys to secure your data from eavesdropping by unauthorized wireless users. The values for the keys must be set up exactly the same on the access points as they are on the wireless stations.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

6.13.8 No Access 802.1x + No WEP

Select **No Access 802.1x + No WEP** to deny all wireless stations access to your wired network and block all wireless stations from communicating with the ZyWALL.

6.14 Configuring MAC Filter

The MAC filter screen allows you to configure the ZyWALL to give exclusive access to specific devices (**Allow Association**) or exclude specific devices from accessing the ZyWALL (**Deny Association**). Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC addresses of the devices to configure this screen.

To change your ZyWALL's MAC filter settings, click **WIRELESS LAN**, then the **MAC Filter** tab. The screen appears as shown.

Figure 44 MAC Address Filter

The following table describes the labels in this menu.

Table 37 MAC Address Filter

LABEL	DESCRIPTION
Active	Select or clear the check box to enable or disable MAC address filtering.
	Enable MAC address filtering to have the router allow or deny access to wireless stations based on MAC addresses. Disable MAC address filtering to have the router not perform MAC filtering on the wireless stations.
Association	Define the filter action for the list of MAC addresses in the MAC address filter table.
	Select **Deny** to block access to the router, MAC addresses not listed will be allowed to access the router. Select **Allow** to permit access to the router, MAC addresses not listed will be denied access to the router.
#	This is the index number of the MAC address.
User Name	Enter a descriptive name for the MAC address.
MAC Address	Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the wireless stations that are allowed or denied access to the ZyWALL in these address fields.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

6.15 Introduction to RADIUS

RADIUS is based on a client-sever model that supports authentication and accounting, where access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks among others:

- **Authentication**

  Determines the identity of the users.

- **Accounting**

  Keeps track of the client's network activity.

RADIUS user is a simple package exchange in which your ZyWALL acts as a message relay between the wireless station and the network RADIUS server.

6.15.1 Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- **Access-Request**

  Sent by an access point requesting authentication.

- **Access-Reject**

  Sent by a RADIUS server rejecting access.

- **Access-Accept**

  Sent by a RADIUS server allowing access.

- **Access-Challenge**

  Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- **Accounting-Request**

  Sent by the access point requesting accounting.

- **Accounting-Response**

  Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

6.15.2 EAP Authentication Overview

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, the access point helps a wireless station and a RADIUS server perform authentication.

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

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

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

Figure 45 EAP Authentication
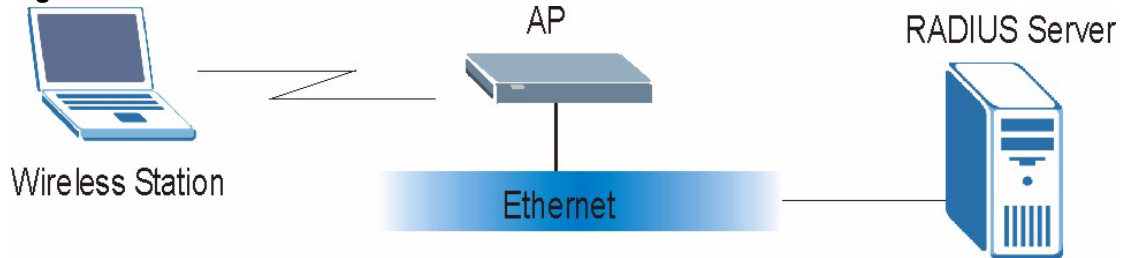
The details below provide a general description of how IEEE 802.1x EAP authentication works. For an example list of EAP-MD5 authentication steps, see Appendix G Wireless LAN With IEEE 802.1x on the IEEE 802.1x.

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

6.16 Introduction to Local User Database

By storing user profiles locally on the ZyWALL, your ZyWALL is able to authenticate wireless users without interacting with a network RADIUS server. However, there is a limit on the number of users you may authenticate in this way.

6.17 Authentication Server

A ZyWALL set to be a VPN extended authentication server can use either the local user database internal to the ZyWALL or an external RADIUS server for an unlimited number of users. The ZyWALL uses the same local user database for VPN extended authentication and wireless LAN security.

6.18 Configuring Local User Database

To change your ZyWALL's local user list, click **AUTH SERVER**. The **Local User Database** screen appears as shown.

Figure 46   Local User Database

The following table describes the labels in this screen.

Table 38 Local User Database

LABEL	DESCRIPTION
Active	Select this check box to enable the user profile.
User Name	Enter the user name of the user profile.
Password	Enter a password up to 31 characters long for this user profile.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

6.19 Configuring RADIUS

Use RADIUS if you want to authenticate wireless users using an external server.

To set up your ZyWALL's RADIUS Server settings, click **AUTH SERVER,** then the **RADIUS** tab. The screen appears as shown.

Figure 47 RADIUS

The following table describes the labels in this screen.

Table 39 RADIUS

LABEL	DESCRIPTION
Authentication Server	
Active	Select the check box to enable user authentication through an external authentication server.
	Clear the check box to enable user authentication using the local user profile on the ZyWALL.
Server IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	The default port of the RADIUS server for authentication is **1812**.
	You need not change this value unless your network administrator instructs you to do so with additional information.
Key	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the ZyWALL.
	The key is not sent over the network. This key must be the same on the external authentication server and ZyWALL.
Accounting Server	
Active	Select the check box to enable user accounting through an external authentication server.
Server IP Address	Enter the IP address of the external accounting server in dotted decimal notation.
Port Number	The default port of the RADIUS server for accounting is **1813**.
	You need not change this value unless your network administrator instructs you to do so with additional information.
Key	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the ZyWALL.
	The key is not sent over the network. This key must be the same on the external accounting server and ZyWALL.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

CHAPTER 7
WAN Screens

This chapter describes how to configure WAN settings.

7.1 WAN Overview

See Chapter 3 Wizard Setup for more information on the fields in the WAN screens.

7.2 Multiple WAN

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

The ZyWALL has two WAN ports. You can connect one port to one ISP (or network) and connect the other to a second ISP (or network).

The ZyWALL can balance the load between the two WAN ports (see the Load Balancing Introduction section).

You can use policy routing to specify the WAN port that specific services go through. An ISP may give traffic from certain (more expensive) connections priority over the traffic from other accounts. You could route delay intolerant traffic (like voice over IP calls) through this kind of connection. Other traffic could be routed through a cheaper broadband Internet connection that does not provide priority service. If one WAN port's connection goes down, the ZyWALL can automatically send its traffic through the other WAN port. See Chapter 18 Policy Route for details.

The ZyWALL's NAT feature allows you to configure sets of rules for one WAN port and separate sets of rules for the other WAN port. Refer to Chapter 16 Network Address Translation (NAT) for details.

You can select through which WAN port you want to send out traffic from UPnP-enabled applications (see Chapter 22 UPnP).

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

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

7.3 Load Balancing Introduction

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

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

7.4 Load Balancing Algorithms

The ZyWALL uses three load balancing methods (**Least Load First**, **Weighted Round Robin** and **Spillover**) to decide which WAN port the traffic for a session[1] (from the LAN) should use.

The following sections describe each load balancing method. The available bandwidth you configure on the ZyWALL refers to the actual bandwidth provided by the ISP and the measured bandwidth refers to as the bandwidth an interface is currently using.

7.4.1 Least Load First

The least load first algorithm uses the current (or recent) outbound and/or inbound bandwidth utilization of each WAN interface as the load balancing index(es) when making decisions about to which WAN interface a new LAN-originated session is to be distributed. The outbound bandwidth utilization is defined as the measured outbound throughput over the available outbound bandwidth and the inbound bandwidth utilization is defined as the measured inbound throughput over the available inbound bandwidth.

7.4.1.1 Example 1

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

---

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

Figure 48 Least Load First Example
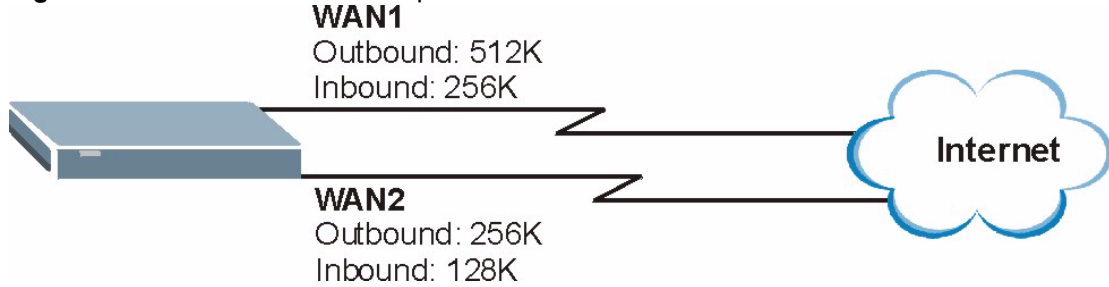
If the outbound bandwidth utilization is used as the load balancing index and the measured outbound throughput of WAN 1 is 412K and WAN 2 is 198K, the ZyWALL calculates the load balancing index as shown in the table below.

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

Table 40 Least Load First: Example 1

INTERFACE	OUTBOUND		LOAD BALANCING INDEX (M/A)
	AVAILABLE (A)	MEASURED (M)	
WAN 1	512 K	412 K	0.8
WAN 2	256 K	198 K	0.77

7.4.1.2 Example 2

This example uses the same network scenario as in Figure 48, but uses both the outbound and inbound bandwidth utilization in calculating the load balancing index. If the measured inbound stream throughput for both WAN 1 and WAN 2 is 102K, the ZyWALL calculates the average load balancing indices as shown in the table below.

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

Table 41 Least Load First: Example 2

INTERFACE	OUTBOUND		INBOUND		AVERAGE LOAD BALANCING INDEX (OM / OA + IM / IA) / 2
	AVAILABLE (OA)	MEASURED (OM)	AVAILABLE (IA)	MEASURED (IM)	
WAN 1	512 K	412 K	256 K	102 K	(0.8 + 0.4) / 2 = 0.6
WAN 2	256 K	198 K	128 K	102 K	(0.77 + 0.8) / 2 = 0.79

7.4.2 Weighted Round Robin

Similar to the Round Robin (RR) algorithm, the Weighted Round Robin (WRR) algorithm sets the ZyWALL to send traffic through each WAN interface in turn. In addition, the WAN interfaces are assigned weights. An interface with a larger weight gets more of the traffic than an interface with a smaller weight.

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

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

Figure 49   Weighted Round Robin Algorithm Example
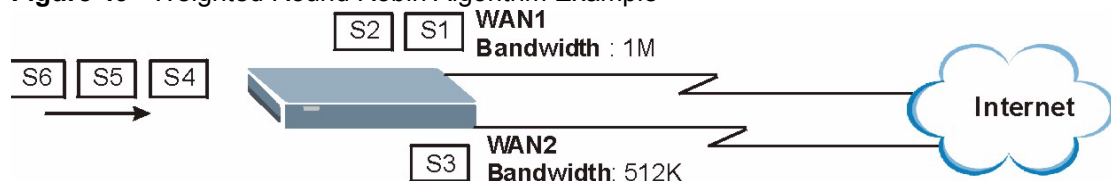
7.4.3 Spillover

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

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

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

Figure 50 Spillover Algorithm Example
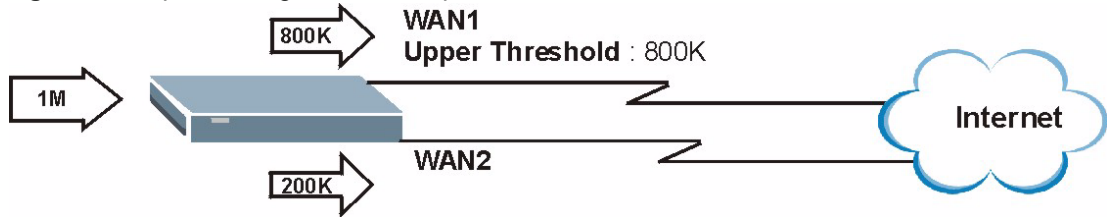
7.5 TCP/IP Priority (Metric)

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

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

2 The priorities of the WAN port routes must always be higher than the dial-backup and traffic redirect route priorities.

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

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

7.6 Configuring General

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

Figure 51   General

The following table describes the labels in this screen.

Table 42 General

LABEL	DESCRIPTION
Active/Passive (Fail Over) Mode	Select the Active/Passive (fail over) operation mode to have the ZyWALL use the second highest priority WAN port as a back up. This means that the ZyWALL will normally use the highest priority (primary) WAN port (depending on the priorities you configure in the **Route Priority** fields). The ZyWALL will switch to the secondary (second highest priority) WAN port when the primary WAN port's connection fails.
Fall Back to Primary WAN When Possible	This field determines the action the ZyWALL takes after the primary WAN port fails and the ZyWALL starts using the secondary WAN port.
	Select this check box to have the ZyWALL change back to using the primary WAN port when the ZyWALL can connect through the primary WAN port again.
	Clear this check box to have the ZyWALL continue using the secondary WAN port, even after the ZyWALL can connect through the primary WAN port again. The ZyWALL continues to use the secondary WAN port until it's connection fails (at which time it will change back to using the primary WAN port if its connection is up.
Active/Active Mode	Select **Active/Active Mode** to have the ZyWALL use both of the WAN ports at the same time and allow you to enable load balancing.
Load Balancing Algorithm	Select **Least Load First**, **Weighted Round Robin** or **Spillover** to activate load balancing and set the related fields. Otherwise, select **None**.
	Refer to the Configuring Load Balancing section for load balancing configuration.
Route Priority	
WAN1 WAN2 Traffic Redirect Dial Backup	The default WAN connection is "1' as your broadband connection via the WAN port should always be your preferred method of accessing the WAN. The ZyWALL switches from WAN port 1 to WAN port 2 if WAN port 1's connection fails and then back to WAN port 1 when WAN port 1's connection comes back up. The default priority of the routes is **WAN 1**, **WAN 2**, **Traffic Redirect** and then **Dial Backup**:
	You have three choices for an auxiliary connection (**WAN 2**, **Traffic Redirect** and **Dial Backup**) in the event that your regular WAN connection goes down. If **Dial Backup** is preferred to **Traffic Redirect**, then type "14" in the **Dial Backup Priority (metric)** field (and leave the **Traffic Redirect Priority (metric)** at the default of "15").
	The **Dial Backup** field is available only when you enable the corresponding dial backup feature in the **Dial Backup** screen.
Connectivity Check	
Check Period	The ZyWALL tests a WAN connection by periodically sending a ping to either the default gateway or the address in the **Ping this Address** field.
	Type a number of seconds (5 to 300) to set the time interval between checks. Allow more time if your destination IP address handles lots of traffic.
Check Timeout	Type the number of seconds (1 to 10) for your ZyWALL to wait for a response to the ping before considering the check to have failed. This setting must be less than the **Check Period**. Use a higher value in this field if your network is busy or congested.
Check Fail Tolerance	Type how many WAN connection checks can fail (1-10) before the connection is considered "down" (not connected). The ZyWALL still checks a "down" connection to detect if it reconnects.

Table 42 General (continued)

LABEL	DESCRIPTION
Check WAN1/2 Connectivity	Select the check box to have the ZyWALL periodically test the respective WAN port's connection.
	Select **Ping Default Gateway** to have the ZyWALL ping the WAN port's default gateway IP address.
	Select **Ping this Address** and enter a domain name or IP address of a reliable nearby computer (for example, your ISP's DNS server address) to have the ZyWALL ping that address. For a domain name, use up to 63 alphanumeric characters (hyphens, periods and the underscore are also allowed) without spaces.
Check Traffic Redirection Connectivity	Select the check box to have the ZyWALL periodically test the traffic redirect connection.
	Select **Ping Default Gateway** to have the ZyWALL ping the backup gateway's IP address.
	Select **Ping this Address** and enter a domain name or IP address of a reliable nearby computer (for example, your ISP's DNS server address) to have the ZyWALL ping that address. For a domain name, use up to 63 alphanumeric characters (hyphens, periods and the underscore are also allowed) without spaces.
Windows Networking (NetBIOS over TCP/IP):	NetBIOS (Network Basic Input/Output System) are TCP or UDP 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.
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 between WAN and DMZ	Select this check box to forward NetBIOS packets from the WAN to the DMZ and from the DMZ to the WAN.
	Clear this check box to block all NetBIOS packets going from the WAN to the DMZ and from the DMZ to the WAN.
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.

7.7 Configuring Load Balancing

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

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

7.7.1 Least Load First

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

Figure 52 Load Balancing: Least Load First

The following table describes the related fields in this screen.

Table 43 Load Balancing: Least Load First

LABEL	DESCRIPTION
Active/Active Mode	Select **Active/Active Mode** and set the related fields to enable load balancing on the ZyWALL.
Load Balancing Algorithm	Select a load balancing method to use from the drop-down list box.
Time Frame	You can set the ZyWALL to get the measured bandwidth using the average bandwidth in the specified time interval.
	Enter the time interval between 10 and 600 seconds.
Load Balancing Index(es)	Specify the direction of the traffic utilization you want the ZyWALL to use in calculating the load balancing index.
	Select **Outbound Only**, **Inbound Only** or **Outbound + Inbound**.
Interface	This field displays the name of the WAN interface (**WAN1** and **WAN2**).
Available Inbound Bandwidth	This field is applicable when you select **Outbound + Inbound** or **Inbound Only** in the **Load Balancing Index(es)** field.
	Specify the inbound (or downstream) bandwidth (in kilo bites per second) for the interface.
Available Outbound Bandwidth	This field is applicable when you select **Outbound + Inbound** or **Outbound Only** in the **Load Balancing Index(es)** field.
	Specify the outbound (or upstream) bandwidth (in kilo bites per second) for the interface.

7.7.2 Weighted Round Robin

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

Figure 53 Load Balancing: Weighted Round Robin
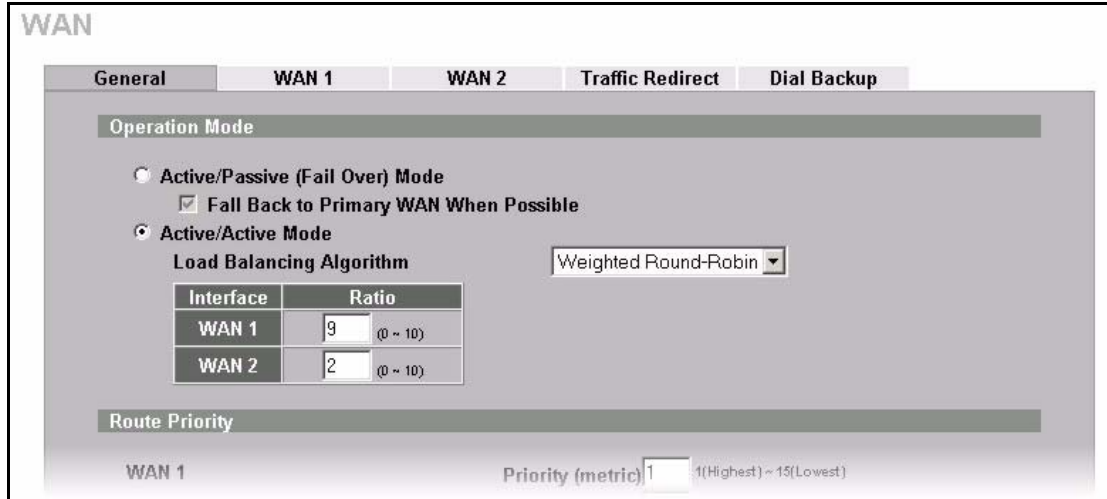
The following table describes the related fields in this screen.

Table 44 Load Balancing: Weighted Round Robin

LABEL	DESCRIPTION
Active/Active Mode	Select **Active/Active Mode** and set the related fields to enable load balancing on the ZyWALL.
Load Balancing Algorithm	Select a load balancing method to use from the drop-down list box.
Interface	This field displays the name of the WAN interface (**WAN1** and **WAN2**).
Ratio	Specify the weighted ration for the interface. Enter 0 to set the ZyWALL not to send traffic load to the interface.

7.7.3 Spillover

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

Configure the **Route Priority** metrics in the **WAN General** screen to determine the primary and secondary WANs. By default, WAN1 is the primary WAN and WAN2 is the secondary WAN.

Figure 54 Load Balancing: Spillover

The following table describes the related fields in this screen.

Table 45 Load Balancing: Spillover

LABEL	DESCRIPTION
Active/Active Mode	Select **Active/Active Mode** and set the related fields to enable load balancing on the ZyWALL.
Load Balancing Algorithm	Select a load balancing method to use from the drop-down list box.
Time Frame	You can set the ZyWALL to get the measured bandwidth using the average bandwidth in the specified time interval. Enter the time interval between 10 and 600 seconds.
Send traffic to secondary WAN when primary WAN bandwidth exceeds	Specify the maximum allowable bandwidth on the primary WAN. Once this maximum bandwidth is reached, the ZyWALL sends the new session traffic that exceeds this limit to the secondary WAN. The ZyWALL continues to send traffic of existing session to the primary WAN.

7.8 Configuring WAN Setup

To change your ZyWALL's WAN ISP, IP and MAC settings, click **WAN**, then the **WAN1** or **WAN2** tab. The screen differs by the encapsulation.

> **Note:** The WAN1 and WAN2 IP addresses must be on different subnets.

> **Note:** The warning message "Warning! No NAT rule configured in system" appears in the status bar when NAT is set to use **Full Feature** address mapping rules, but there are no NAT address mapping rules configured.

7.8.1 Ethernet Encapsulation

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

Figure 55 WAN: Ethernet Encapsulation

The following table describes the labels in this screen.

Table 46 WAN: Ethernet Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	You must choose the Ethernet option when the WAN port is used as a regular Ethernet.

Table 46   WAN: Ethernet Encapsulation (continued)

LABEL	DESCRIPTION
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.
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 16 Network Address Translation (NAT).
RIP Direction	RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. 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**.

Table 46 WAN: Ethernet Encapsulation (continued)

LABEL	DESCRIPTION
RIP Version	The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyWALL sends (it recognizes both formats when receiving).
	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.
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.

7.8.2 PPPoE Encapsulation

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

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example Radius). 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 56 WAN: PPPoE Encapsulation

The following table describes the labels not previously discussed.

Table 47 WAN: PPPoE Encapsulation

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 personal computer (PC) 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.
Nailed-Up	Select **Nailed-Up** if you do not want the connection to time out.
Idle Timeout	This value specifies the time in seconds that elapses before the ZyWALL automatically disconnects from the PPPoE server.
WAN IP Address Assignment	
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
My WAN IP Address	Enter your WAN IP address in this field if you selected **Use Fixed IP Address.**
Remote IP Subnet Mask	Enter the gateway IP subnet mask (if your ISP gave you one) in this field if you selected **Use Fixed IP Address**.
Remote IP Address	Enter the gateway IP address (if your ISP gave you one) in this field if you selected **Use Fixed IP Address**.

7.8.3 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 57   WAN: PPTP Encapsulation

The following table describes the labels not previously discussed.

Table 48 WAN: PPTP Encapsulation

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.
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.

7.9 Traffic Redirect

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

Figure 58 Traffic Redirect WAN Setup
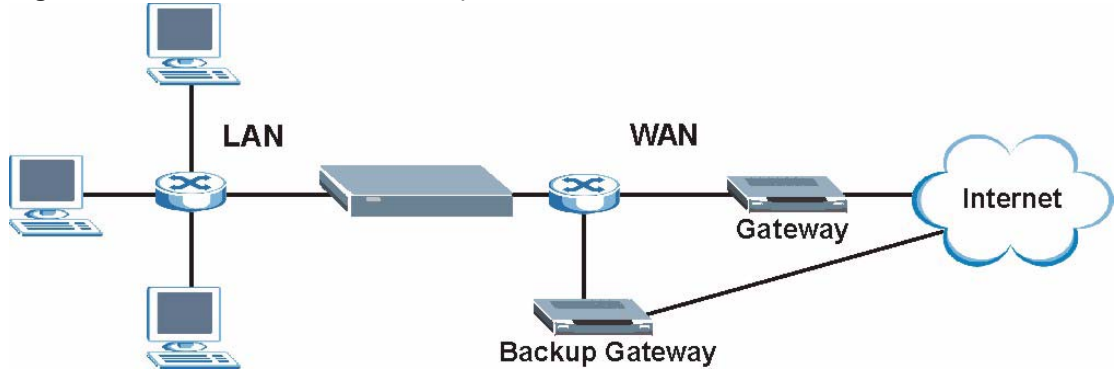
The following network topology allows you to avoid triangle route security issues (see Appendix I Triangle Route) when the backup gateway is connected to the LAN or DMZ. Use IP alias to configure the LAN into two or three logical networks with the ZyWALL itself as the gateway for each LAN network. Put the protected LAN in one subnet (Subnet 1 in the following figure) and the backup gateway in another subnet (Subnet 2). Configure a LAN to LAN/ZyWALL firewall rule that forwards packets from the protected LAN (Subnet 1) to the backup gateway (Subnet 2).

Figure 59 Traffic Redirect LAN Setup
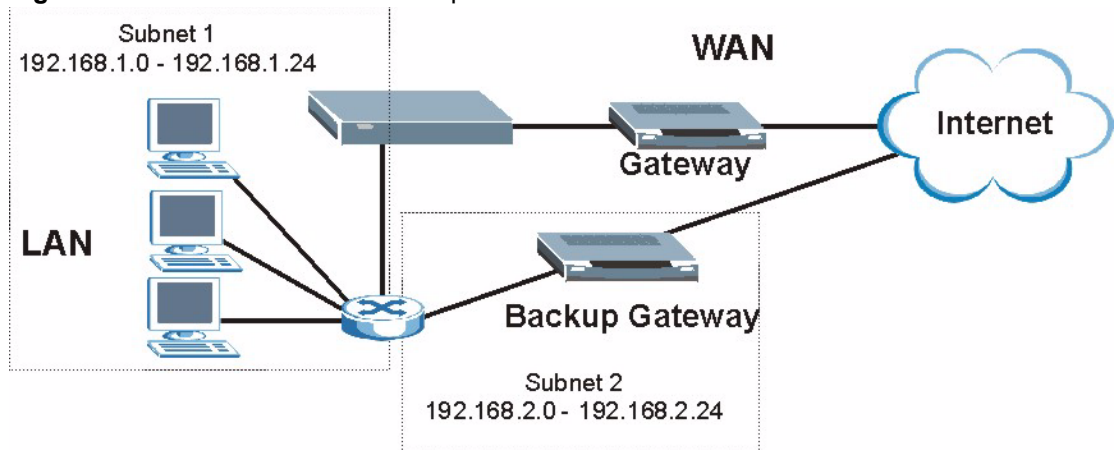
7.10 Configuring Traffic Redirect

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

Figure 60   Traffic Redirect
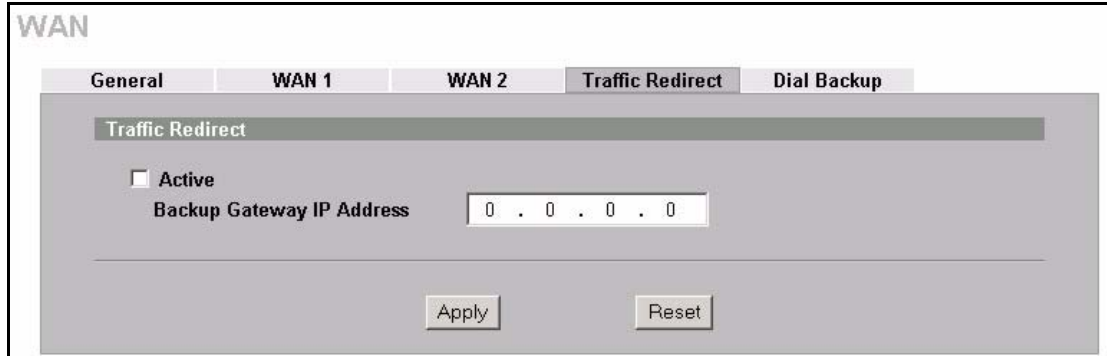
The following table describes the labels in this screen.

Table 49   Traffic Redirect

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

7.11 Configuring Dial Backup

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

Figure 61 Dial Backup Setup

The following table describes the labels in this screen.

Table 50   Dial Backup Setup

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

Table 50 Dial Backup Setup (continued)

LABEL	DESCRIPTION
Enable RIP	Select this check box to turn on RIP (Routing Information Protocol), which allows a router to exchange routing information with other routers.
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.
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**, **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.
Broadcast Dial Backup Route	Select this check box to forward the backup route broadcasts to the WAN.
Enable Multicast	Select this check box to turn on IGMP (Internet Group Multicast Protocol). IGMP is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data.
Multicast Version	Select **IGMP-v1** or **IGMP-v2**. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see *sections 4* and *5* of *RFC 2236*.
PPP Options	
PPP Encapsulation	Select **CISCO PPP** from the drop-down list box if your dial backup WAN device uses Cisco PPP encapsulation, otherwise select **Standard PPP**.
Enable Compression	Select this check box to turn on stac compression.
Budget	
Always On	Select this check box to have the dial backup connection on all of the time.
Configure Budget	Select this check box to have the dial backup connection on during the time that you select.
Allocated Budget	Type the amount of time (in minutes) that the dial backup connection can be used during the time configured in the **Period** field. Set an amount that is less than the time period configured in the **Period** field.
Period	Type the time period (in hours) for how often the budget should be reset. For example, to allow calls to this remote node for a maximum of 10 minutes every hour, set the **Allocated Budget** to 10 (minutes) and the **Period** to 1 (hour).
Idle Timeout	Type the number of seconds of idle time (when there is no traffic from the ZyWALL to the remote node) for the ZyWALL to wait before it automatically disconnects the dial backup connection. This option applies only when the ZyWALL initiates the call. The dial backup connection never times out if you set this field to "0" (it is the same as selecting **Always On**).

Table 50   Dial Backup Setup (continued)

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

7.12 Advanced Modem Setup

7.12.1 AT Command Strings

For regular telephone lines, the default Dial string tells the modem that the line uses tone dialing. `ATDT` is the command for a switch that requires tone dialing. If your switch requires pulse dialing, change the string to `ATDP`.

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

7.12.2 DTR Signal

The majority of WAN devices default to hanging up the current call when the DTR (Data Terminal Ready) signal is dropped by the DTE. When the Drop DTR When Hang Up check box is selected, the ZyWALL uses this hardware signal to force the WAN device to hang up, in addition to issuing the drop command `ATH`.

7.12.3 Response Strings

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

7.13 Configuring Advanced Modem Setup

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

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

Figure 62 Advanced Setup

The following table describes the labels in this screen.

Table 51 Advanced Setup

LABEL	DESCRIPTION
AT Command Strings	
Dial	Type the AT Command string to make a call.
Drop	Type the AT Command string to drop a call. "~" represents a one second wait, for example, "~~~+++~~ath" can be used if your modem has a slow response time.
Answer	Type the AT Command string to answer a call.
Drop DTR When Hang Up	Select this check box to have the ZyWALL drop the DTR (Data Terminal Ready) signal after the "AT Command String: Drop" is sent out.
AT Response Strings	
CLID	Type the keyword that precedes the CLID (Calling Line Identification) in the AT response string. This lets the ZyWALL capture the CLID in the AT response string that comes from the WAN device. CLID is required for CLID authentication.
Called ID	Type the keyword preceding the dialed number.
Speed	Type the keyword preceding the connection speed.
Call Control	

Table 51 Advanced Setup (continued)

LABEL	DESCRIPTION
Dial Timeout (sec)	Type a number of seconds for the ZyWALL to try to set up an outgoing call before timing out (stopping).
Retry Count	Type a number of times for the ZyWALL to retry a busy or no-answer phone number before blacklisting the number.
Retry Interval (sec)	Type a number of seconds for the ZyWALL to wait before trying another call after a call has failed. This applies before a phone number is blacklisted.
Drop Timeout (sec)	Type the number of seconds for the ZyWALL to wait before dropping the DTR signal if it does not receive a positive disconnect confirmation.
Call Back Delay (sec)	Type a number of seconds for the ZyWALL to wait between dropping a callback request call and dialing the corresponding callback call.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving.

C H A P T E R 8
DMZ Screens

This chapter describes how to configure the ZyWALL's DMZ.

8.1 DMZ Overview

The DeMilitarized Zone (DMZ) auto-negotiating 10/100 Mbps Ethernet port provides a way for public servers (Web, e-mail, FTP, etc.) to be visible to the outside world (while still being protected from DoS (Denial of Service) attacks such as SYN flooding and Ping of Death). These public servers can also still be accessed from the secure LAN.

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

It is highly recommended that you connect all of your public servers to the DMZ port. If you have more than one public server, connect a hub to the DMZ port.

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

8.2 Configuring DMZ

The DMZ port and the computers connected to it can have private or public IP addresses.

When the DMZ uses public IP addresses, the WAN and DMZ ports must use public IP addresses that are on separate subnets. See Appendix C IP Subnetting for information on IP subnetting. If you do not configure SUA NAT or any full feature NAT mapping rules for the public IP addresses on the DMZ, the ZyWALL will route traffic to the public IP addresses on the DMZ without performing NAT. This may be useful for hosting servers for NAT unfriendly applications (see Chapter 16 Network Address Translation (NAT) for more information).

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

Unlike the LAN, the ZyWALL does not assign TCP/IP configuration via DHCP to computers connected to the DMZ ports(s). Manually assign the computers static IP addresses (in the same subnet as the DMZ port's IP address), DNS server addresses and the ZyWALL's DMZ IP address as the default gateway.

From the main menu, click **DMZ**. The screen appears as shown next.

Figure 63 DMZ
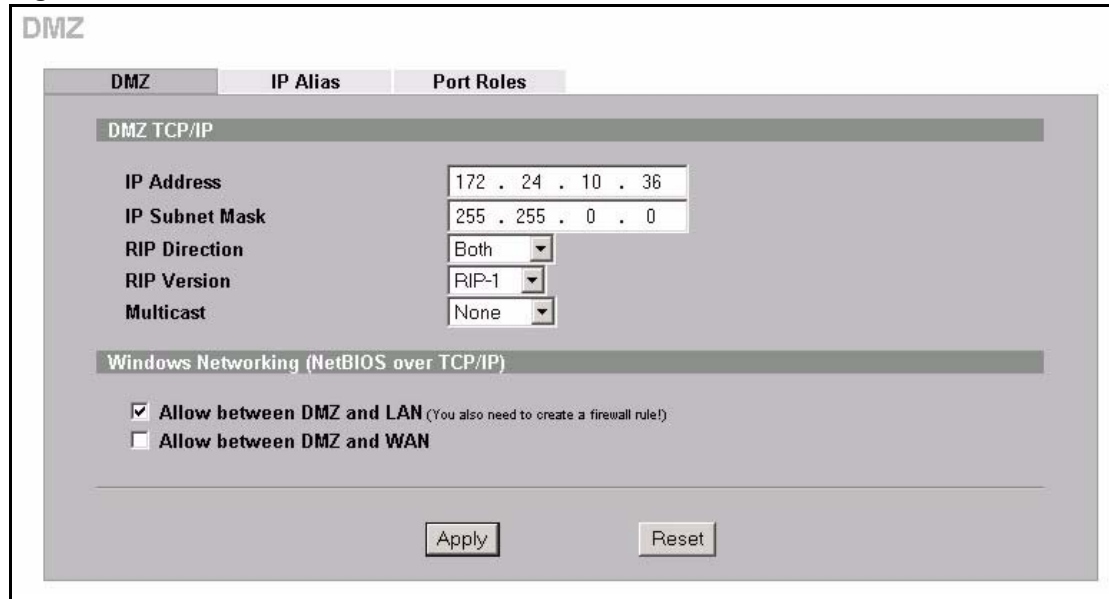
The following table describes the labels in this screen.

Table 52 DMZ

LABEL	DESCRIPTION
DMZ TCP/IP	
IP Address	Type the IP address of your ZyWALL's DMZ port in dotted decimal notation. **Note:** Make sure the IP addresses of the LAN, WAN and DMZ are on separate subnets.
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your ZyWALL will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyWALL 255.255.255.0.
RIP Direction	RIP (Routing Information Protocol, RFC1058 and RFC 1389) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Select the RIP direction from **Both**/**In Only**/**Out Only**/**None**. When set to **Both** or **Out Only**, the ZyWALL will broadcast its routing table periodically. When set to **Both** or **In Only**, it will incorporate the RIP information that it receives; when set to **None**, it will not send any RIP packets and will ignore any RIP packets received. **Both** is the default.
RIP Version	The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the ZyWALL sends (it recognizes both formats when receiving). **RIP-1** is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to **Both** and the Version set to **RIP-1**.

Table 52 DMZ (continued)

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

8.3 Configuring IP Alias

IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The ZyWALL supports three logical DMZ interfaces via its single physical Ethernet interface with the ZyWALL itself as the gateway for each DMZ network.

The IP alias IP addresses can be either private or public regardless of whether the physical DMZ interface is set to use a private or public IP address. Use NAT if you want to make DMZ computers with private IP addresses publicly accessible (see Chapter 16 Network Address Translation (NAT) for more information). When you use IP alias, you can have the DMZ use both public and private IP addresses at the same time.

> **Note:** Make sure that the subnets of the logical networks do not overlap.

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

Figure 64 IP Alias

The following table describes the labels in this screen.

Table 53 IP Alias

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

Table 53 IP Alias (continued)

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

8.4 DMZ Public IP Address Example

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

Figure 65 DMZ Public Address Example
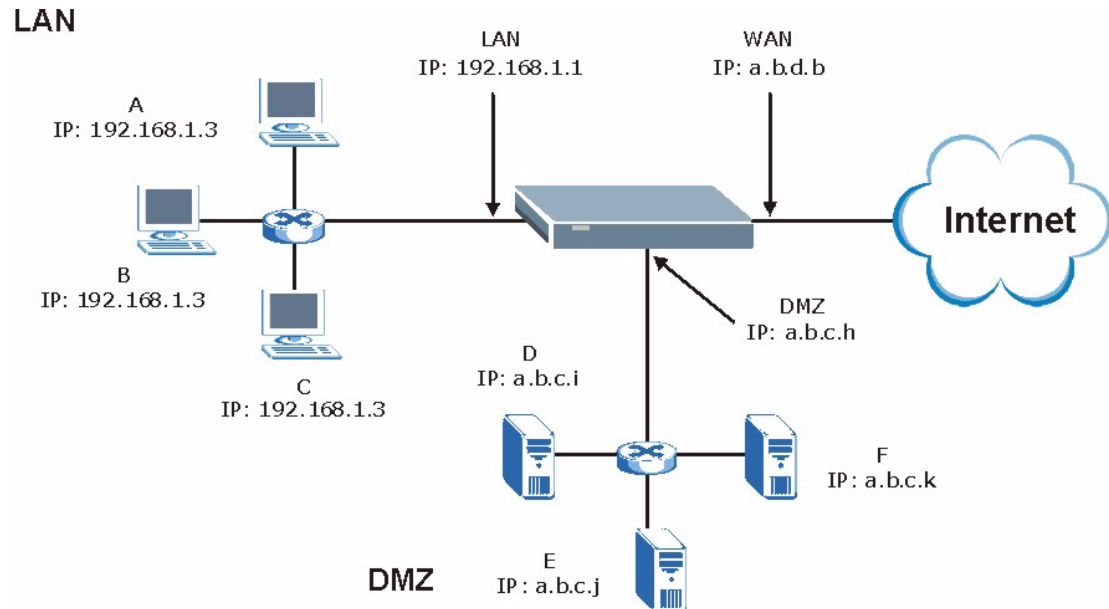
8.5 DMZ Private and Public IP Address Example

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

Configure both DMZ and DMZ IP alias to use this kind of network setup. You also need to configure NAT for the private DMZ IP addresses.

Figure 66 DMZ Private and Public Address Example

8.6 Configuring Port Roles

To configure a LAN/DMZ port as a LAN or DMZ port, select its radio button next to **LAN** or **DMZ** and click **Apply**. Otherwise, click **Reset** to restore the previous configuration. The radio buttons correspond to Ethernet ports on the front panel of the ZyWALL. By default, ports 1 to 4 are all LAN ports.

> **Note:** Do the following if you are configuring from a computer connected to a LAN or DMZ port and changing the port's role:
> 1. Make sure your computer's IP address is in the same subnet as the ZyWALL's LAN or DMZ IP address.
> 2. A port's IP address varies as its role changes, use the appropriate LAN or DMZ IP address to access the ZyWALL.

Click **DMZ**, then **Port Roles**. The screen appears as shown.

Figure 67   Port Roles
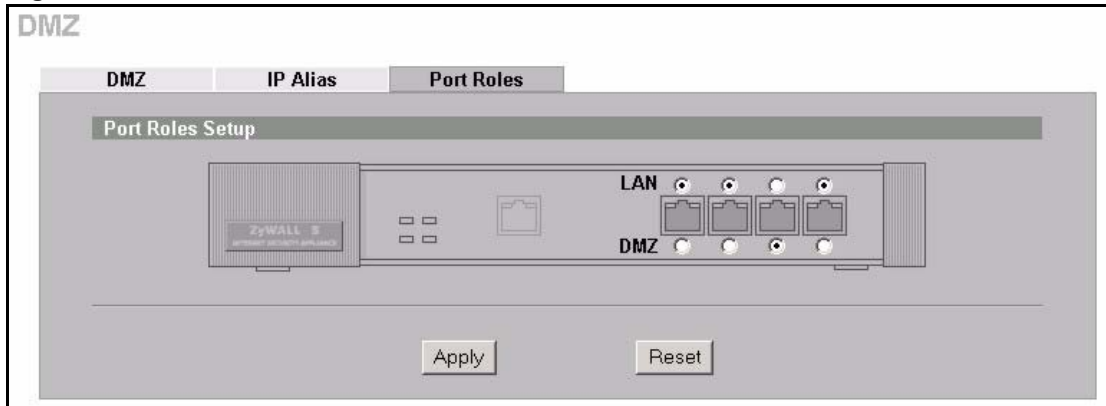
After you change the LAN/DMZ port roles and click **Apply**, please wait for few seconds until the following screen appears. Click **Return** to go back to the **Port Roles** screen.

Figure 68   Port Roles Change Complete

CHAPTER 9
Firewalls

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

9.1 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.

9.2 Types of Firewalls

There are three main types of firewalls:

1 Packet Filtering Firewalls

2 Application-level Firewalls

3 Stateful Inspection Firewalls

9.2.1 Packet Filtering Firewalls

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

9.2.2 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.

9.2.3 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 the Stateful Inspection section for more information on Stateful Inspection.

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

9.3 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 (in SMT menu 21.2 or in the web configurator). 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 allows you to physically separate the network into the following areas:

- The WAN (Wide Area Network) port(s) attaches to the broadband modem (cable or ADSL) connecting to the Internet.
- The LAN (Local Area Network) port(s) 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 69 ZyWALL Firewall Application
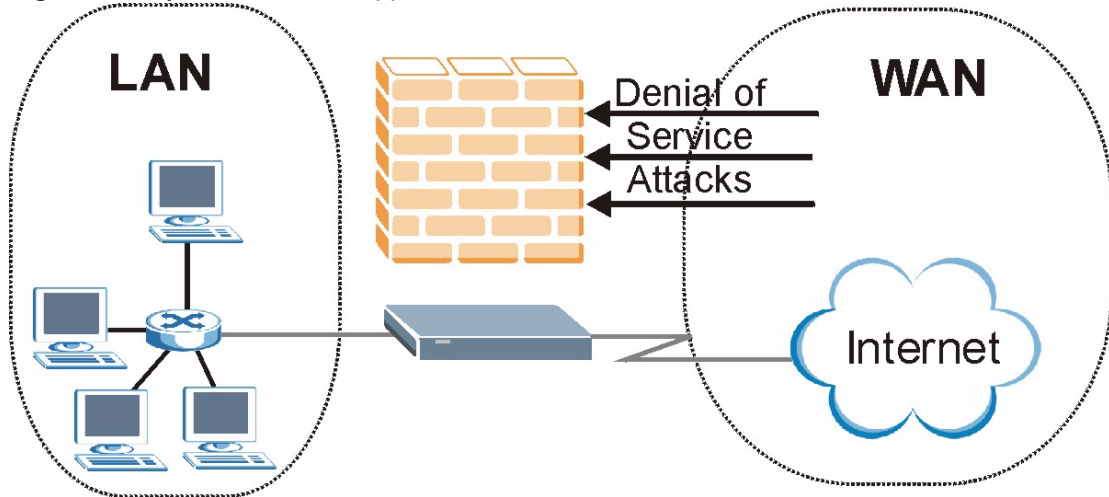
9.4 Denial of Service

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.

9.4.1 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 54 Common IP Ports

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

9.4.2 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 70   Three-Way Handshake
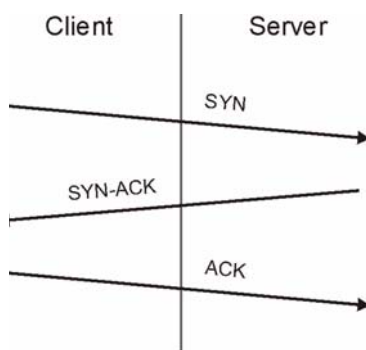
Under normal circumstances, the application that initiates a session sends a SYN (synchronize) packet to the receiving server. The receiver sends back an ACK (acknowledgment) packet and its own SYN, and then the initiator responds with an ACK (acknowledgment). After this handshake, a connection is established.

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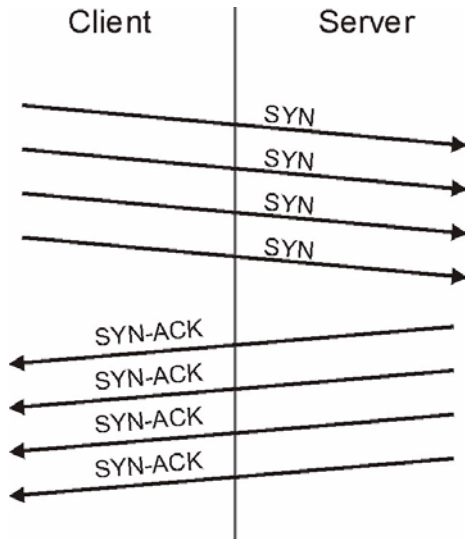
b   In a **LAND Attack**, hackers flood SYN packets into the network with a spoofed source IP address of the targeted system. This makes it appear as if the host computer sent the packets to itself, making the system unavailable while the target system tries to respond to itself.

• 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 72 Smurf Attack
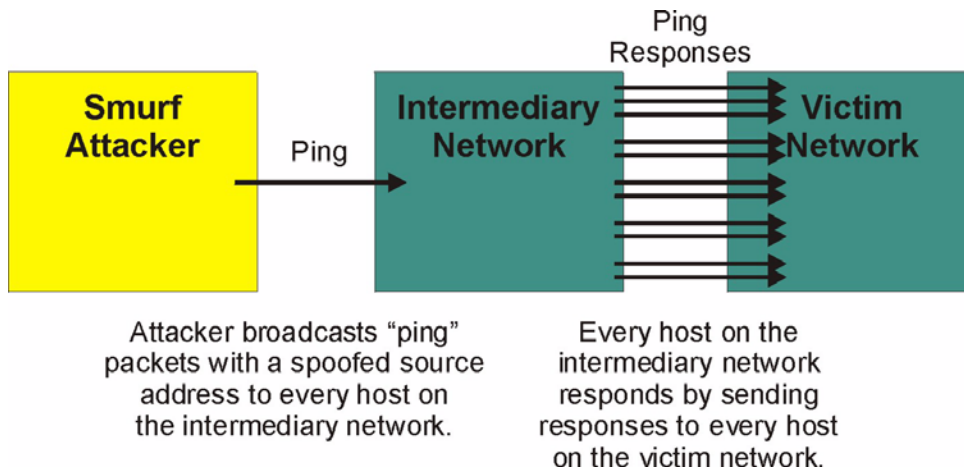
9.4.2.1 ICMP Vulnerability

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

Table 55 ICMP Commands That Trigger Alerts

5	REDIRECT
13	TIMESTAMP_REQUEST
14	TIMESTAMP_REPLY
17	ADDRESS_MASK_REQUEST
18	ADDRESS_MASK_REPLY

9.4.2.2 Illegal Commands (NetBIOS and SMTP)

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

Table 56 Legal NetBIOS Commands

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

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

Table 57 Legal SMTP Commands

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

9.4.2.3 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.

9.5 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 73 Stateful Inspection
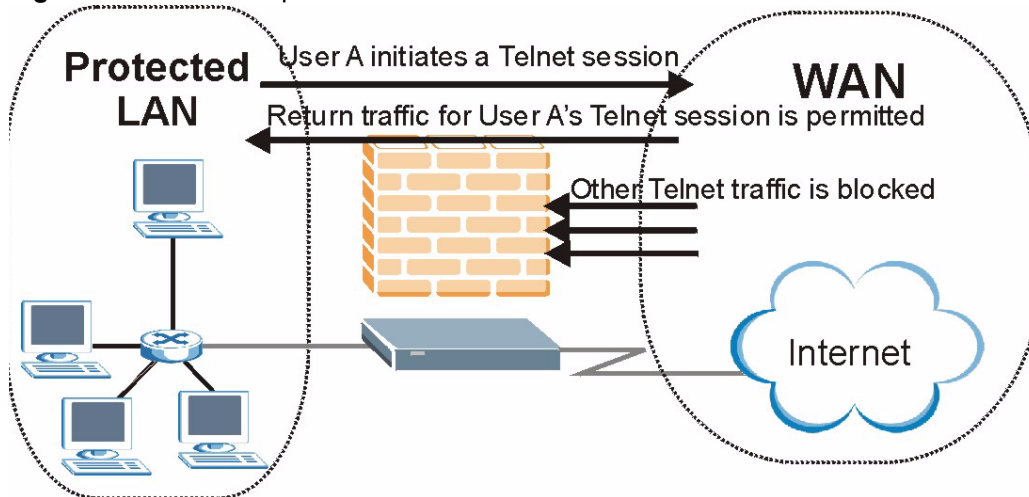
The previous figure shows the ZyWALL's default firewall rules in action as well as demonstrates how stateful inspection works. User A can initiate a Telnet session from within the LAN and responses to this request are allowed. However other Telnet traffic initiated from the WAN is blocked.

9.5.1 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.

9.5.2 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).

9.5.3 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 "Upper Layer Protocols" shown next), 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).

9.5.4 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.

9.5.5 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.

9.6 Guidelines For Enhancing Security With Your Firewall

1 Change the default password via SMT 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.

9.7 Packet Filtering Vs Firewall

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

9.7.1 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.

9.7.1.1 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.

9.7.2 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.

9.7.2.1 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.

C H A P T E R 1 0
Firewall Screens

This chapter shows you how to configure your ZyWALL firewall.

10.1 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. SMT screens allow you to activate the firewall. CLI commands provide limited configuration options and are only recommended for advanced users, please refer to Appendix N Firewall Commands for firewall CLI commands.

10.2 Firewall Policies Overview

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

• LAN to LAN/ZyWALL	• WAN to LAN	• DMZ to LAN
• LAN to WAN	• WAN to WAN/ZyWALL	• DMZ to WAN
• LAN to DMZ	• WAN to DMZ	• DMZ to DMZ/ZyWALL

> **Note:** The LAN includes both the LAN port and the WLAN.

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
• LAN to DMZ
• WAN to DMZ
• DMZ 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.

- DMZ to LAN
- DMZ to DMZ/ZyWALL

    This prevents computers on the DMZ from communicating between networks or subnets connected to the DMZ interface 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.

10.3 Rule Logic Overview

> **Note:** Study these points carefully before configuring rules.

10.3.1 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 the Types of Firewalls section)?

4 What IP services will be affected?

5 What computers on the LAN or DMZ 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.

10.3.2 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.

10.3.3 Key Fields For Configuring Rules

10.3.3.1 Action

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

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

10.3.3.2 Service

Select the service from the **Service** scrolling list box. If the service is not listed, it is necessary to first define it. See the Predefined Services section for more information on predefined services.

10.3.3.3 Source Address

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

10.3.3.4 Destination Address

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

10.4 Connection Direction Examples

This section describes examples for firewall rules for connections going from LAN to WAN and from WAN to LAN. Rules for the DMZ work in a similar fashion.

LAN to LAN/ZyWALL, WAN to WAN/ZyWALL and DMZ to DMZ/ZyWALL rules apply to packets coming in on the associated interface (LAN, WAN, or DMZ 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 and DMZ to DMZ/ZyWALL polices apply in the same way to the WAN and DMZ ports.

10.4.1 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 74   LAN to WAN Traffic
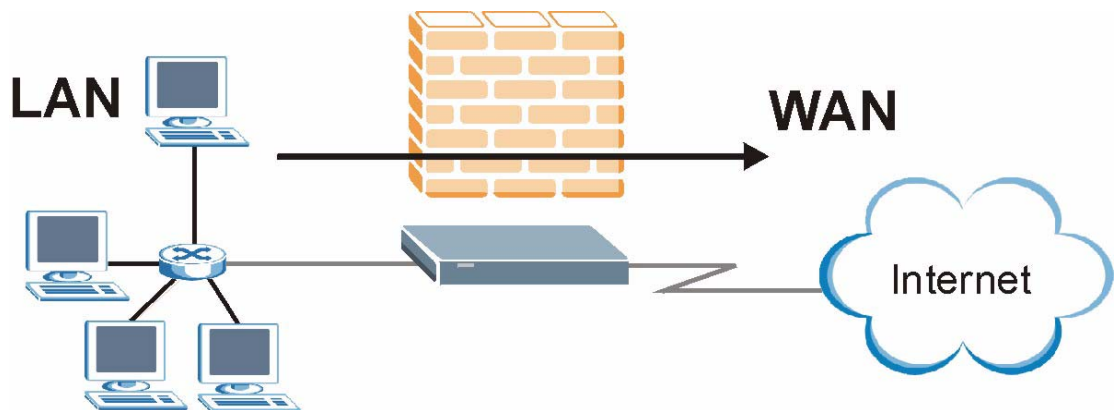
10.4.2 WAN To LAN Rules

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 75 WAN to LAN Traffic
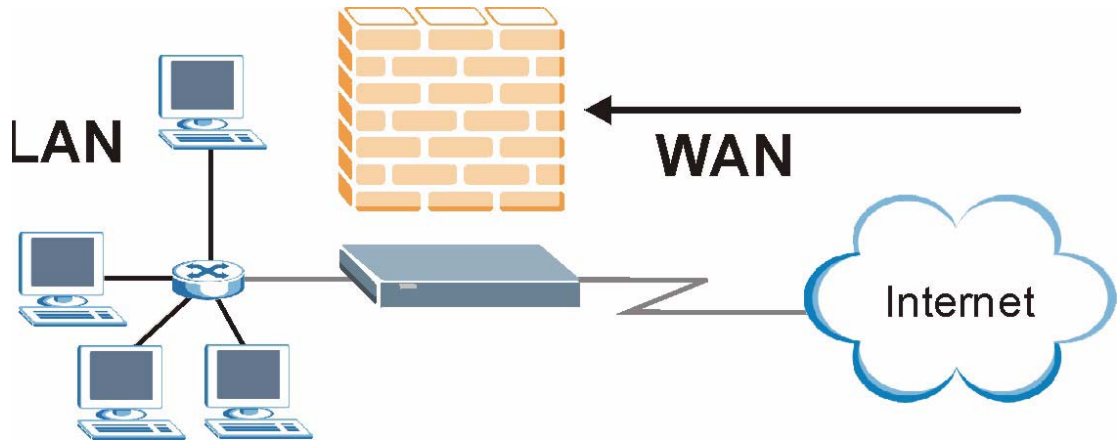
10.5 Alerts

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 79). 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.

10.6 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 76 Default Rule (Router Mode)
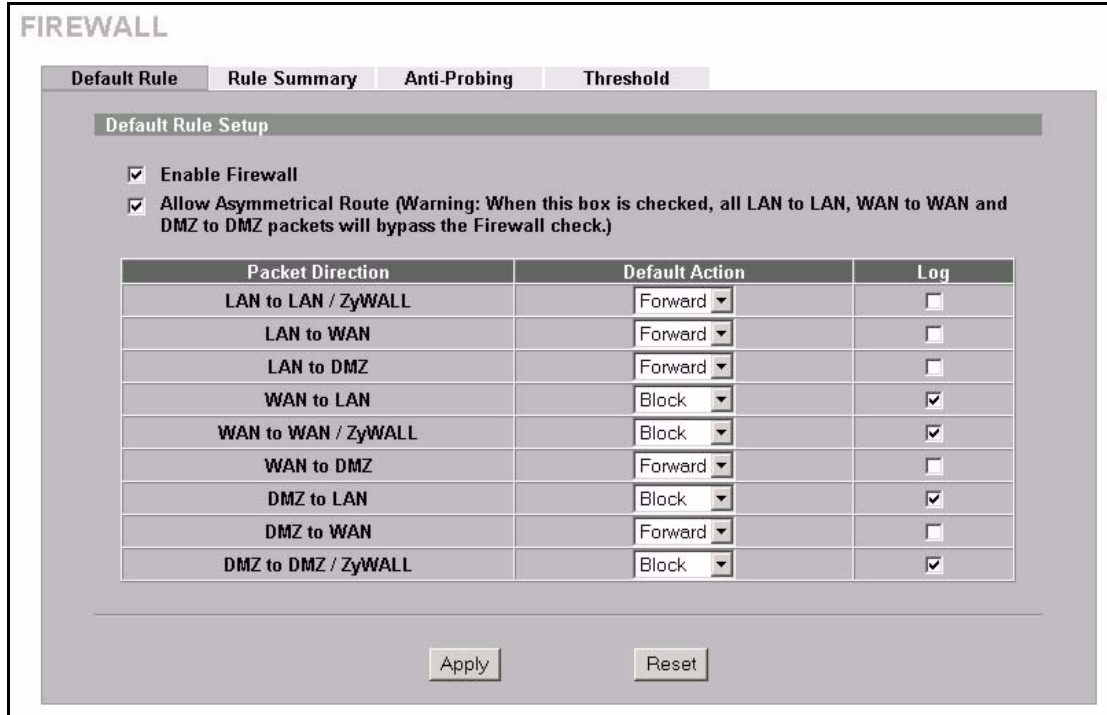
The following table describes the labels in this screen.

Table 58 Default Rule (Router Mode)

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 I Triangle Route for more on triangle route topology.
Packet Direction	This is the direction of travel of packets (**LAN to LAN/ZyWALL**, **LAN to WAN**, **LAN to DMZ**, **WAN to LAN**, **WAN to WAN/ZyWALL**, **WAN to DMZ**, **DMZ to LAN**, **DMZ to WAN** or **DMZ to DMZ/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.

Figure 77   Default Rule (Bridge Mode)

The following table describes the labels in this screen.

Table 59   Default Rule (Bridge Mode)

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 I Triangle Route for more on triangle route topology.
Packet Direction	This is the direction of travel of packets (**LAN to LAN/ZyWALL**, **LAN to WAN**, **LAN to DMZ**, **WAN to LAN**, **WAN to WAN/ZyWALL**, **WAN to DMZ**, **DMZ to LAN**, **DMZ to WAN** or **DMZ to DMZ/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.
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.
Log Broadcast Frame	Select the check box to create a log for any Layer 2 broadcast frames that are traveling in the selected direction.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to begin configuring this screen afresh.

10.6.1 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 78 Rule Summary
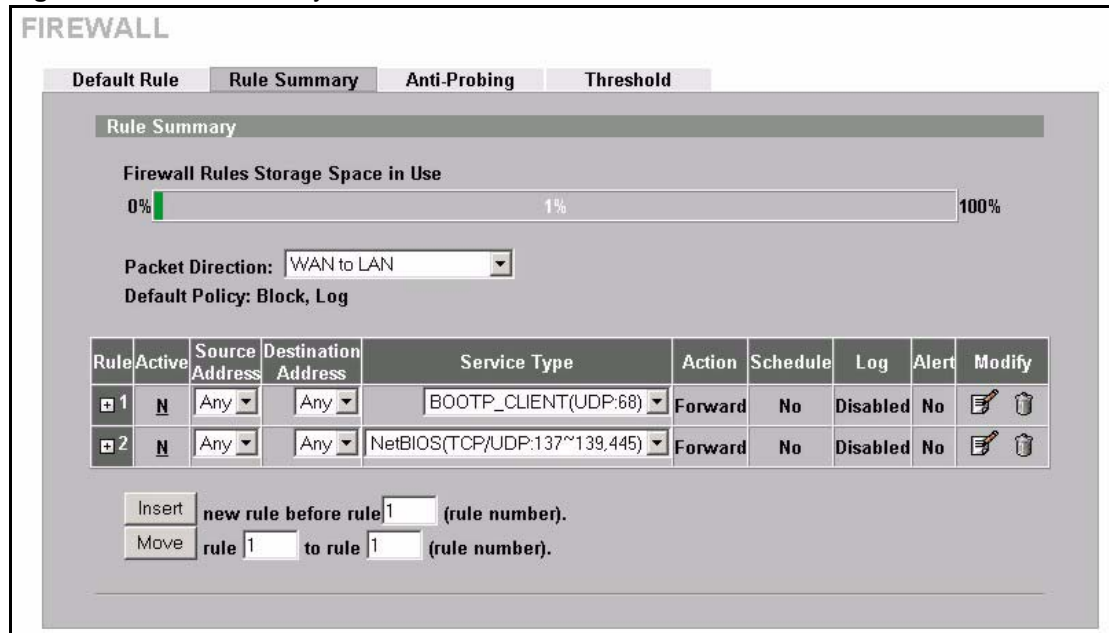
The following table describes the labels in this screen.

Table 60 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 (**LAN to LAN/ZyWALL**, **LAN to WAN**, **LAN to DMZ**, **WAN to WAN/ZyWALL**, **WAN to LAN**, **WAN to DMZ, DMZ to DMZ/ZyWALL**, **DMZ to LAN** or **DMZ to WAN**) 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**).

Table 60 Rule Summary

LABEL	DESCRIPTION
Source Address	This drop-down list box displays the source addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to **Any**.
Destination Address	This drop-down list box displays the destination addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to **Any**.
Service Type	This drop-down list box displays the services to which this firewall rule applies. Please note that a blank service type is equivalent to **Any**. See Table 63 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**).
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.

10.6.2 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 79   Creating/Editing A Firewall Rule

The following table describes the labels in this screen.

Table 61 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	Please see Table 63 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 61   Creating/Editing A Firewall Rule

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

10.6.3 Configuring Custom Services

Configure customized ports for services not predefined by the ZyWALL (see the Predefined Services section 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 80   Creating/Editing A Custom Service
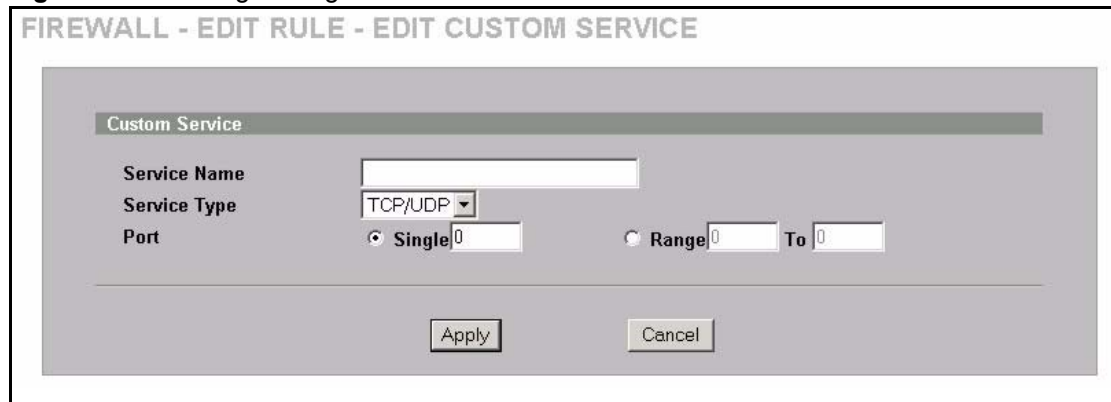
The following table describes the labels in this screen.

Table 62   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.

10.7 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 81 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 82 Rule Edit Example

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 83 Edit Custom Service Example

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 84 My Service Rule Configuration

Figure 85 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.

10.8 Predefined Services

The **Available Services** list box in the **Edit Rule** screen (see Figure 79) 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 63 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 63 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.
IP(AX.25:0)	AX.25 (Amateur X.25, an "Amateur" version of X.25) is the communications protocol used for packet radio.
IP(IPv6:0)	IPv6 (Internet Protocol version 6) is a protocol designed by the IETF to replace and solve many problems of the version 4 (IPv4).
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 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.

Table 63   Predefined Services (continued)

SERVICE	DESCRIPTION
RTELNET(TCP:107)	Remote Telnet.
RTSP(TCP/UDP:554)	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP(TCP:115)	Simple File Transfer Protocol.
SMTP(TCP:25)	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP(TCP/UDP:161)	Simple Network Management Program.
SNMP-TRAPS(TCP/UDP:162)	Traps for use with the SNMP (RFC:1215).
SQL-NET(TCP:1521)	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
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.

10.9 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 the 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 86 Anti-Probing

The following table describes the labels in this screen.

Table 64 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 **DMZ** to reply to incoming DMZ Ping requests. Otherwise select **LAN & WAN & DMZ** to reply to both incoming LAN and WAN and DMZ Ping requests.
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.

10.10 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.

10.10.1 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.

10.10.2 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 70). 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.

10.10.2.1 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 87 Firewall Threshold
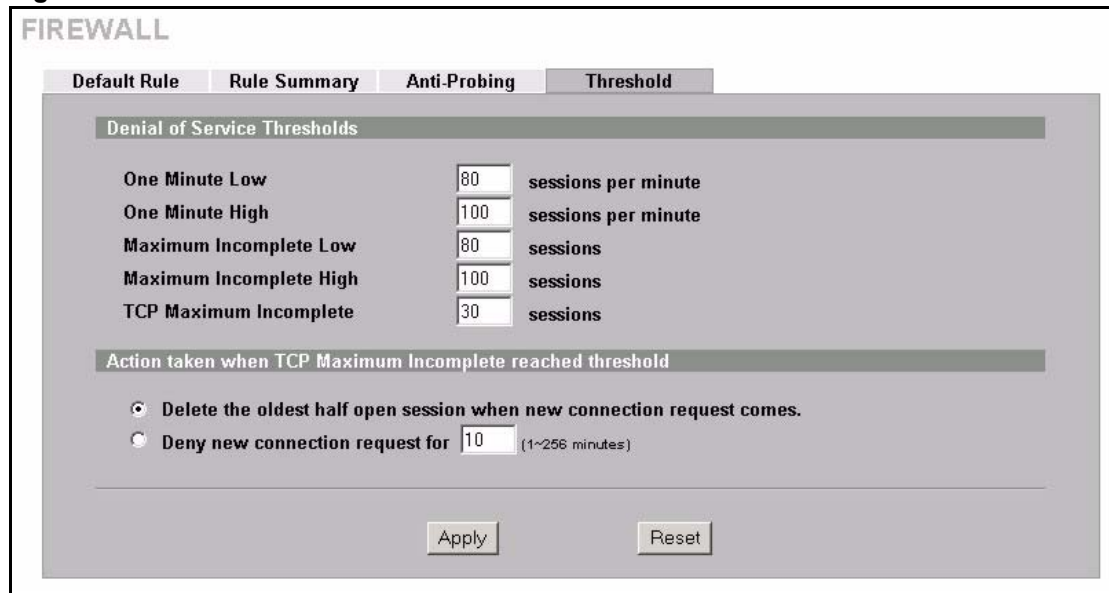
The following table describes the labels in this screen.

Table 65 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 65 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 11
Content Filtering Screens

This chapter provides an overview of content filtering.

11.1 Content Filtering Overview

Content filtering allows you to block certain web features, such as Cookies, and/or restrict specific websites. With content filtering, you can do the following:

11.1.1 Restrict Web Features

The ZyWALL can block web features such as ActiveX controls, Java applets, cookies and disable web proxies.

11.1.2 Create a Filter List

You can select categories, such as pornography or racial intolerance, to block from a pre-defined list.

11.1.3 Customize Web Site Access

You can specify URLs to which the ZyWALL blocks access. You can alternatively block access to all URLs except ones that you specify. You can also have the ZyWALL block access to URLs that contain key words that you specify.

11.2 General Content Filter Configuration

Click **CONTENT FILTER** and the screen will display as shown. Use this screen to enable content filtering, configure a schedule, and create a denial message. You can also choose specific computers to be included in or excluded from the content filtering configuration.

Figure 88   Content Filter : General

The following table describes the labels in this screen.

Table 66   Content Filter : General

LABEL	DESCRIPTION
General Setup	
Enable Content Filter	Select this check box to enable the content filter.
Restrict Web Features	Select the check box(es) to restrict a feature. When you download a page containing a restricted feature, that part of the web page will appear blank or grayed out.
Block ActiveX	ActiveX is a tool for building dynamic and active web pages and distributed object applications. When you visit an ActiveX web site, ActiveX controls are downloaded to your browser, where they remain in case you visit the site again.
Java	Java is a programming language and development environment for building downloadable Web components or Internet and intranet business applications of all kinds.

Table 66 Content Filter : General

LABEL	DESCRIPTION
Cookies	Cookies are files stored on a computer's hard drive. Some web servers use them to track usage and provide service based on ID.
Web Proxy	A server that acts as an intermediary between a user and the Internet to provide security, administrative control, and caching service. When a proxy server is located on the WAN it is possible for LAN users to circumvent content filtering by pointing to this proxy server.
Schedule to Block	Content filtering scheduling applies to the Filter List, Customized sites and Keywords. Restricted web server data, such as ActiveX, Java, Cookies and Web Proxy are not affected.
Always Block	Click this option button to have content filtering always active with Time of Day limitations not enforced. This is enabled by default.
Block From/To	Click this option button to have content filtering only active during the time interval specified. In the **Block From** and **To** fields, enter the time period, in 24-hour format, during which content filtering will be enforced.
Message to display when a site is blocked	
Denied Access Message	Enter a message to be displayed when a user tries to access a restricted web site. The default message is Please contact your network administrator!!
Redirect URL	Enter the URL of a web page to which to send the user when the ZyWALL's content filtering blocks access to a web site. Type up to 128 characters. The web page that you specify displays in the lower part of the screen. The denied access message displays in the top of the screen. If you do not specify a redirect URL, only the denied access message displays and the lower part of the screen is blank.
Exempt Computers	
Enforce content filter policies for all computers	Select this checkbox to have all users on your LAN follow content filter policies (default).
Include specified address ranges in the content filter enforcement	Select this checkbox to have a specific range of users on your LAN follow content filter policies.
Exclude specified address ranges from the content filter enforcement	Select this checkbox to exempt a specific range of users on your LAN from content filter policies.
Add Address Ranges	
From	Type the beginning IP address (in dotted decimal notation) of the specific range of users on your LAN.
To	Type the ending IP address (in dotted decimal notation) of the specific range of users on your LAN, then click **Add Range**.
Address List	This text field shows the address ranges that are blocked.
Add Range	Click **Add Range** after you have filled in the **From** and **To** fields above.
Delete Range	Click **Delete Range** after you select the range of addresses you wish to delete.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

11.3 Content Filtering with an External Database

When you register for and enable external database content filtering, your ZyWALL accesses an external database that has millions of web sites categorized based on content. You can have the ZyWALL block, block and/or log access to web sites based on these categories. The content filtering lookup process is described below.

Figure 89   Content Filtering Lookup Procedure
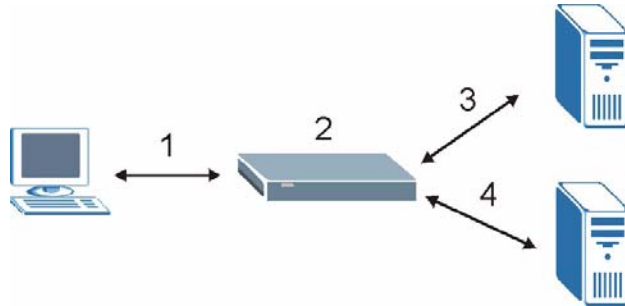
1 A computer behind the ZyWALL tries to access a web site.

2 The ZyWALL looks up the web site in its cache. If an attempt to access the web site was made in the past, a record of that web site's category will be in the ZyWALL's cache. The ZyWALL block, block and log or just log the request based on your configuration.

The ZyWALL drops a web site address record from the content filter cache after the content filter cache timeout period (default 72 hours) expires. All of the web site address records are also cleared from the local cache when the ZyWALL restarts. You can use `ip urlfilter webControl cache timeout` on the command line to configure how long a web site address remains in the cache.

3 If the ZyWALL has no record of the web site, it will query the external content filtering database and simultaneously send the request to the web server.

The external content filtering database may change a web site's category or categorize a previously uncategorized web site.

4 The external content filtering server sends the category information back to the ZyWALL, which then blocks and/or logs access to the web site. The web site's address and category are then stored in the ZyWALL's content filtering cache.

11.4 Categories and Registering

To register for and configure category-based content filtering, click **CONTENT FILTER**, and then the **Categories** tab to display the screen shown next. Use this screen to enable external database content filtering and select which web site categories to block and/or log. You must register for external content filtering before you can use it (see Chapter 12 Content Filtering Registration and Reports for detailed information).

Figure 90 Content Filter : Categories
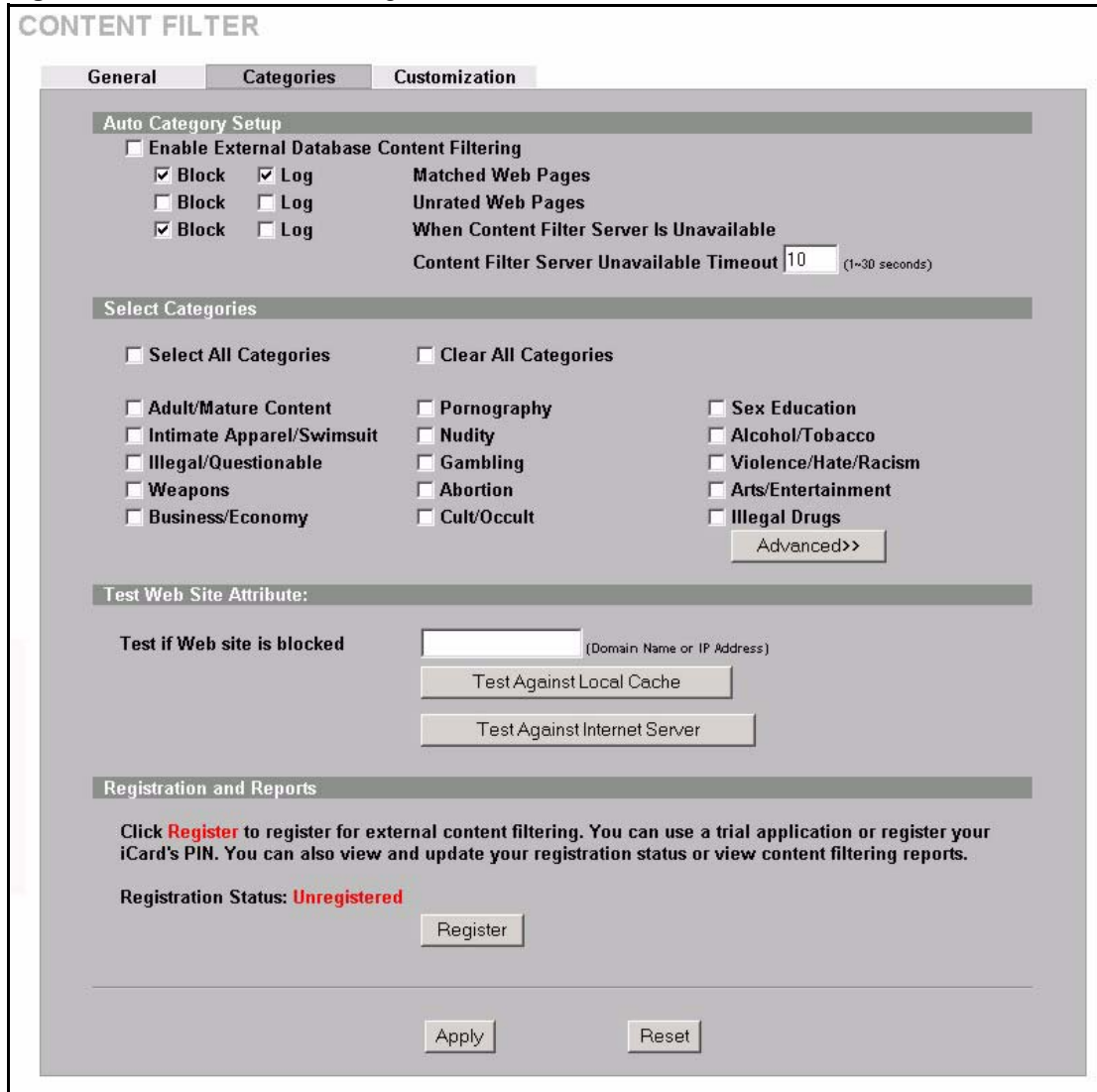
The following table describes the labels in this screen.

Table 67 Content Filter : Categories

LABEL	DESCRIPTION
Auto Category Setup	
Enable External Database Content Filtering	Enable external database content filtering to have the ZyWALL check an external database to find to which category a requested web page belongs. The ZyWALL then blocks or forwards access to the web page depending on the configuration of the rest of this page.
Matched Web Pages	Select **Block** to prevent users from accessing web pages that match the categories that you select below.
	When external database content filtering blocks access to a web page, it displays the denied access message that you configured in the **CONTENT FILTER General** screen along with the category of the blocked web page.
	Select **Log** to record attempts to access prohibited web pages.

Table 67 Content Filter : Categories (continued)

LABEL	DESCRIPTION
Unrated Web Pages	Select **Block** to prevent users from accessing web pages that the external database content filtering has not categorized.
	When the external database content filtering blocks access to a web page, it displays the denied access message that you configured in the **CONTENT FILTER General** screen along with the category of the blocked web page.
	Select **Log** to record attempts to access web pages that are not categorized.
When Content Filter Server Is Unavailable	Select **Block** to block access to any requested web page if the external content filtering database is unavailable. The following are possible causes:
	There is no response from the external content filtering server within the time period specified in the **Content Filter Server Unavailable Timeout** field.
	The ZyWALL is not able to resolve the domain name of the external content filtering database.
	There is an error response from the external content filtering database. This can be caused by an expired content filtering registration (External content filtering's license key is invalid").
	Select **Log** to record attempts to access web pages that occur when the external content filtering database is unavailable.
Content Filter Server Unavailable Timeout	Specify a number of seconds (1 to 30) for the ZyWALL to wait for a response from the external content filtering server. If there is still no response by the time this period expires, the ZyWALL blocks or allows access to the requested web page based on the setting in the **Block When Content Filter Server Is Unavailable** field.
Select Categories	
Select All Categories	Select this check box to restrict access to all site categories listed below.
Clear All Categories	Select this check box to clear the selected categories below.
Adult/Mature Content	Selecting this category excludes pages that contain material of adult nature that does not necessarily contain excessive violence, sexual content, or nudity. These pages include very profane or vulgar content and pages that are not appropriate for children.
Pornography	Selecting this category excludes pages that contain sexually explicit material for the purpose of arousing a sexual or prurient interest.
Sex Education	Selecting this category excludes pages that provide graphic information (sometimes graphic) on reproduction, sexual development, safe sex practices, sexuality, birth control, and sexual development. It also includes pages that offer tips for better sex as well as products used for sexual enhancement.
Intimate Apparel/Swimsuit	Selecting this category excludes pages that contain images or offer the sale of swimsuits or intimate apparel or other types of suggestive clothing. It does not include pages selling undergarments as a subsection of other products offered.
Nudity	Selecting this category excludes pages containing nude or seminude depictions of the human body. These depictions are not necessarily sexual in intent or effect, but may include pages containing nude paintings or photo galleries of artistic nature. This category also includes nudist or naturist pages that contain pictures of nude individuals.

Table 67 Content Filter : Categories (continued)

LABEL	DESCRIPTION
Alcohol/Tobacco	Selecting this category excludes pages that promote or offer the sale alcohol/tobacco products, or provide the means to create them. It also includes pages that glorify, tout, or otherwise encourage the consumption of alcohol/tobacco. It does not include pages that sell alcohol or tobacco as a subset of other products.
Illegal/Questionable	Selecting this category excludes pages that advocate or give advice on performing illegal acts such as service theft, evading law enforcement, fraud, burglary techniques and plagiarism. It also includes pages that provide or sell questionable educational materials, such as term papers. **Note:** This category includes sites identified as being malicious in any way (such as having viruses, spyware and etc.).
Gambling	Selecting this category excludes pages where a user can place a bet or participate in a betting pool (including lotteries) online. It also includes pages that provide information, assistance, recommendations, or training on placing bets or participating in games of chance. It does not include pages that sell gambling related products or machines. It also does not include pages for offline casinos and hotels (as long as those pages do not meet one of the above requirements).
Violence/Hate/Racism	Selecting this category excludes pages that depict extreme physical harm to people or property, or that advocate or provide instructions on how to cause such harm. It also includes pages that advocate, depict hostility or aggression toward, or denigrate an individual or group on the basis of race, religion, gender, nationality, ethnic origin, or other characteristics.
Weapons	Selecting this category excludes pages that sell, review, or describe weapons such as guns, knives or martial arts devices, or provide information on their use, accessories, or other modifications. It does not include pages that promote collecting weapons, or groups that either support or oppose weapons use.
Abortion	Selecting this category excludes pages that provide information or arguments in favor of or against abortion, describe abortion procedures, offer help in obtaining or avoiding abortion, or provide information on the effects, or lack thereof, of abortion.
Arts/Entertainment	Selecting this category excludes pages that promote and provide information about motion pictures, videos, television, music and programming guides, books, comics, movie theatres, galleries, artists or reviews on entertainment.
Business/Economy	Selecting this category excludes pages devoted to business firms, business information, economics, marketing, business management and entrepreneurship. This does not include pages that perform services that are defined in another category (such as Information Technology companies, or companies that sell travel services).
Cult/Occult	Selecting this category excludes pages that promote or offer methods, means of instruction, or other resources to affect or influence real events through the use of spells, curses, magic powers and satanic or supernatural beings.
Illegal Drugs	Selecting this category excludes pages that promote, offer, sell, supply, encourage or otherwise advocate the illegal use, cultivation, manufacture, or distribution of drugs, pharmaceuticals, intoxicating plants or chemicals and their related paraphernalia.

Table 67 Content Filter : Categories (continued)

LABEL	DESCRIPTION
Education	Selecting this category excludes pages that offer educational information, distance learning and trade school information or programs. It also includes pages that are sponsored by schools, educational facilities, faculty, or alumni groups.
Cultural Institutions	Selecting this category excludes pages sponsored by cultural institutions, or those that provide information about museums, galleries, and theaters (not movie theaters). It includes groups such as 4H and the Boy Scouts of America.
Financial Services	Selecting this category excludes pages that provide or advertise banking services (online or offline) or other types of financial information, such as loans. It does not include pages that offer market information, brokerage or trading services.
Brokerage/Trading	Selecting this category excludes pages that provide or advertise trading of securities and management of investment assets (online or offline). It also includes insurance pages, as well as pages that offer financial investment strategies, quotes, and news.
Games	Selecting this category excludes pages that provide information and support game playing or downloading, video games, computer games, electronic games, tips, and advice on games or how to obtain cheat codes. It also includes pages dedicated to selling board games as well as journals and magazines dedicated to game playing. It includes pages that support or host online sweepstakes and giveaways.
Government/Legal	Selecting this category excludes pages sponsored by or which provide information on government, government agencies and government services such as taxation and emergency services. It also includes pages that discuss or explain laws of various governmental entities.
Military	Selecting this category excludes pages that promote or provide information on military branches or armed services.
Political/Activist Groups	Selecting this category excludes pages sponsored by or which provide information on political parties, special interest groups, or any organization that promotes change or reform in public policy, public opinion, social practice, or economic activities.
Health	Selecting this category excludes pages that provide advice and information on general health such as fitness and well-being, personal health or medical services, drugs, alternative and complimentary therapies, medical information about ailments, dentistry, optometry, general psychiatry, self-help, and support organizations dedicated to a disease or condition.
Computers/Internet	Selecting this category excludes pages that sponsor or provide information on computers, technology, the Internet and technology-related organizations and companies.
Hacking/Proxy Avoidance	Pages providing information on illegal or questionable access to or the use of communications equipment/software, or provide information on how to bypass proxy server features or gain access to URLs in any way that bypasses the proxy server.
Search Engines/Portals	Selecting this category excludes pages that support searching the Internet, indices, and directories.
Web Communications	Selecting this category excludes pages that allow or offer Web-based communication via e-mail, chat, instant messaging, message boards, etc.
Job Search/Careers	Selecting this category excludes pages that provide assistance in finding employment, and tools for locating prospective employers.

Table 67 Content Filter : Categories (continued)

LABEL	DESCRIPTION
News/Media	Selecting this category excludes pages that primarily report information or comments on current events or contemporary issues of the day. It also includes radio stations and magazines. It does not include pages that can be rated in other categories.
Personals/Dating	Selecting this category excludes pages that promote interpersonal relationships.
Reference	Selecting this category excludes pages containing personal, professional, or educational reference, including online dictionaries, maps, census, almanacs, library catalogues, genealogy-related pages and scientific information.
Chat/Instant Messaging	Selecting this category excludes pages that provide chat or instant messaging capabilities or client downloads.
Email	Selecting this category excludes pages offering web-based email services, such as online email reading, e-cards, and mailing list services.
Newsgroups	Selecting this category excludes pages that offer access to Usenet news groups or other messaging or bulletin board systems.
Religion	Selecting this category excludes pages that promote and provide information on conventional or unconventional religious or quasi-religious subjects, as well as churches, synagogues, or other houses of worship. It does not include pages containing alternative religions such as Wicca or witchcraft (Cult/Occult) or atheist beliefs (Political/Activist Groups).
Shopping	Selecting this category excludes pages that provide or advertise the means to obtain goods or services. It does not include pages that can be classified in other categories (such as vehicles or weapons).
Auctions	Selecting this category excludes pages that support the offering and purchasing of goods between individuals. This does not include classified advertisements.
Real Estate	Selecting this category excludes pages that provide information on renting, buying, or selling real estate or properties.
Society/Lifestyle	Selecting this category excludes pages providing information on matters of daily life. This does not include pages relating to entertainment, sports, jobs, sex or pages promoting alternative lifestyles such as homosexuality. Personal homepages fall within this category if they cannot be classified in another category.
Gay/Lesbian	Selecting this category excludes pages that provide information, promote, or cater to gay and lesbian lifestyles. This does not include pages that are sexually oriented.
Restaurants/Dining/Food	Selecting this category excludes pages that list, review, discuss, advertise and promote food, catering, dining services, cooking and recipes.
Sports/Recreation/Hobbies	Selecting this category excludes pages that promote or provide information about spectator sports, recreational activities, or hobbies. This includes pages that discuss or promote camping, gardening, and collecting.
Travel	Selecting this category excludes pages that promote or provide opportunity for travel planning, including finding and making travel reservations, vehicle rentals, descriptions of travel destinations, or promotions for hotels or casinos.
Vehicles	Selecting this category excludes pages that provide information on or promote vehicles, boats, or aircraft, including pages that support online purchase of vehicles or parts.

Table 67 Content Filter : Categories (continued)

LABEL	DESCRIPTION
Humor/Jokes	Selecting this category excludes pages that primarily focus on comedy, jokes, fun, etc. This may include pages containing jokes of adult or mature nature. Pages containing humorous Adult/Mature content also have an Adult/Mature category rating.
Streaming Media/MP3	Selecting this category excludes pages that sell, deliver, or stream music or video content in any format, including pages that provide downloads for such viewers.
Software Downloads	Selecting this category excludes pages that are dedicated to the electronic download of software packages, whether for payment or at no charge.
Pay to Surf	Selecting this category excludes pages that pay users in the form of cash or prizes, for clicking on or reading specific links, email, or web pages.
For Kids	Selecting this category excludes pages designed specifically for children.
Web Advertisements	Selecting this category excludes pages that provide online advertisements or banners. This does not include advertising servers that serve adult-oriented advertisements.
Web Hosting	Selecting this category excludes pages of organizations that provide top-level domain pages, as well as web communities or hosting services.
Advanced/Basic	Click **Advanced** to see an expanded list of categories, or click **Basic** to see a smaller list.
Test Web Site Attribute	
Test if Web site is blocked	You can check whether or not the content filter currently blocks any given web page. Enter a web site URL in the text box.
Test Against Local Cache	Click this button to test whether or not the web site above is saved in the ZyWALL's database of restricted web pages.
Test Against Internet Server	Click this button to test whether or not the web site above is saved in the external content filter server's database of restricted web pages.
Registration and Reports	
Registration Status	This read-only field displays **Registered** if you have successfully registered the ZyWALL for category-based content filtering (using an external database). This field displays **Unregistered** if you have not successfully registered the ZyWALL or your registration has expired. **Note:** This field only displays whether or not you have successfully registered, not whether or not content filtering is active. See the Viewing Content Filtering Reports section for how to check the content filtering activation.

Table 67 Content Filter : Categories (continued)

LABEL	DESCRIPTION
Register	Click **Register** to go to a web site where you can register for category-based content filtering (using an external database). You can use a trial application or register your iCard's PIN. Refer to the web site's on-line help for details. **Note:** The web site displays a registration successful web page. It may take up to another ten minutes for content filtering to be activated. See the Viewing Content Filtering Reports section for how to check the content filtering activation. You can manage your registration status or view content filtering reports after you register this device. **Note:** You cannot access the web site if you have enabled content filtering in the **Content Filtering General** screen and blocked access to web pages that use Java.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

11.5 Customization

You can create a list of good (allowed) web site addresses and a list of bad (blocked) web site addresses on the ZyWALL. You can also block web sites based on whether the web site's address contains a keyword. To add or remove specific sites or keywords from the filter list on your ZyWALL, click **CONTENT FILTER**, then the **Customization** tab. The screen appears as shown.

Figure 91 Content Filter : Customization

The following table describes the labels in this screen.

Table 68 Content Filter : Customization

LABEL	DESCRIPTION
Web Site List Customization	
Enable Web site customization	Select this check box to allow trusted web sites and block forbidden web sites. Content filter list customization may be enabled and disabled without re-entering these site names.
Disable all Web traffic except for trusted Web sites	When this box is selected, the ZyWALL only allows Web access to sites on the **Trusted Web Site** list. If they are chosen carefully, this is the most effective way to block objectionable material.

Table 68   Content Filter : Customization (continued)

LABEL	DESCRIPTION
Don't block Java/ActiveX/ Cookies/Web proxy to trusted Web sites	When this box is selected, the ZyWALL will permit Java, ActiveX and Cookies from sites on the **Trusted Web Site** list to the LAN. In certain cases, it may be desirable to allow Java, ActiveX or Cookies from sites that are known and trusted.
Trusted Web Sites	These are sites that you want to allow access to, regardless of their content rating, can be allowed by adding them to this list. You can enter up to 32 entries.
Add Trusted Web Site	Enter host names such as www.good-site.com into this text field. Do not enter the complete URL of the site – that is, do not include "http://". All subdomains are allowed. For example, entering "zyxel.com" also allows "www.zyxel.com", "partner.zyxel.com", "press.zyxel.com", etc.
Trusted Web Sites	This list displays the trusted web sites already added.
Add	Click this button when you have finished adding the host name in the text field above.
Delete	Select a web site name from the **Trusted Web Site List**, and then click this button to delete it from that list.
Forbidden Web Site List	Sites that you want to block access to, regardless of their content rating, can be allowed by adding them to this list. You can enter up to 32 entries.
Add Forbidden Web Site	Enter host names such as www.bad-site.com into this text field. Do not enter the complete URL of the site – that is, do not include "http://". All subdomains are allowed. For example, entering "bad-site.com" also blocks "www.bad-site.com", "partner.bad-site.com", "press.bad-site.com", etc.
Forbidden Web Sites	This list displays the forbidden web sites already added.
Add	Click this button when you have finished adding the host name in the text field above.
Delete	Select a web site name from the **Forbidden Web Site List**, and then click this button to delete it from that list.
Keyword Blocking	**Keyword Blocking** allows you to block websites with URLs that contain certain keywords in the domain name or IP address. **Note:** See the Customizing Keyword Blocking URL Checking section for how to set how much of the URL the ZyWALL checks.
Block Web sites which contain these keywords.	Select this checkbox to enable keyword blocking.
Add Keyword	Enter a keyword (up to 31 printable ASCII characters) to block. You can also enter a numerical IP address.
Keyword List	This list displays the keywords already added.
Add	Click this button when you have finished adding the key words field above.
Delete	Select a keyword from the **Keyword List**, and then click this button to delete it from that list.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

11.6 Customizing Keyword Blocking URL Checking

You can use commands to set how much of a website's URL the content filter is to check for keyword blocking. See the appendices for information on how to access and use the command interpreter.

11.6.1 Domain Name or IP Address URL Checking

By default, the ZyWALL checks the URL's domain name or IP address when performing keyword blocking.

This means that the ZyWALL checks the characters that come before the first slash in the URL.

For example, with the URL www.zyxel.com.tw/news/pressroom.php, content filtering only searches for keywords within www.zyxel.com.tw.

11.6.2 Full Path URL Checking

Full path URL checking has the ZyWALL check the characters that come before the last slash in the URL.

For example, with the URL www.zyxel.com.tw/news/pressroom.php, full path URL checking searches for keywords within www.zyxel.com.tw/news/.

Use the `ip urlfilter customize actionFlags 6 [disable | enable]` command to extend (or not extend) the keyword blocking search to include the URL's full path.

11.6.3 File Name URL Checking

Filename URL checking has the ZyWALL check all of the characters in the URL.

For example, filename URL checking searches for keywords within the URL www.zyxel.com.tw/news/pressroom.php.

Use the `ip urlfilter customize actionFlags 8 [disable | enable]` command to extend (or not extend) the keyword blocking search to include the URL's complete filename.

C H A P T E R 12
Content Filtering Registration and Reports

This chapter describes how to register for content filtering and view content filtering reports.

Before you activate content filtering, you must create an account at myZyXEL.com and register your device.

> **Note:** To activate content filtering, you need to access myZyXEL.com via the device on which you wish to register for content filtering.

You can only use the content filtering with the device upon which you register it. You cannot change devices. Your device's MAC address and serial number (see the sticker on the rear side of your device) identify it. You need to register separately for each device on which you wish to enable content filtering.

When registering, you need to enter a PIN (see your iCard). Be sure to buy the correct iCard for your device. If you wish to try content filtering before buying an iCard, then fill in the trial application for a free 30-day trial.

Content filtering reports are generated statistics and charts of access attempts to web sites belonging to the categories you selected in your device content filter screen.

You can also view content filtering reports during the free trial.

12.1 Introduction to myZyXEL.com

myZyXEL.com is ZyXEL's online services center where you can register your ZyXEL device. You can also generate an activation key and service set key that may be needed to use device-specific feature(s).

12.1.1 A Note on myZyXEL.com Numbers

You need the following (unique) numbers to register and activate device-specific feature(s).

Table 69   myZyXEL.com Numbers

TYPES	DESCRIPTION
Serial Number	You need the serial number to register your ZyXEL device. Locate the serial number on your ZyXEL device.
Authentication Code	This is the LAN MAC address of your ZyXEL device. You need this number to register your ZyXEL device at myZyXEL.com. Locate the MAC address on your ZyXEL device.

12.2 myZyXEL.com Account Registration

1 Go to myZyXEL.com using your web browser.

2 Create a new account (if you don't have one already) with a user name and password by clicking the hyperlink as shown in the next screen.

Figure 92   myZyXEL.com Login Screen

3 Fill in the required fields and click **Submit**.

Figure 93 myZyXEL.com Account Registration

4 A screen appears indicating you have created an account at myZyXEL.com.

Figure 94 Account Registration Successful

5 You will receive a confirmation e-mail. Click the URL in the e-mail to activate your account.

Figure 95 Account Confirmation E-Mail
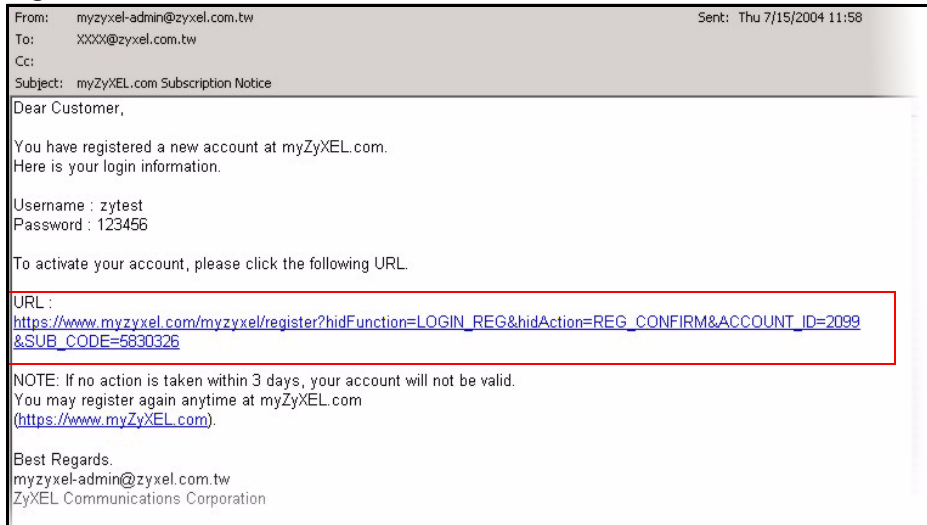
6 Click **Continue** to go to the myZyXEL.com login screen.

Figure 96 myZyXEL.com Account Activation

12.3 Registering Your ZyXEL Device

1 After you have created a myZyXEL.com account, log in and register your ZyXEL device by clicking the hyperlink as shown in the next screen.

Figure 97 Logged Into myZyXEL.com
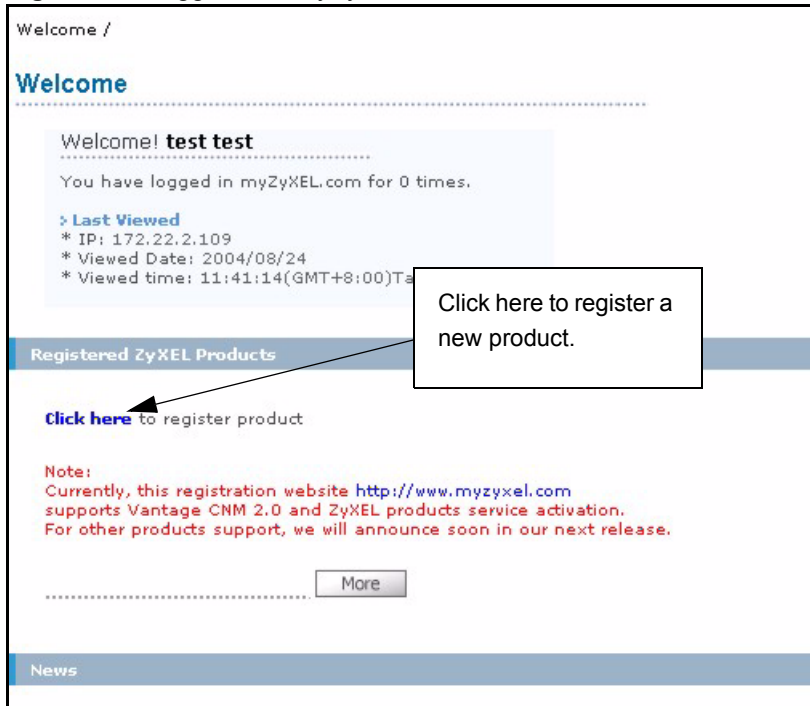
2 Click **Add** in the next screen.

Figure 98 Product Registration
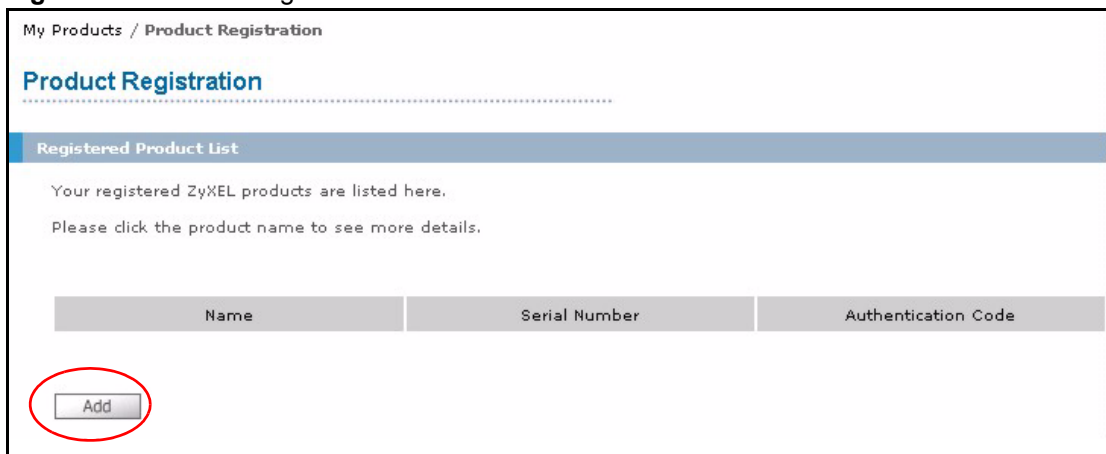
3 The **Add New Product** screen displays. Enter the product serial number in the **Serial Number** field.

4 Your device category and model number may automicatically display in the **Category** and **Model** fields respectively. Otherwise, select the correct ones from the drop-down list boxes.

5 Enter the device MAC address in the **Authentication Code** field.

6 Enter a descriptive name in the **Friendly Name** field for identifying your device.

7 Click **Register**.

Figure 99   Add New Product

8 Specify the purchase information and click **Continue**.

Figure 100   Product Survey

9 Click **Continue** again.

10 After you have registered your ZyXEL device, you can view its registration details in the screen shown next.

Figure 101 Service Management

12.4 Content Filtering Registration

1 In your ZyXEL device's web configurator, click **CONTENT FILTER**, **Categories** and then the **Register** button. The following screen opens.

2 Enter the user name and password from your myZyXEL.com account (see Figure 92).

3 After you register your ZyXEL device, click **My Product** in the navigation panel.

4 Click the product name link for your device to view its registration details in the **Service Management** screen.

Figure 102 myZyXEL.com: My Product

5 Click **Activate** for the content filtering service to display the next screen.

Figure 103   myZyXEL.com: Service Management.

6 Enter the PIN code exactly as shown on your iCard (you do not enter a PIN if you are registering for the trial period) in the **License Key (PIN code)** field.
From the **Activation Date** drop-down list boxes, select the date when you want your content filtering to start and click **Submit** under **Registration Information**.

7 Otherwise, click **Submit** under **Content Filtering Trial** to register for a 30 day trial period. With the trial registration, content filtering functions for 30 days beginning from the date you apply for the trial.
After the trial, you cannot apply for another trial. If you've already registered an iCard's PIN number, then you also cannot apply for a trial.
If you have applied for a trial, you can still register the PIN code from an iCard by clicking **Upgrade** in the **Service Activation** field of the **Service Management** screen.

Figure 104   Service Registration

8 A screen displays showing you the service is registered. Click **Continue** to proceed to the **Service Management** screen.

Figure 105 Service Registration: Successful

Figure 106 Service Management: Service Registered

9 You can go on to update your product registration information, view content filtering reports or click **LOGOUT** at any time to exit myZyXEL.com.

12.5 Checking Content Filtering Activation

After you register for content filtering, the web site displays a registration successful web page. This does not mean the content filtering is active yet. You need to wait up to ten minutes for content filtering to be activated.

Since there will be no content filtering activation notice, you can do the following to see if content filtering is active.

1 Go to your device's web configurator's **CONTENT FILTER Categories** screen.

2 Select at least one category and click **Apply**.

3 Enter a valid URL or IP address of a web site in the **Test if Web site is blocked** field and click the **Test Against Internet Server** button.
When content filtering is active, you should see an access blocked or access forwarded message. An error message displays if content filtering is not active.

12.6 Updating Product Registration Information

1 Click **CONTENT FILTER**, **Categories** and then **Register**. The myZyXEL.com login screen opens (see Figure 2).

2 After entering the user name and password from your myZyXEL.com account, click **My Product** (see Figure 102) and the link for your ZyWALL to open the **Service Management** screen where you can modify your registration information (see Figure 105).

3 From this screen, you may click **Rename** under **Manage Product** to modify your product's name, click **Transfer** under **Manage Product** to move the registered product to another pre-registered user account at myZyXEL.com, click **Delete** under **Manage Product** to remove the product registration or click **Reinstall** under **Manage Product** to install the product again with another authentication code (for up to three times). If you have activated a service on a registered product, you cannot delete that product. You cannot modify the PIN code, activation date or expiry date. Change the information that you need to modify and click **Submit**.

12.7 Viewing Content Filtering Reports

Content filtering reports are generated statistics and charts of access attempts to web sites belonging to the categories you selected in your device content filter screen.

You need to register your iCard before you can view content filtering reports.

Alternatively, you can also view content filtering reports during the free trial (up to 30 days).

1 In the **Service Management** screen (see Figure 105) click **Content Filtering** in the **Service Name** field to open the following screen.

Figure 107 Cerberian Login Screen

2 Enter your ZyXEL device's MAC address (in lower case) in the **Name** field. Type the password that you configured during account registration at myZyXEL.com.

3 Click **Reports**.

Figure 108 Content Filtering Reports Main Screen

> **Note:** The ZyWALL does not support Single User Reports at the time of writing.

4 Select either **Allow** or **Block** reports. Select a time period in the **Select Date Range** field and click **Run Report**.

5 A chart and list of requested web site categories display in the lower half of the screen.

Figure 109 Global Report Screen Example
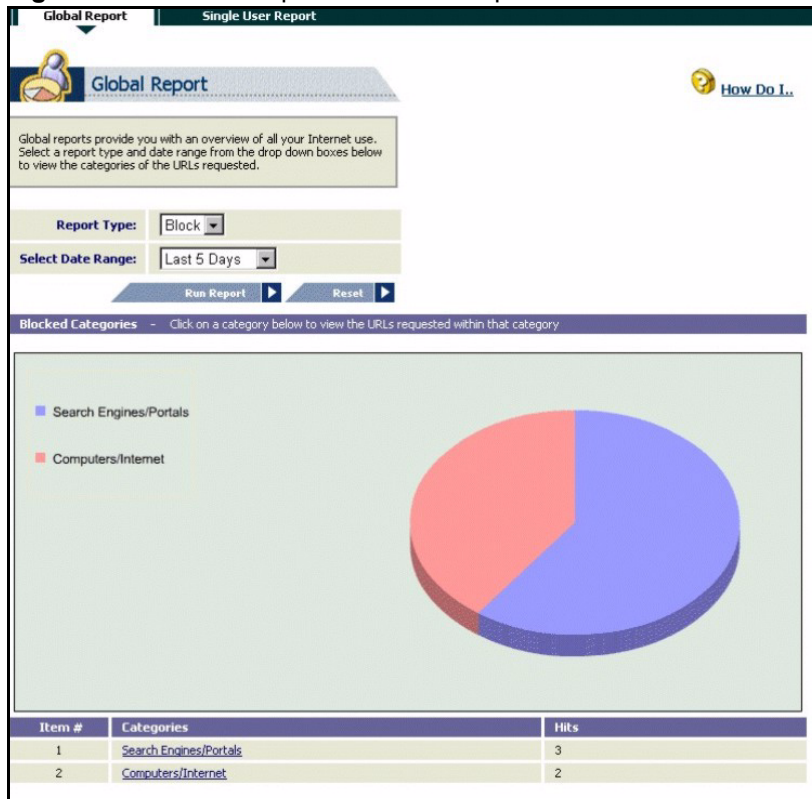
6 Click a category to see the URLs that were requested.

Figure 110 Requested URLs Example

12.8 Configuration File

If you restore the ZyWALL to the default rom file or upload a different rom file after you register, then you must go to the **Service Management** screen (see Figure 106) and click **Refresh** in the **Remark** field.

CHAPTER 13
Introduction to IPSec

This chapter introduces the basics of IPSec VPNs. This chapter is only applicable when the ZyWALL is in router mode.

13.1 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.

13.1.1 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.

13.1.2 Security Association

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

13.1.3 Other Terminology

13.1.3.1 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 111 Encryption and Decryption
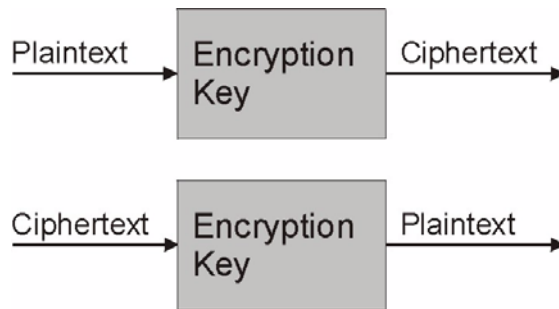
13.1.3.2 Data Confidentiality

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

13.1.3.3 Data Integrity

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

13.1.3.4 Data Origin Authentication

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

13.1.4 VPN Applications

The ZyWALL supports the following VPN applications.

13.1.4.1 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.

13.1.4.2 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.

13.1.4.3 Unsupported IP Applications

A VPN tunnel may be created to add support for unsupported emerging IP applications. See Chapter 1 Getting to Know Your ZyWALL for an example of a VPN application.

13.2 IPSec Architecture

The overall IPSec architecture is shown as follows.

Figure 112 IPSec Architecture
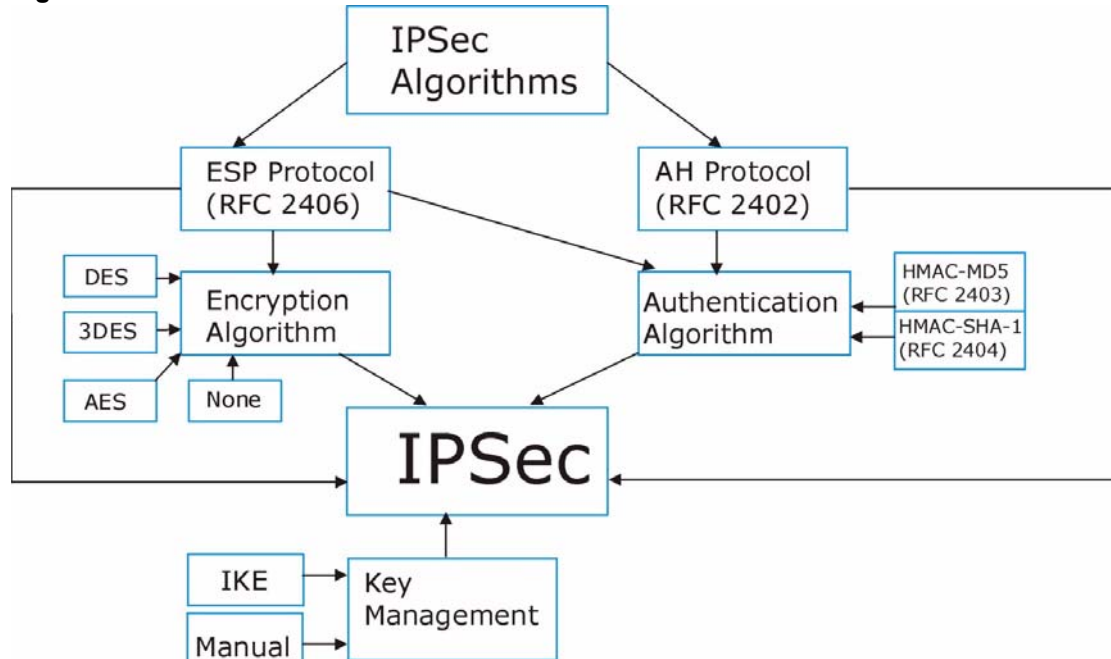
13.2.1 IPSec Algorithms

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. Please see the IPSec Algorithms section for more information.

13.2.2 Key Management

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

13.3 Encapsulation

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

Figure 113 Transport and Tunnel Mode IPSec Encapsulation

Original IP Packet	IP Header	TCP Header	Data		

Transport Mode Protected Packet	IPSec Header	IP Header	TCP Header	Data	

Tunnel Mode Protected Packet	IP Header	IPSec Header	IP Header	TCP Header	Data
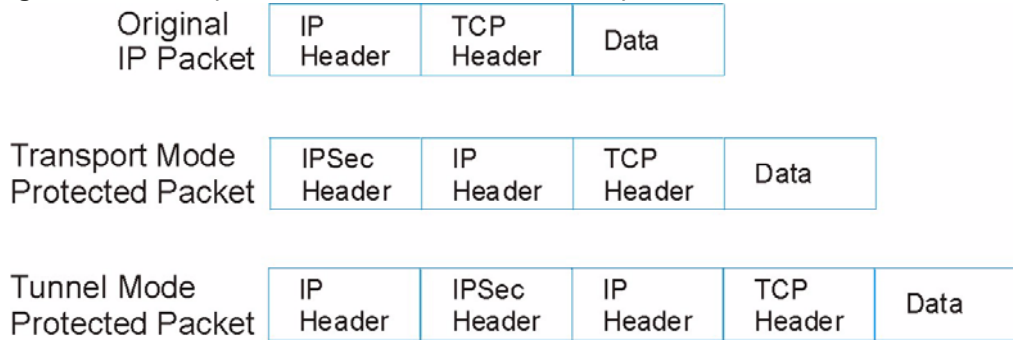
13.3.1 Transport Mode

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.

13.3.2 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.

13.4 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 the NAT Traversal section for details).

Table 70   VPN and NAT

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

Chapter 13 Introduction to IPSec

C HAPTER 14
VPN Screens

This chapter introduces the VPN Web Configurator. See Chapter 23 Logs Screens for information on viewing logs and see Appendix S Log Descriptions for IPSec log descriptions.

14.1 VPN/IPSec Overview

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

14.2 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.

14.2.1 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.

14.2.2 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 71 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.	

14.3 My IP Address

My IP Address identifies the WAN IP address of the ZyWALL. You can select **IP Address** and enter the ZyWALL's static WAN IP address (if it has one) or leave the field set to 0.0.0.0. Otherwise you can select **My Domain Name** and choose one of the dynamic domain names that you have configured (in the **DDNS** screen) to have the ZyWALL use that dynamic domain name's IP address. The ZyWALL has to rebuild the VPN tunnel if the **My IP Address** changes after setup.

14.4 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).

14.4.1 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 the Telecommuter VPN/IPSec Examples section 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.

14.5 Summary Screen

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

Figure 114   IPSec Summary Fields
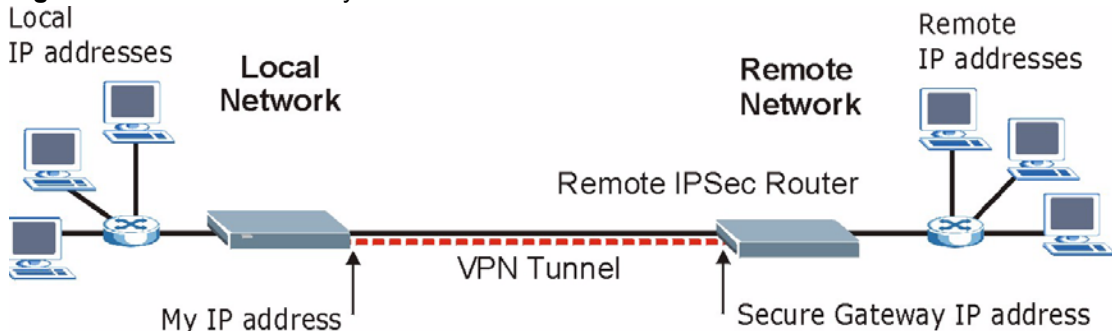
Local and remote IP addresses must be static.

Click **VPN** to open the **VPN Rules** screen. This is a read-only menu of your IPSec rules (tunnels). Edit an IPSec rule by clicking the edit icon to configure the associated submenus.

Figure 115 VPN Rules
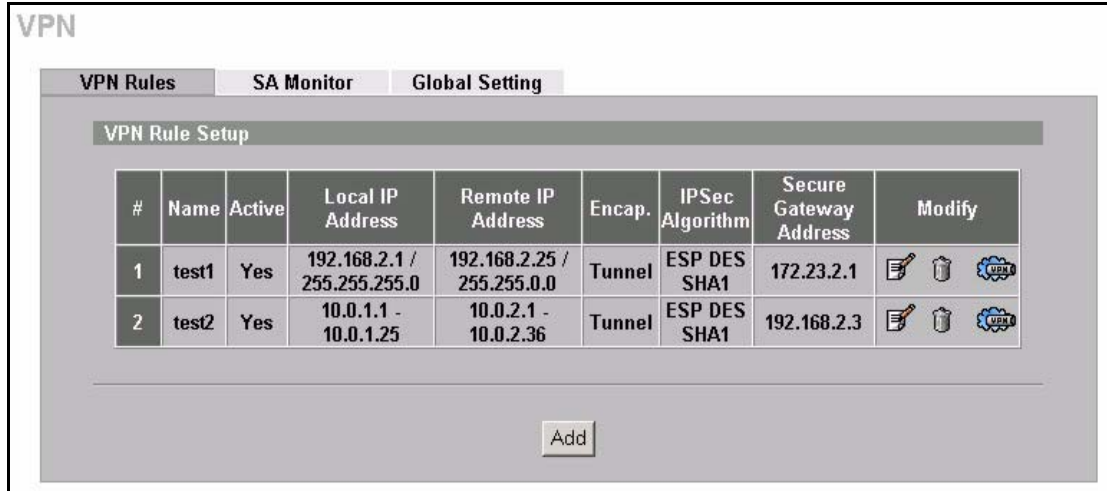
The following table describes the labels in this screen.

Table 72 VPN Rules

LABEL	DESCRIPTION
#	This is the VPN policy index number.
Name	This field displays the identification name for this VPN policy.
Active	This field displays whether the VPN policy is active or not. A **Yes** signifies that this VPN policy is active. **No** signifies that this VPN policy is not active.
Local IP Address	This is the IP address(es) of computer(s) on your local network behind your ZyWALL.
	The same (static) IP address is displayed twice when the **Local Address Type** field in the **Edit VPN Rule** (or **Manual Key**) screen is configured to **Single Address**.
	The beginning and ending (static) IP addresses, in a range of computers are displayed when the **Local Address Type** field in the **Edit VPN Rule** (or **Manual Key**) screen is configured to **Range Address**.
	A (static) IP address and a subnet mask are displayed when the **Local Address Type** field in the **Edit VPN Rule** (or **Manual Key**) screen is configured to **Subnet Address**.
Remote IP Address	This is the IP address(es) of computer(s) on the remote network behind the remote IPSec router.
	This field displays **N/A** when the **Secure Gateway Address** field displays **0.0.0.0**. In this case only the remote IPSec router can initiate the VPN.
	The same (static) IP address is displayed twice when the **Remote Address Type** field in the **Edit VPN Rule** (or **Manual Key**) screen is configured to **Single Address**.
	The beginning and ending (static) IP addresses, in a range of computers are displayed when the **Remote Address Type** field in the **Edit VPN Rule** (or **Manual Key**) screen is configured to **Range Address**.
	A (static) IP address and a subnet mask are displayed when the **Remote Address Type** field in the **Edit VPN Rule** (or **Manual Key**) screen is configured to **Subnet Address**.
Encap.	This field displays **Tunnel** or **Transport** mode (**Tunnel** is the default selection).

Table 72 VPN Rules

LABEL	DESCRIPTION
IPSec Algorithm	This field displays the security protocols used for an SA. Both **AH** and **ESP** increase ZyWALL processing requirements and communications latency (delay).
Secure Gateway Address	This is the static WAN IP address or URL of the remote IPSec router. This field displays **0.0.0.0** when you configure the **Secure Gateway Address** field in the **Edit VPN Rule** screen to **0.0.0.0.**
Modify	Click the edit icon to edit the VPN policy. Click the delete icon to remove the VPN policy. A window displays asking you to confirm that you want to delete the VPN rule. When a VPN policy is deleted, subsequent policies move up in the page list. Click the dial icon to dial up the connection manually. If a VPN tunnel has been built and dialed up, every time you click this icon, a warning message appears in the status bar on the bottom of the screen.
Add	Click **Add** to add a new VPN policy.

14.6 Keep Alive

When you initiate an IPSec tunnel with keep alive enabled, the ZyWALL automatically renegotiates the tunnel when the IPSec SA lifetime period expires (see the IKE Phases section 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 keep alive 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 keep alive 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.

14.7 NAT Traversal

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

Figure 116 NAT Router Between IPSec Routers
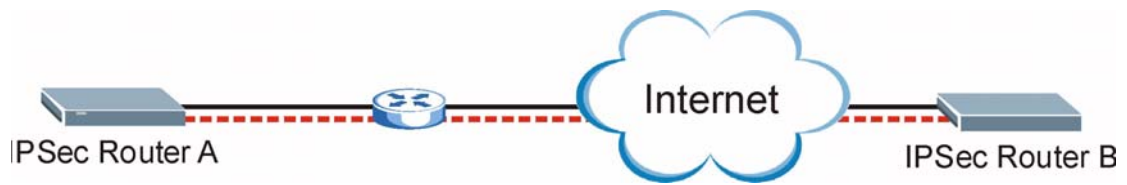
Normally you cannot set up a VPN connection with a NAT router between the two IPSec routers because the NAT router changes the header of the IPSec packet. In the previous figure, IPSec router A sends an IPSec packet in an attempt to initiate a VPN. The NAT router changes the IPSec packet's header so 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.

14.7.1 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 the figure) to receive an initiating IPSec packet from IPSec router B, set the NAT router to forward UDP port 500 to IPSec router A.

14.7.2 X-Auth (Extended Authentication)

Extended authentication provides added security by 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 ZyWALL. 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 (see the Authentication Server section).

A ZyWALL can be an extended authentication server for some VPN connections and an extended authentication client for other VPN connections.

14.7.3 Remote DNS Server

In cases where you want to use domain names to access Intranet servers on a remote network that has a DNS server, you must identify that DNS server. You cannot use DNS servers on the LAN or from the ISP since these DNS servers cannot resolve domain names to private IP addresses on the remote network

The following figure depicts an example where three VPN tunnels are created from ZyWALL A; one to branch office **2**, one to branch office **3** and another to headquarters. In order to access computers that use private domain names on the headquarters (**HQ**) network, the ZyWALL at branch office **1** uses the Intranet DNS server in headquarters. The DNS server feature for VPN does not work with Windows 2000 or Windows XP

Figure 117   VPN Host using Intranet DNS Server Example
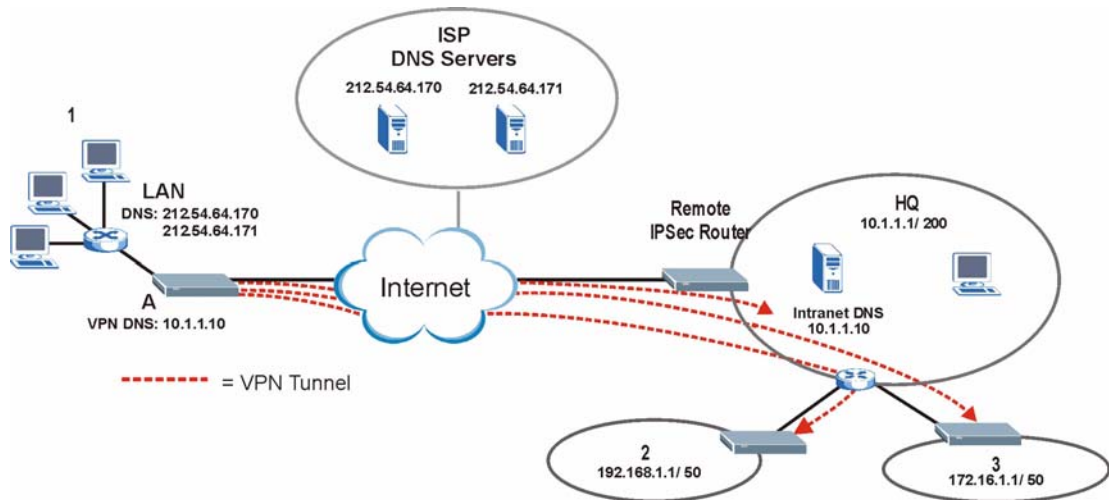
> **Note:** If you do not specify an Intranet DNS server on the remote network, then the VPN host must use IP addresses to access the computers on the remote network.

14.8 ID Type and Content

With aggressive negotiation mode (see the Negotiation Mode section), 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 the Telecommuters Using Unique VPN Rules Example section 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 the Negotiation Mode section), 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 the Editing VPN Policies section). 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 73 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 74 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** 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.
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 Addr** field below.	

14.8.1 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 75 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 76 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

14.9 Pre-Shared Key

A pre-shared key identifies a communicating party during a phase 1 IKE negotiation (see the IKE Phases section 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.

14.10 Editing VPN Policies

Click the edit icon on the **VPN Rules** screen to edit VPN policies.

Figure 118 Edit VPN Rule

The following table describes the labels in this screen.

Table 77 Edit VPN Rule

LABEL	DESCRIPTION
Property	
Active	Select this check box to activate this VPN tunnel. This option determines whether a VPN rule is applied before a packet leaves the firewall.
Keep Alive	Select this check box to turn on the keep alive feature for this SA.
	Turn on Keep Alive to have the ZyWALL automatically reinitiate the SA after the SA lifetime times out, even if there is no traffic. The remote IPSec router must also have keep alive enabled in order for this feature to work.
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.
Key Management	Select **IKE** or **Manual Key** from the drop-down list box. **IKE** provides more protection so it is generally recommended. **Manual Key** is a useful option for troubleshooting.
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.
Encapsulation Mode	Select **Tunnel** mode or **Transport** mode from the drop-down list box.
DNS Server (for IPSec VPN)	If there is a private DNS server that services the VPN, type its IP address here. The ZyWALL assigns this additional DNS server to the ZyWALL's DHCP clients that have IP addresses in this IPSec rule's range of local addresses.
	A DNS server allows clients on the VPN to find other computers and servers on the VPN by their (private) domain names.
Extended Authentication	
Enable Extended Authentication	Select this check box to activate extended authentication.
Server Mode	Select **Server Mode** to have this ZyWALL authenticate extended authentication clients that request this VPN connection.
	You must also configure the extended authentication clients' usernames and passwords in the auth server's local user database or a RADIUS server (see the Authentication Server section).
	Click **Local User** to go to the **Local User Database** screen where you can view and/or edit the list of users and passwords. Click **RADIUS** to go to the **RADIUS** screen where you can configure the ZyWALL to check an external RADIUS server.
	During authentication, if the ZyWALL (in server mode) does not find the extended authentication clients' user name in its internal user database and an external RADIUS server has been enabled, it attempts to authenticate the client through the RADIUS server.
Client Mode	Select **Client Mode** to have your ZyWALL use a username and password when initiating this VPN connection to the extended authentication server ZyWALL. Only a VPN extended authentication client can initiate this VPN connection.

Table 77   Edit VPN Rule (continued)

LABEL	DESCRIPTION
User Name	Enter a user name for your ZyWALL to be authenticated by the VPN peer (in server mode). The user name can be up to 31 case-sensitive ASCII characters, but spaces are not allowed. You must enter a user name and password when you select client mode.
Password	Enter the corresponding password for the above user name. The password can be up to 31 case-sensitive ASCII characters, but spaces are not allowed.
Local Policy	Local IP addresses must be static and correspond to the remote IPSec router's configured remote IP addresses.
	Two active SAs can have the same configured 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.
	In order to have more than one active rule with the **Secure Gateway Address** field set to **0.0.0.0**, the ranges of the local IP addresses cannot overlap between rules.
	If you configure an active rule with **0.0.0.0** in the **Secure Gateway Address** field and the LAN's full IP address range as the local IP address, then you cannot configure any other active rules with the **Secure Gateway Address** field set to **0.0.0.0**.
Address Type	Use the drop-down menu 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 your LAN behind your ZyWALL. When the **Address Type** field is configured to **Subnet Address**, this is a (static) IP address on the LAN behind your ZyWALL.
Ending IP Address/ Subnet Mask	When the **Address Type** field is configured to **Single Address**, this field is N/A. When the **Address Type** field is configured to **Range Address**, enter the end (static) IP address, in a range of computers on the LAN behind your ZyWALL. When the **Address Type** field is configured to **Subnet Address**, this is a subnet mask on the LAN behind your ZyWALL.
Remote Policy	Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses. The remote fields do not apply when the **Secure Gateway Address** field is configured to **0.0.0.0**. In this case only the remote IPSec router can initiate the VPN.
	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 menu to choose **Single Address**, **Range Address**, or **Subnet Address**. Select **Single Address** with a single IP address. Select **Range Address** for a specific range of IP addresses. Select **Subnet Address** to specify IP addresses on a network by their subnet mask.
Starting IP Address	When the **Address Type** field is configured to **Single Address**, enter a (static) IP address on the network behind the remote IPSec router. When the Addr Type field is configured to **Range Address**, enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Address Type** field is configured to **Subnet Address**, enter a (static) IP address on the network behind the remote IPSec router.

Table 77 Edit VPN Rule (continued)

LABEL	DESCRIPTION
Ending IP Address/ Subnet Mask	When the **Address Type** field is configured to **Single Address**, this field is N/A. When the **Address Type** field is configured to **Range Address**, enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Address Type** field is configured to **Subnet Address**, enter a subnet mask on the network behind the remote IPSec router.
Authentication Method	
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 IP Address** field (refer to the **My IP Address** 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 77   Edit VPN Rule (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 **Secure Gateway Address** field (refer to the **Secure 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 **Secure Gateway Address** field (refer to the **Secure 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 to 255 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.
Gateway Information	

Chapter 14 VPN Screens

Table 77 Edit VPN Rule (continued)

LABEL	DESCRIPTION
My Address	**IP Address** identifies the WAN IP address of the ZyWALL. You can select **IP Address** and 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 Address** changes after setup.
	The following applies if the **My Address** field is configured as 0.0.0.0:
	• When the WAN port operation mode is set to Active/Passive, the ZyWALL uses the IP address (static or dynamic) of the WAN port that is in use.
	• When the WAN port operation mode is set to Active/Active, the ZyWALL uses the IP address (static or dynamic) of the primary (highest priority) WAN port to set up the VPN tunnel as long as the corresponding WAN1 or WAN2 connection is up. If the corresponding WAN1 or WAN2 connection goes down, the ZyWALL uses the IP address of the other WAN port.
	• If both WAN connections go down, the ZyWALL uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect. See the chapter on WAN for details on dial backup and traffic redirect.
	Select **My Domain Name** and choose one of the dynamic domain names that you have configured (in the **DDNS** screen) to have the ZyWALL use that dynamic domain name's IP address.
Secure Gateway Address	Type the WAN IP address or the URL (up to 31 characters) of the IPSec router with which you're making the VPN connection. Set this field to **0.0.0.0** if the remote IPSec router has a dynamic WAN IP address (the **Key Management** field must be set to **IKE**).
	In order to have more than one active rule with the **Secure Gateway Address** field set to **0.0.0.0**, the ranges of the local IP addresses cannot overlap between rules.
	If you configure an active rule with **0.0.0.0** in the **Secure Gateway Address** field and the LAN's full IP address range as the local IP address, then you cannot configure any other active rules with the **Secure Gateway Address** field set to **0.0.0.0**.
IPSec Algorithm	
ESP	Select ESP if you want to use ESP (Encapsulation Security Payload). The ESP protocol (RFC 2406) provides encryption as well as some of the services offered by **AH**. If you select **ESP** here, you must select options from the **Encryption Algorithm** and **Authentication Algorithm** fields (described below).
Encryption Algorithm	Select **DES**, **3DES**, **AES** or **NULL** 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**.
	Select **NULL** to set up a tunnel without encryption. When you select **NULL**, you do not enter an encryption key.
Authentication Algorithm	Select **SHA1** or **MD5** from the drop-down list box. **MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slower. Select **MD5** for minimal security and **SHA-1** for maximum security.

Table 77 Edit VPN Rule (continued)

LABEL	DESCRIPTION
AH	Select **AH** if you want to use AH (Authentication Header Protocol). The AH protocol (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not for confidentiality, for which the ESP was designed. If you select **AH** here, you must select options from the **Authentication Algorithm** field (described below).
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.
Advanced	Click **Advanced** to configure more detailed settings of your IKE key management.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving.

14.11 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 119 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 the Perfect Forward Secrecy (PFS) section. 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.

14.11.1 X-Auth and IKE

X-Auth (Extended Authentication) inserts a new exchange between IKE phases 1 and 2 for client authentication.

14.11.2 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.

14.11.3 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.

14.11.4 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).

14.12 Configuring Advanced VPN Rule

Select **Advanced** at the bottom of the **Edit VPN Rule** screen. This is the **VPN Rule - Edit-Advanced** screen as shown next.

Figure 120 Edit VPN Rule: Advanced

The following table describes the labels in this screen.

Table 78   Edit VPN Rule: Advanced

LABEL	DESCRIPTION
Phase 1	
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.
Phase 2	
Active Protocol	Use the drop-down list box to choose from **ESP** or **AH**.
Encryption Algorithm	This field is available when you select **ESP** in the **Active Protocol** field. Select **DES**, **3DES**, **AES** or **NULL** 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**. Select **NULL** to set up a tunnel without encryption. When you select **NULL**, you do not enter an encryption key.
Authentication Algorithm	Select **SHA1** or **MD5** from the drop-down list box. **MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slower. Select **MD5** for minimal security and **SHA-1** for maximum security.
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.

Table 78   Edit VPN Rule: Advanced

LABEL	DESCRIPTION
Encapsulation	Select **Tunnel** mode or **Transport** mode from the drop-down list box.
Perfect Forward Secrecy (PFS)	Perfect Forward Secrecy (PFS) is disabled (**NONE**) by default in phase 2 IPSec SA setup. This allows faster IPSec setup, but is not so secure. Choose **DH1** or **DH2** from the drop-down list box 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. Select **YES** from the drop-down menu to enable replay detection, or select **NO** to disable it.
Protocol	Enter 1 for ICMP, 6 for TCP, 17 for UDP, etc. 0 is the default and signifies any protocol.
Local Port	
Start	"0" is the default and signifies any port. Type a port number from 0 to 65535. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.
End	Type a port number in this field to define a port range. This port number must be greater than that specified in the previous field. If **Local Port Start** is left at 0, **Local Port End** will also remain at 0.
Remote Port	
Start	Type up to 32 characters to identify this VPN policy. You may use any character, including spaces, but the ZyWALL drops trailing spaces.
End	Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field. If **Remote Port Start is** left at 0, **Remote Port End** will also remain at 0.
Apply	Click **Apply** to save your changes back to the ZyWALL and return to the **Edit VPN Rule** screen.
Cancel	Click **Cancel** to return to the **Edit VPN Rule** screen without saving your changes.

14.13 Manual Key Setup

Manual key management is useful if you have problems with **IKE** key management.

14.13.1 Security Parameter Index (SPI)

An SPI is used to distinguish different SAs terminating at the same destination and using the same IPSec protocol. This data allows for the multiplexing of SAs to a single gateway. The **SPI** (Security Parameter Index) along with a destination IP address uniquely identify a particular Security Association (SA). The **SPI** is transmitted from the remote VPN gateway to the local VPN gateway. The local VPN gateway then uses the network, encryption and key values that the administrator associated with the SPI to establish the tunnel.

> **Note:** Current ZyXEL implementation assumes identical outgoing and incoming SPIs.

14.14 Configuring Manual Key

You only configure **VPN Manual Key** when you select **Manual Key** in the **Key Management** field on the **Edit VPN Rule** screen. This is the **VPN Manual Key** screen as shown next.

Figure 121   VPN Manual Setup

The following table describes the labels in this screen.

Table 79   VPN Manual Setup

LABEL	DESCRIPTION
Property	
Active	Select this check box to activate this VPN policy.

Table 79 VPN Manual Setup

LABEL	DESCRIPTION
Name	Type up to 32 characters to identify this VPN policy. You may use any character, including spaces, but the ZyWALL drops trailing spaces.
Key Management	Select **IKE** or **Manual Key** from the drop-down list box. **Manual** is a useful option for troubleshooting if you have problems using **IKE** key management.
DNS Server (for IPSec VPN)	If there is a private DNS server that services the VPN, type its IP address here. The ZyWALL assigns this additional DNS server to the ZyWALL's DHCP clients that have IP addresses in this IPSec rule's range of local addresses. A DNS server allows clients on the VPN to find other computers and servers on the VPN by their (private) domain names.
Local Policy	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.
Remote Policy	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.
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.
Gateway Address	

Table 79   VPN Manual Setup

LABEL	DESCRIPTION
My Address	**IP Address** identifies the WAN IP address of the ZyWALL. You can select **IP Address** and 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 Address** changes after setup. The following applies if the **My Address** field is configured as 0.0.0.0: • When the WAN port operation mode is set to Active/Passive, the ZyWALL uses the IP address (static or dynamic) of the WAN port that is in use. • When the WAN port operation mode is set to Active/Active, the ZyWALL uses the IP address (static or dynamic) of the primary (highest priority) WAN port to set up the VPN tunnel as long as the corresponding WAN1 or WAN2 connection is up. If the corresponding WAN1 or WAN2 connection goes down, the ZyWALL uses the IP address of the other WAN port. • If both WAN connections go down, the ZyWALL uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect. See the chapter on WAN for details on dial backup and traffic redirect. Select **My Domain Name** and choose one of the dynamic domain names that you have configured (in the **DDNS** screen) to have the ZyWALL use that dynamic domain name's IP address.
Secure Gateway Addr	Type the WAN IP address or the URL (up to 31 characters) of the IPSec router with which you're making the VPN connection.
IPSec Property	
SPI	Type a unique **SPI** (Security Parameter Index) from one to four characters long. Valid Characters are "0, 1, 2, 3, 4, 5, 6, 7, 8, and 9".
Encapsulation Mode	Select **Tunnel** mode or **Transport** mode from the drop-down list box.
ESP	Select **ESP** if you want to use ESP (Encapsulation Security Payload). The ESP protocol (RFC 2406) provides encryption as well as some of the services offered by **AH**. If you select ESP here, you must select options from the **Encryption Algorithm** and **Authentication Algorithm** fields (described next).
Encryption Algorithm	Select **DES**, **3DES** or **NULL** from the drop-down list box. When **DES** is used for data communications, both sender and receiver must know the **Encryption Key**, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on DES that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. Select **NULL** to set up a tunnel without encryption. When you select **NULL**, you do not enter an encryption key.
Authentication Algorithm	Select **SHA1** or **MD5** from the drop-down list box. **MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slower. Select **MD5** for minimal security and **SHA-1** for maximum security.
AH	Select **AH** if you want to use AH (Authentication Header Protocol). The AH protocol (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not for confidentiality, for which the ESP was designed. If you select **AH** here, you must select options from the **Authentication Algorithm** field (described next).
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.

Table 79 VPN Manual Setup

LABEL	DESCRIPTION
Encryption Key (Only with ESP)	With **DES**, type a unique key 8 characters long. With **3DES**, type a unique key 24 characters long. Any characters may be used, including spaces, but trailing spaces are truncated.
Authentication Key	Type a unique authentication key to be used by IPSec if applicable. Enter 16 characters for **MD5** authentication or 20 characters for **SHA-1** authentication. Any characters may be used, including spaces, but trailing spaces are truncated.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving.

14.15 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 the Keep Alive section on keep alive to have the ZyWALL renegotiate an IPSec SA when the SA lifetime expires, even if there is no traffic.

Figure 122 SA Monitor
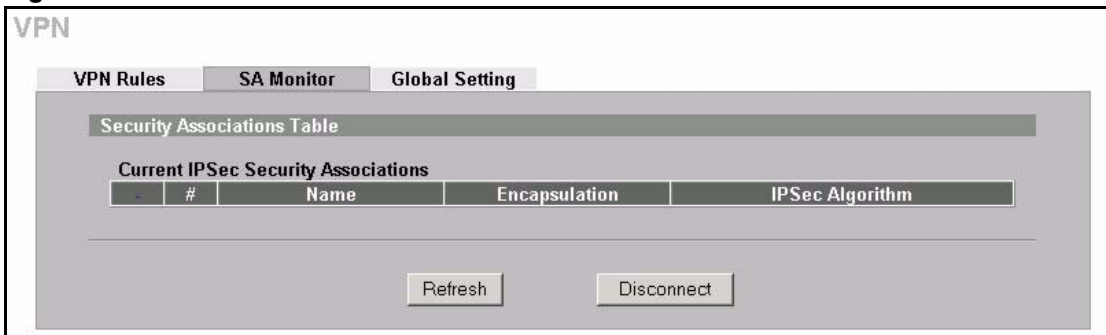
The following table describes the labels in this screen.

Table 80 SA Monitor

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.

Table 80 SA Monitor

LABEL	DESCRIPTION
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**.
Previous Page (if applicable)	Click **Previous Page** to view more items in the summary.
Next Page (If applicable)	Click **Next Page** to view more items in the summary.

14.16 Configuring Global Setting

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

Figure 123 Global Setting

The following table describes the labels in this screen.

Table 81 Global Setting

LABEL	DESCRIPTION
Windows Networking (NetBIOS over TCP/IP)	NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to find other computers. It may sometimes be necessary to allow NetBIOS packets to pass through VPN tunnels in order to allow local computers to find computers on the remote network and vice versa.
Allow Through IPSec Tunnel	Select this check box to send NetBIOS packets through the VPN connection.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

14.17 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.

14.17.1 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 124   Telecommuters Sharing One VPN Rule Example
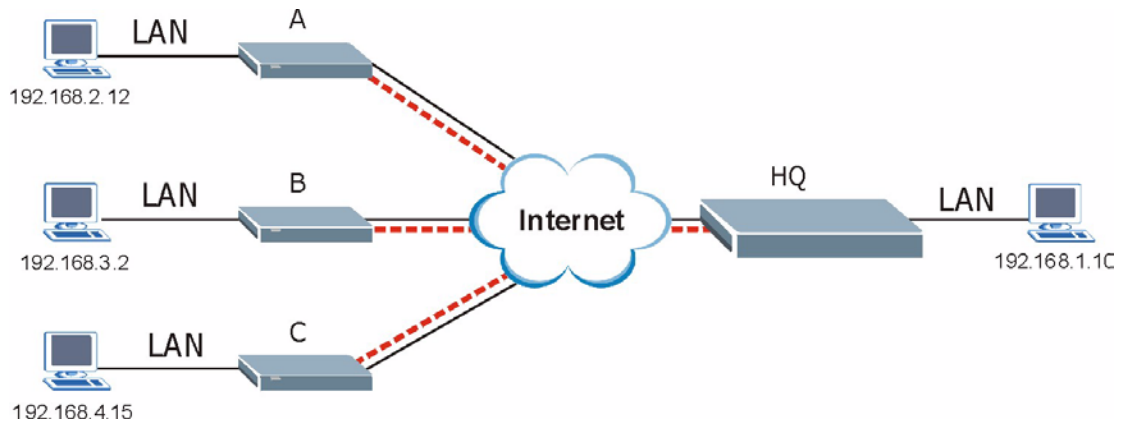
Table 82   Telecommuters Sharing One VPN Rule Example

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

14.17.2 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 the Negotiation Mode section), 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 125 Telecommuters Using Unique VPN Rules Example
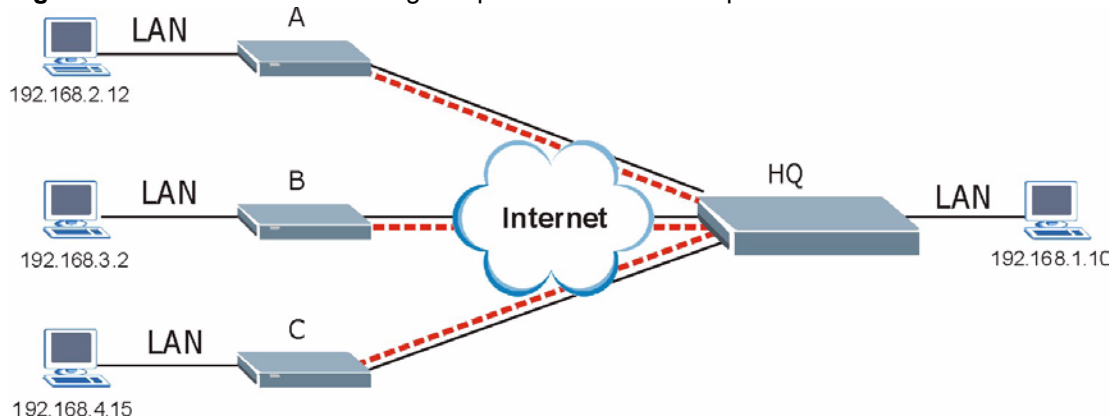
Table 83 Telecommuters Using Unique VPN Rules Example

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:

Table 83 Telecommuters Using Unique VPN Rules Example

TELECOMMUTERS	HEADQUARTERS
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
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

14.18 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.

C H A P T E R 15
Certificates

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

15.1 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).

15.1.1 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.

15.2 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.

15.3 Configuration Summary

This section summarizes how to manage certificates on the ZyWALL.

Figure 126 Certificate Configuration Overview
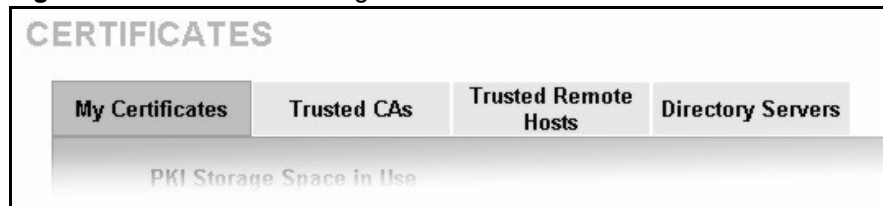
Use the **My Certificate** screens to generate and export self-signed certificates or certification requests and import the ZyWALL's CA-signed certificates.

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).

15.4 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 127 My Certificates

The following table describes the labels in this screen.

Table 84 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.

Table 84 My Certificates (continued)

LABEL	DESCRIPTION
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.
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 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 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.

15.5 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.

15.6 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:** 1. You can only import a certificate that matches a corresponding certification request that was generated by the ZyWALL.
> **Note:** 2. The certificate you import replaces the corresponding request in the My Certificates screen.
> **Note:** 3. You must remove any spaces from the certificate's filename before you can import it.

Figure 128   My Certificate Import

The following table describes the labels in this screen.

Table 85 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.

15.7 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 129 My Certificate Create

The following table describes the labels in this screen.

Table 86 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.
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 63 ASCII characters. The domain name or e-mail address is for identification purposes only and can be any string.
Organizational Unit	Type up to 63 characters to identify the organizational unit or department to which the certificate owner belongs. You may use any character, including spaces, but the ZyWALL drops trailing spaces.
Organization	Type up to 63 characters to identify the company or group to which the certificate owner belongs. You may use any character, including spaces, but the ZyWALL drops trailing spaces.
Country	Type up to 63 characters to identify the nation where the certificate owner is located. You may use any character, including spaces, but the ZyWALL drops trailing spaces.
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 the My Certificate Details section) 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.

Table 86   My Certificate Create (continued)

LABEL	DESCRIPTION
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.
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.

15.8 My Certificate Details

Click **CERTIFICATES**, and then **My Certificates** to open the **My Certificates** screen (see Figure 127). 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 130 My Certificate Details

The following table describes the labels in this screen.

Table 87 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 87 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.

15.9 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 131 Trusted CAs
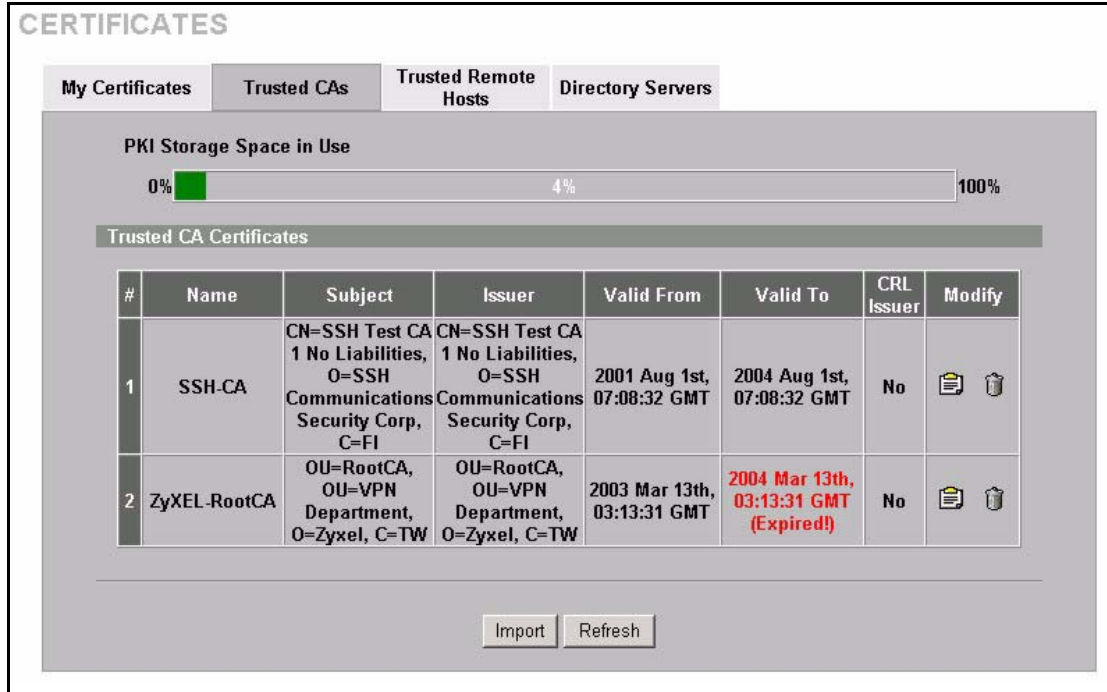
The following table describes the labels in this screen.

Table 88 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 88 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.

15.10 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 132 Trusted CA Import

The following table describes the labels in this screen.

Table 89 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.

15.11 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 133 Trusted CA Details

The following table describes the labels in this screen.

Table 90 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 90 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 90 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.

15.12 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 134 Trusted Remote Hosts
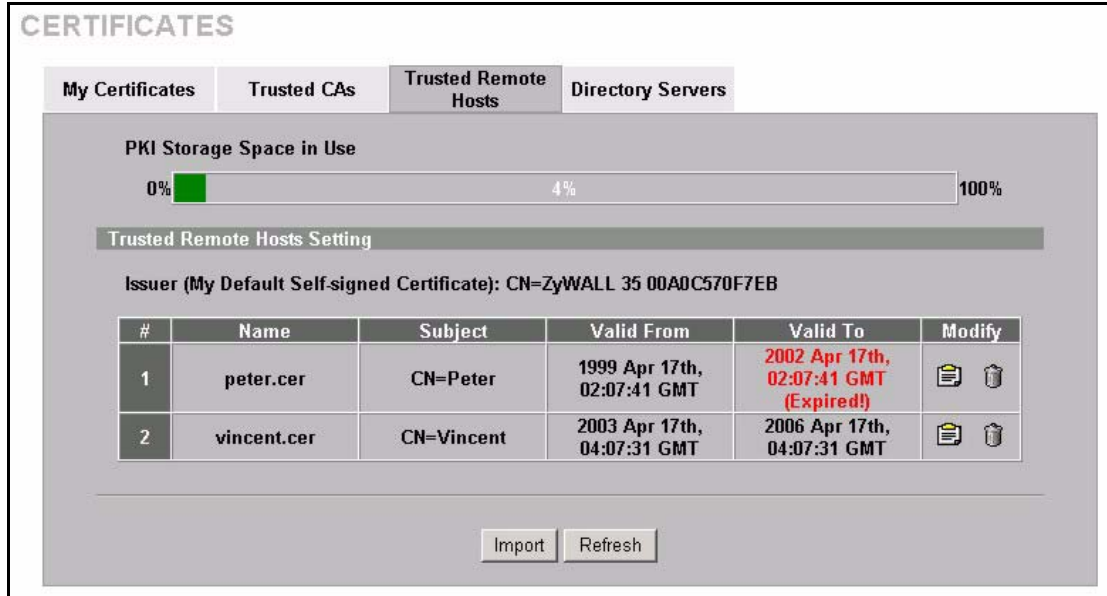
The following table describes the labels in this screen.

Table 91 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.
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 that subsequent certificates move up by one when you take this action.

Table 91 Trusted Remote Hosts (continued)

LABEL	DESCRIPTION
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.

15.13 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.

15.13.1 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 135 Remote Host Certificates
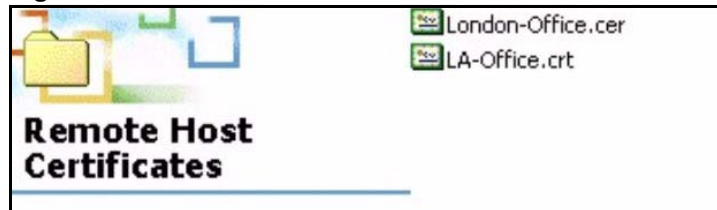
  3 Double-click the certificate's icon to open the **Certificate** window. Click the **Details** tab and scroll down to the **Thumbprint Algorithm** and **Thumbprint** fields.

Figure 136   Certificate Details
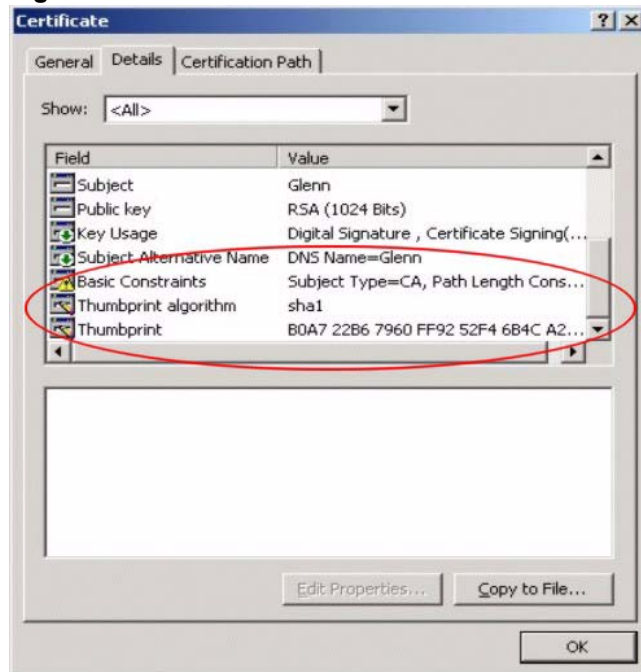
Verify (over the phone for example) that the remote host has the same information in the
Thumbprint Algorithm and **Thumbprint** fields.

15.14 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 137 Trusted Remote Host Import
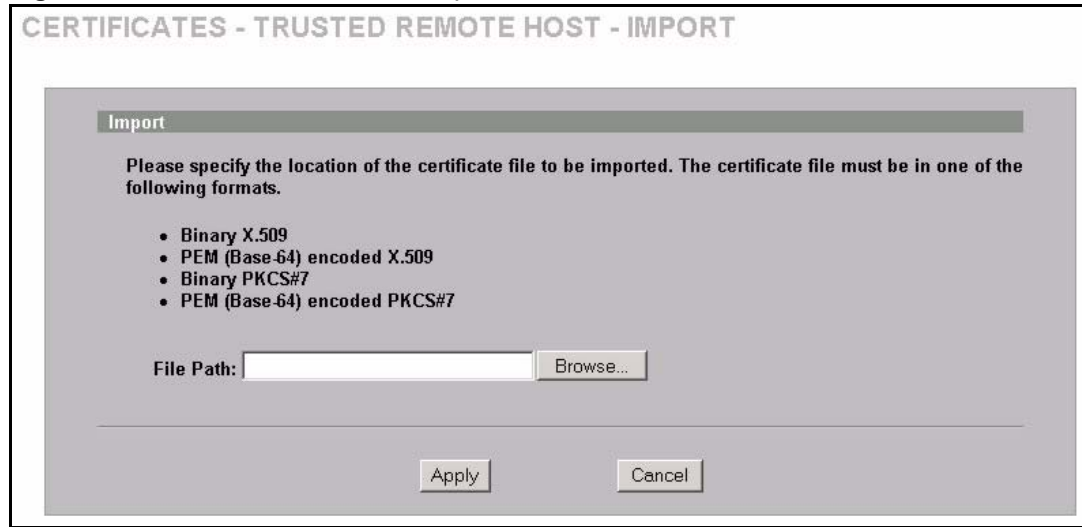
The following table describes the labels in this screen.

Table 92 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.

15.15 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 138 Trusted Remote Host Details
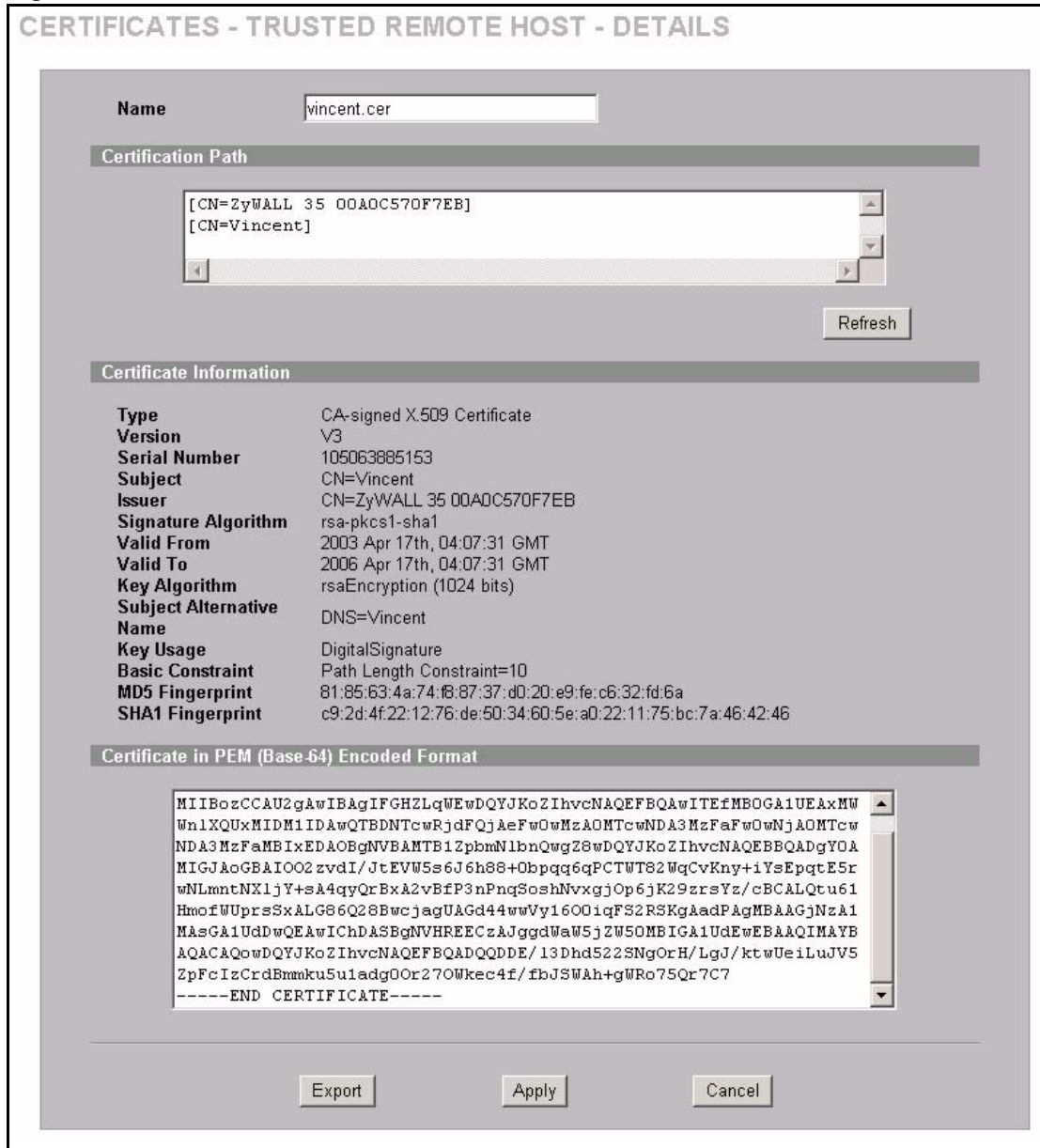
The following table describes the labels in this screen.

Table 93 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 93 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 the Verifying a Trusted Remote Host's Certificate section 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 the Verifying a Trusted Remote Host's Certificate section for how to verify a remote host's certificate.

Table 93 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.

15.16 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 139 Directory Servers
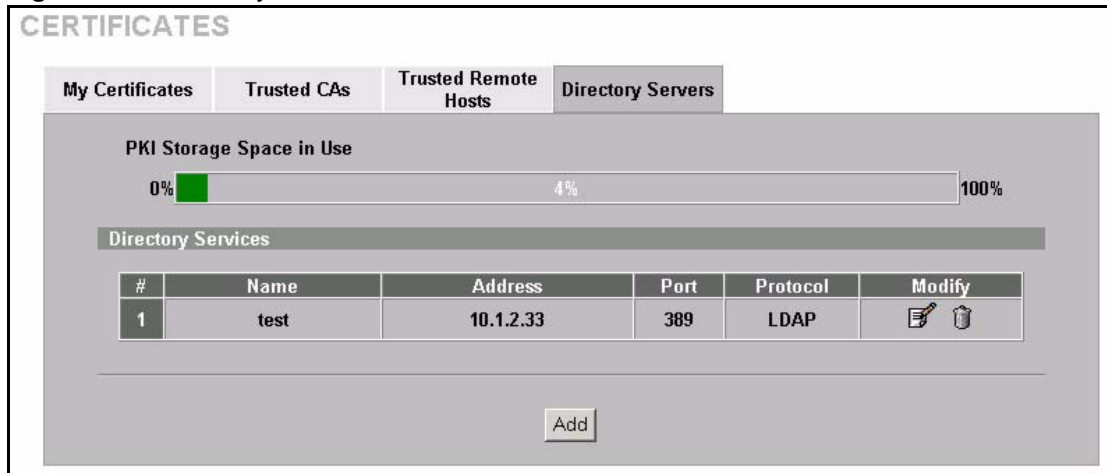
The following table describes the labels in this screen.

Table 94 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.

15.17 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 140 Directory Server Add

The following table describes the labels in this screen.

Table 95 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.

C HAPTER 16
Network Address Translation (NAT)

This chapter discusses how to configure NAT on the ZyWALL.

16.1 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.

16.1.1 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 96 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.

16.1.2 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. Although you can make designated servers on the LAN accessible to the outside world, it is strongly recommended that you attach those servers to the DMZ port instead. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping), NAT offers the additional benefit of firewall protection. With no servers defined, your ZyWALL filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631*, *The IP Network Address Translator (NAT)*.

16.1.3 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 141   How NAT Works
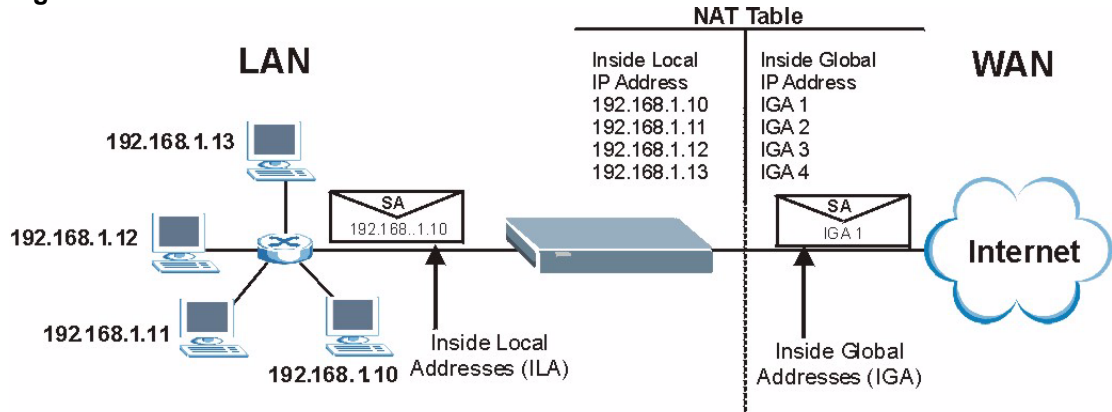
16.1.4 NAT Application

The following figure illustrates a possible NAT application, where three inside LANs (logical LANs using IP Alias) behind the ZyWALL can communicate with three distinct WAN networks. More examples follow at the end of this chapter.

Figure 142   NAT Application With IP Alias
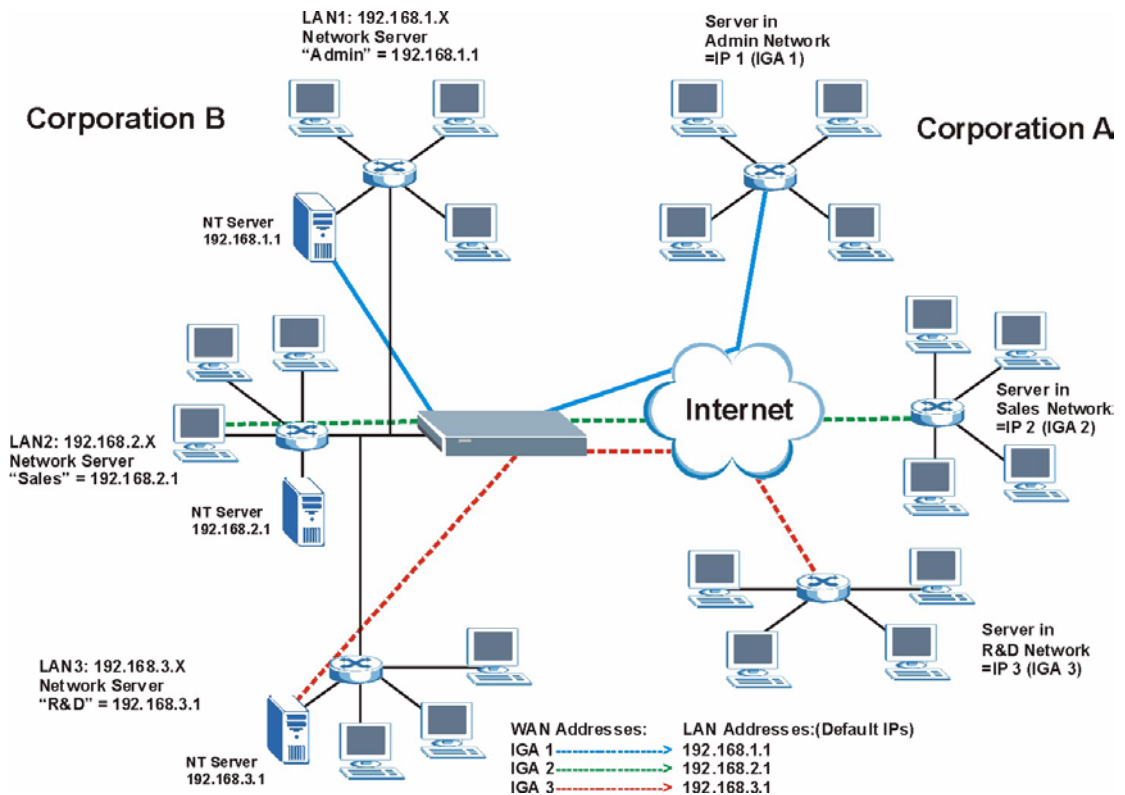
16.1.5 NAT Mapping Types

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

- **One to One**: In One-to-One mode, the ZyWALL maps one local IP address to one global IP address.
- **Many to One**: In Many-to-One mode, the ZyWALL maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature (the **SUA** option).
- **Many to Many Overload**: In Many-to-Many Overload mode, the ZyWALL maps the multiple local IP addresses to shared global IP addresses.
- **Many One to One**: In Many-One-to-One mode, the ZyWALL maps each local IP address to a unique global IP address.
- **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world although, it is highly recommended that you use the DMZ port for these servers instead.

> **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 97 NAT Mapping Types

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

16.2 Using NAT

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

16.2.1 SUA (Single User Account) Versus NAT

SUA (Single User Account) is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. The ZyWALL also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types. Select either **SUA** or **Full Feature** in **NAT Overview**.

Selecting **SUA** means (latent) multiple WAN-to-LAN and WAN-to-DMZ address translation. That means that computers on your DMZ with public IP addresses will still have to undergo NAT mapping if you're using **SUA** NAT mapping. If this is not your intention, then select **Full Feature** NAT and don't configure NAT mapping rules to those computers with public IP addresses on the DMZ.

16.3 Configuring NAT Overview

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

Figure 143 NAT Overview

The following table describes the labels in this screen.

Table 98 NAT Overview

LABEL	DESCRIPTION
Global Settings	
Max. Concurrent Sessions	This read-only field displays the highest number of NAT sessions that the ZyWALL will permit at one time.
Max. Concurrent Sessions Per Host	Use this field to set the highest number of NAT sessions that the ZyWALL will permit a host to have at one time.
WAN Operation Mode	This read-only field displays the operation mode of the ZyWALL's WAN ports.
WAN 1, 2	
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.

Table 98 NAT Overview (continued)

LABEL	DESCRIPTION
Address Mapping Rules	Select **SUA** to have the ZyWALL use its permanent, pre-defined NAT address mapping rules.
	Select **Full Feature** to have the ZyWALL use the address mapping rules that you configure. This is the equivalent of what used to be called full feature NAT.
	The bar displays how many of the ZyWALL's possible address mapping rules are configured. The first number shows how many address mapping rules are configured on the ZyWALL. The second number shows the maximum number of address mapping rules that can be configured on the ZyWALL.
Port Forwarding Rules	The bar displays how many of the ZyWALL's possible port forwarding rules are configured. The first number shows how many port forwarding rules are configured on the ZyWALL. The second number shows the maximum number of port forwarding rules that can be configured on the ZyWALL.
Port Triggering Rules	The bar displays how many of the ZyWALL's possible trigger port rules are configured. The first number shows how many trigger port rules are configured on the ZyWALL. The second number shows the maximum number of trigger port rules that can be configured on the ZyWALL.
Copy to WAN 2 (and Copy to WAN 1)	Click **Copy to WAN 2** (or **Copy to WAN 1**) to duplicate this WAN port's NAT port forwarding or trigger port rules on the other WAN port.
	Note: Using the copy button overwrites the other WAN port's existing rules.
	The copy button is best suited for initial NAT configuration where you have configured NAT port forwarding or trigger port rules for one port and want to use similar rules for the other WAN port. You can use the other NAT screens to edit the NAT rules after you copy them from one WAN port to the other.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

16.4 Configuring Address Mapping

Ordering your rules is important because the ZyWALL applies the rules in the order that you specify. When a rule matches the current packet, the ZyWALL takes the corresponding action and the remaining rules are ignored. If there are any empty rules before your new configured rule, your configured rule will be pushed up by that number of empty rules. For example, if you have already configured rules 1 to 6 in your current set and now you configure rule number 9. In the set summary screen, the new rule will be rule 7, not 9. Now if you delete rule 4, rules 5 to 7 will be pushed up by 1 rule, so old rules 5, 6 and 7 become new rules 4, 5 and 6.

To change your ZyWALL's Address Mapping settings, click **NAT**, then the **Address Mapping** tab. The screen appears as shown (some of the screen's blank rows are not shown).

Figure 144 Address Mapping

The following table describes the labels in this screen.

Table 99 Address Mapping

LABEL	DESCRIPTION
SUA Address Mapping Rules	This read-only table displays the default address mapping rules.
Full Feature Address Mapping Rules	
WAN Interface	Select the WAN port for which you want to view or configure address mapping rules.
Go To Page	Choose a page from the drop-down list box to display the corresponding summary page of address mapping rules.
#	This is the rule index number.
Local Start IP	This refers to the Inside Local Address (ILA), which is the starting local IP address. If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the **Local Start IP** address. Local IP addresses are **N/A** for **Server** port mapping.
Local End IP	This is the end Inside Local Address (ILA). If the rule is for all local IP addresses, then this field displays 255.255.255.255 as the **Local End IP** address. This field is **N/A** for **One-to-One** and **Server** mapping types.

Table 99   Address Mapping (continued)

LABEL	DESCRIPTION
Global Start IP	This refers to the Inside Global IP Address (IGA), that is the starting global IP address. 0.0.0.0 is for a dynamic IP address from your ISP with **Many-to-One** and **Server** mapping types.
Global End IP	This is the ending Inside Global Address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server** mapping types.
Type	1. **One-to-One** mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type. 2. **Many-to-One** mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported only. 3. **Many-to-Many Overload** mode maps multiple local IP addresses to shared global IP addresses. 4. **Many One-to-One** mode maps each local IP address to unique global IP addresses. 5. **Server** allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Modify	Click the edit icon to go to the screen where you can edit the address mapping rule. Click the delete icon to delete an existing address mapping rule. A window display asking you to confirm that you want to delete the address mapping rule. Note that subsequent address mapping rules move up by one when you take this action.
Insert	Click **Insert** to insert a new mapping rule before an existing one.

16.4.1 Address Mapping Edit

To edit an address mapping rule, click the **Edit** button to display the screen shown next.

Figure 145   Address Mapping Edit

The following table describes the labels in this screen.

Table 100 Address Mapping Edit

LABEL	DESCRIPTION
Type	Choose the port mapping type from one of the following. 1. **One-to-One**: One-to-one mode maps one local IP address to one global IP address. Note that port numbers do not change for One-to-one NAT mapping type. 2. **Many-to-One**: Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature. 3. **Many-to-Many Ov** (Overload): Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses. 4. **Many One-to-One**: Many One-to-one mode maps each local IP address to unique global IP addresses. 5. **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Local Start IP	This is the starting Inside Local IP Address (ILA). Local IP addresses are **N/A** for **Server** port mapping.
Local End IP	This is the end Inside Local IP Address (ILA). If your rule is for all local IP addresses, then enter 0.0.0.0 as the **Local Start IP** address and 255.255.255.255 as the **Local End IP** address. This field is **N/A** for **One-to-One** and **Server** mapping types.
Global Start IP	This is the starting Inside Global IP Address (IGA). Enter **0.0.0.0** here if you have a dynamic IP address from your ISP.
Global End IP	This is the ending Inside Global IP Address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server** mapping types.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving.

16.5 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

16.5.1 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.

16.5.2 Port Forwarding: Services and Port Numbers

The ZyWALL provides the additional safety of the DMZ ports for connecting your publicly accessible servers. This makes the LAN more secure by physically separating it from your public servers.

Use the **Port Forwarding** screen to forward incoming service requests to the server(s) on your local network.

The most often used port numbers are shown in the 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 101   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

16.5.3 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 146 Multiple Servers Behind NAT Example
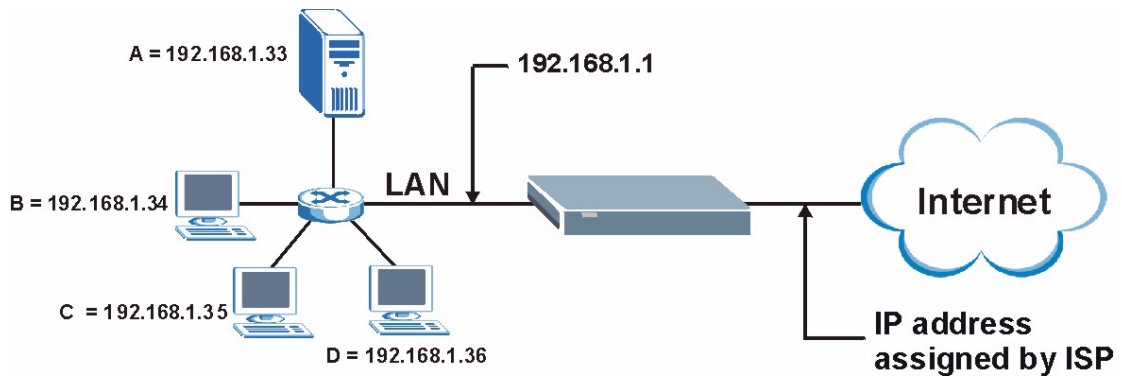
16.5.4 NAT and Multiple WAN

The ZyWALL has two WAN ports. You can configure port forwarding and trigger port rule sets for the first WAN port and separate sets of rules for the second WAN port.

16.5.5 Port Translation

The ZyWALL can translate the destination port number or a range of port numbers of packets coming from the WAN to another destination port number or range of port numbers on the LAN (or DMZ). When you use port forwarding without port translation, a single server on the LAN or DMZ 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 or DMZ 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 147 Port Translation Example
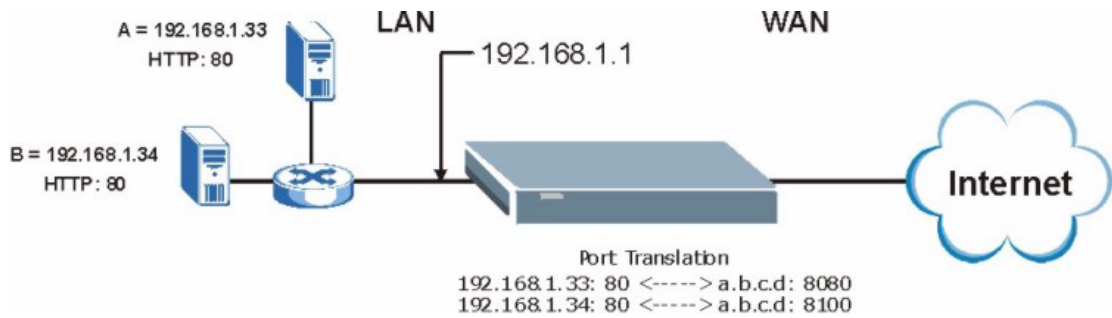
16.6 Configuring Port Forwarding

> **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 101 for port numbers commonly used for particular services.

> **Note:** The last port forwarding rule is reserved for Roadrunner services. The rule is activated only when you set the **WAN Encapsulation** to **Ethernet** and the **Service Type** to something other than **Standard**.

Figure 148 Port Forwarding
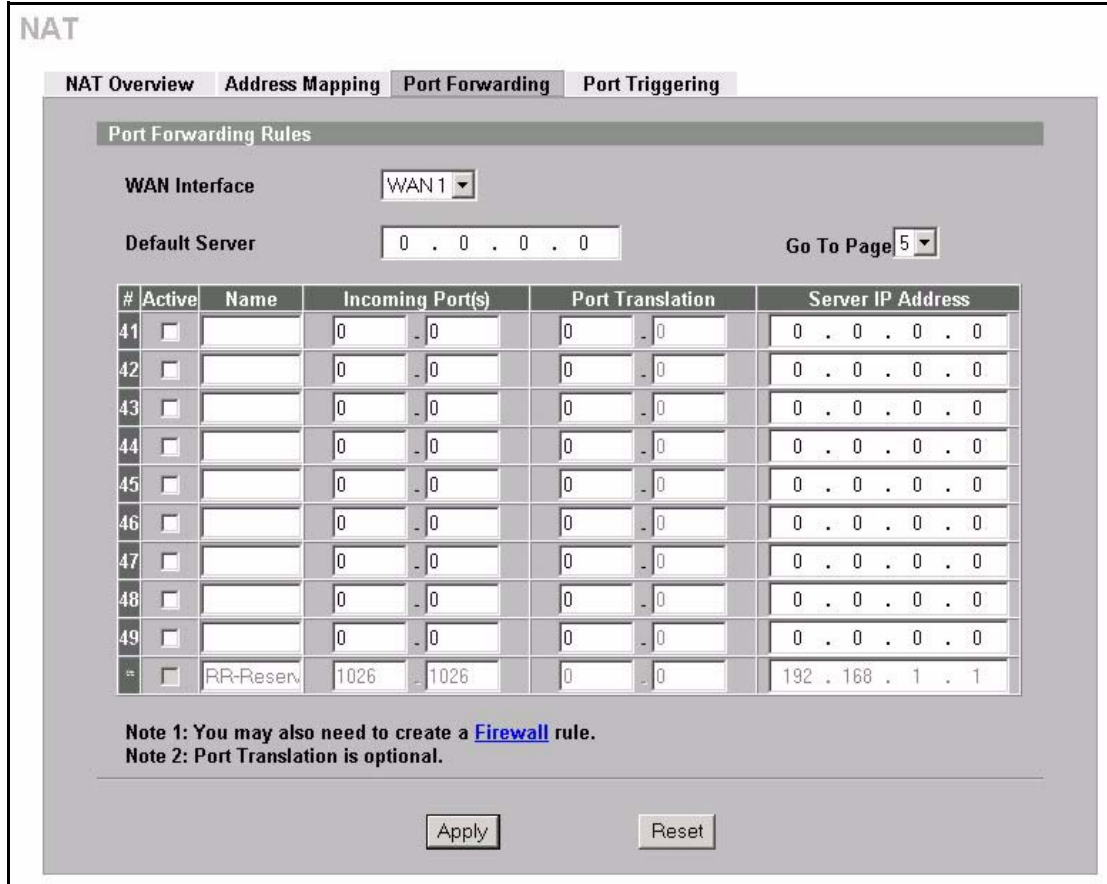
The following table describes the labels in this screen.

Table 102 Port Forwarding

LABEL	DESCRIPTION
WAN Interface	Select the WAN port for which you want to view or configure address mapping rules.
Default Server	In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in this screen. If you do not assign a **Default Server** IP address, the ZyWALL discards all packets received for ports that are not specified here or in the remote management setup.
Go To Page	Choose a page from the drop-down list box to display the corresponding summary page of the port forwarding servers.
#	This is the number of an individual port forwarding server entry.
Active	Select this check box to enable the port forwarding server entry. Clear this check box to disallow forwarding of these ports to an inside server without having to delete the entry.
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.

Table 102 Port Forwarding

LABEL	DESCRIPTION
Server IP Address	Enter the inside IP address of the server here.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

16.7 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 149   Trigger Port Forwarding Process: Example
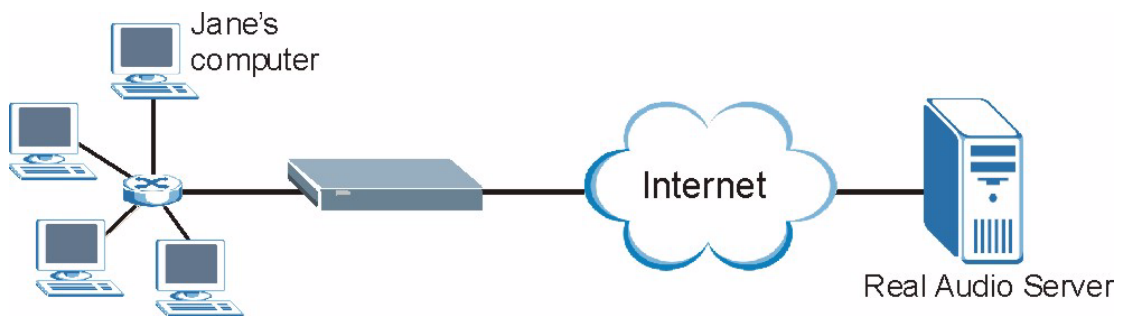
1 Jane requests a file from the Real Audio server (port 7070).

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 150 Port Triggering
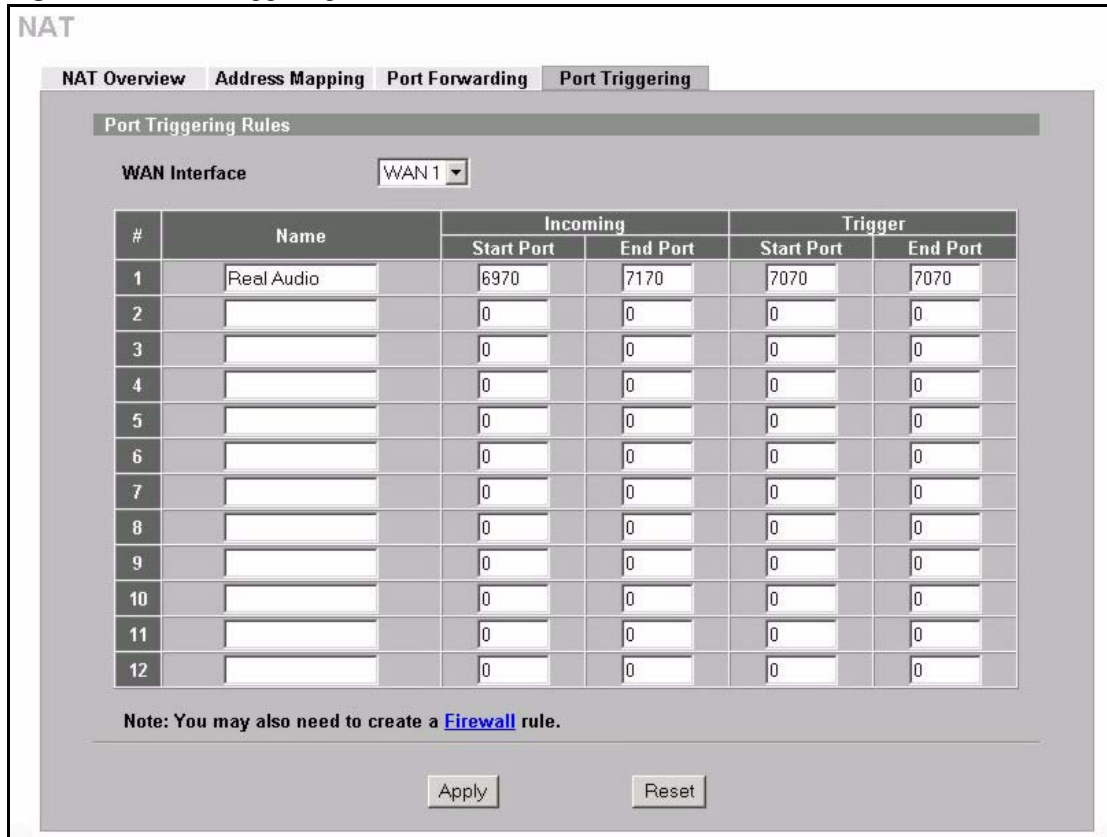
The following table describes the labels in this screen.

Table 103 Port Triggering

LABEL	DESCRIPTION
WAN Interface	Select the WAN port for which you want to view or configure address mapping rules.
#	This is the rule index number (read-only).
Name	Type a unique name (up to 15 characters) for identification purposes. All characters are permitted - including spaces.
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.

Table 103   Port Triggering

LABEL	DESCRIPTION
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 16 Network Address Translation (NAT)

CHAPTER 17
Static Route

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

17.1 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 151   Example of Static Routing Topology
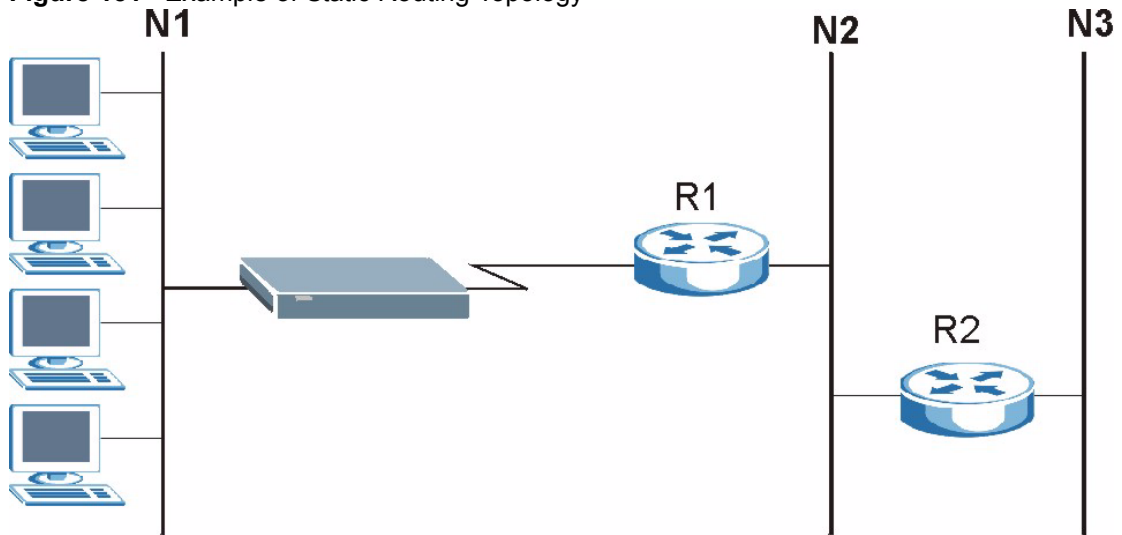
17.2 Configuring IP Static Route

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

> **Note:** The first two static route entries are for default WAN1 and WAN2 routes and cannot be modified or deleted. The name of each 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 152 IP Static Route

The following table describes the labels in this screen.

Table 104 IP Static Route

LABEL	DESCRIPTION
#	This is the number of an individual static route.
Name	This is the name that describes or identifies this route.
Active	This field shows whether this static route is active (**Yes**) or not (**No**).

Table 104   IP Static Route

LABEL	DESCRIPTION
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.

17.2.1 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 153   Edit IP Static Route

The following table describes the labels in this screen.

Table 105   Edit IP Static Route

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.

Table 105   Edit IP Static Route

LABEL	DESCRIPTION
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 18
Policy Route

This chapter covers setting and applying policies used for IP routing.

18.1 Introduction to IP Policy Routing

Traditionally, routing is based on the destination address only and the ZyWALL takes the shortest path to forward a packet. IP Policy Routing (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to incoming packets on a per interface basis, prior to the normal routing.

18.2 Benefits

- Source-Based Routing – Network administrators can use policy-based routing to direct traffic from different users through different connections.
- Quality of Service (QoS) – Organizations can differentiate traffic by setting the precedence or ToS (Type of Service) values in the IP header at the periphery of the network to enable the backbone to prioritize traffic.
- Cost Savings – IPPR allows organizations to distribute interactive traffic on high-bandwidth, high-cost paths while using low-cost paths for batch traffic.
- Load Sharing – Network administrators can use IPPR to distribute traffic among multiple paths.

18.3 Routing Policy

Individual routing policies are used as part of the overall IPPR process. A policy defines the matching criteria and the action to take when a packet meets the criteria. The action is taken only when all the criteria are met. The criteria include the source address and port, IP protocol (ICMP, UDP, TCP, etc.), destination address and port, ToS and precedence (fields in the IP header) and length. The inclusion of length criterion is to differentiate between interactive and bulk traffic. Interactive applications, e.g., telnet, tend to have short packets, while bulk traffic, e.g., file transfer, tends to have large packets.

The actions that can be taken include:

- Routing the packet to a different gateway (and hence the outgoing interface).
- Setting the ToS and precedence fields in the IP header.

IPPR follows the existing packet filtering facility of RAS in style and in implementation.

18.4 IP Routing Policy Setup

Click **POLICY ROUTE** to open the **Policy Route Summary** screen (some of the screen's blank rows are not shown).

Figure 154   Policy Route Summary

The following table describes the labels in this screen.

Table 106 Policy Route Setup

LABEL	DESCRIPTION
#	This is the number of an individual policy route.
Active	This field shows whether the policy is active or inactive.
Source Address/ Port	This is the source IP address range and/or port number range.
Destination Address/Port	This is the destination IP address range and/or port number range.
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.
Protocol	This is the IP protocol and can be **ICMP**, **UDP**, **TCP** or **ALL**.
Action	This field specifies whether action should be taken on criteria **Matched** or **Not Matched**.
Modify	Click the edit icon to go to the screen where you can edit the routing policy on the ZyWALL.
	Click the delete icon to remove an existing routing policy from the ZyWALL. A window display asking you to confirm that you want to delete the address mapping rule.
Move	Type a policy route's index number and the number for where you want to put that rule. Click **Move** to move the rule to the number that you typed.
	The ordering of your rules is important as they are applied in order of their numbering.

18.5 Configuring the IP Policy Route Entry

Click the edit icon to open the screen as shown next.

Figure 155 Edit IP Policy Route

The following table describes the labels in this screen.

Table 107 Edit IP Policy Route

LABEL	DESCRIPTION
Criteria	
Active	Select the check box to activate the policy.
Rule Index	This is the index number of the policy route.
IP Protocol	Select **Predefined** and then the IP protocol from **ALL(0)**, **ICMP(1)**, **IGMP(2)**, **TCP(6)**, **UDP(17)**, **GRE(47)**, **ESP(50)** or **AH(51)**. Otherwise, select **Custom** and enter a number from 0 to 255.
Type of Service	Prioritize incoming network traffic by choosing from **Any**, **Normal**, **Min Delay**, **Max Thruput**, **Max Reliable** or **Mix Cost**.
Precedence	Precedence value of the incoming packet. Select a value from **0** to **7** or **Any**.

Table 107 Edit IP Policy Route (continued)

LABEL	DESCRIPTION
Packet Length	Type a length of packet (in bytes). The operators in the **Len Compare** field apply to incoming packets of this length.
Length Comparison	Choose from **Equal**, **Not Equal**, **Less**, **Greater**, **Less or Equal** or **Greater or Equal**.
Source	
Interface	Use the check box to select **LAN**, **DMZ**, **WAN_1** and/or **WAN_2**.
Starting IP Address	Enter the source starting IP address.
Ending IP Address	Enter the source ending IP address.
Starting Port	Enter the source starting port number. This field is applicable only when you select **TCP** or **UDP** in the IP Protocol field.
Ending Port	Enter the source ending port number. This field is applicable only when you select **TCP** or **UDP** in the IP Protocol field.
Destination	
Starting IP Address	Enter the destination starting IP address.
Ending IP Address	Enter the destination ending IP address.
Starting Port	Enter the destination starting port number. This field is applicable only when you select **TCP** or **UDP** in the IP Protocol field.
Ending Port	Enter the destination ending port number. This field is applicable only when you select **TCP** or **UDP** in the IP Protocol field.
Action Applies to	Specifies whether action should be taken on criteria **Matched** or **Not Matched**.
Routing Action	
Gateway	Select **User-Defined** and enter the IP address of the gateway if you want to specify the IP address of the gateway. The gateway is an immediate neighbor of your ZyWALL that will forward the packet to the destination. The gateway must be a router on the same segment as your ZyWALL's LAN or WAN port.
	Select **WAN Interface** to have the ZyWALL send traffic that matches the policy route through a specific WAN port. Select the WAN port from the drop-down list box.
	Select the **Use another interface when the specified WAN interface is not available.** check box to have the ZyWALL send traffic that matches the policy route through the other WAN interface if it cannot send the traffic through the WAN interface you selected. This option is only available when you select **WAN Interface**.
Converted Type of Service	Set the new TOS value of the outgoing packet. Prioritize incoming network traffic by choosing **Don't Change**, **Normal**, **Min Delay**, **Max Thruput**, **Max Reliable** or **Min Cost**.
Converted Precedence	Set the new outgoing packet precedence value. Values are **0** to **7** or **Don't Change**.
Log	Select **Yes** from the drop-down list box to make an entry in the system log when a policy is executed.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving.

C H A P T E R 19
Bandwidth Management

This chapter describes the functions and configuration of bandwidth management.

19.1 Bandwidth Management Overview

Bandwidth management allows you to allocate an interface's outgoing capacity to specific types of traffic. It can also help you make sure that the ZyWALL forwards certain types of traffic (especially real-time applications) with minimum delay. With the use of real-time applications such as Voice-over-IP (VoIP) increasing, the requirement for bandwidth allocation is also increasing.

- Bandwidth management addresses questions such as:
- Who gets how much access to specific applications?
- What priority level should you give to each type of traffic?
- Which traffic must have guaranteed delivery?
- How much bandwidth should be allotted to guarantee delivery?

Bandwidth management also allows you to configure the allowed output for an interface to match what the network can handle. This helps reduce delays and dropped packets at the next routing device. For example, you can set the WAN interface speed to 1000kbps if the broadband device connected to the WAN port has an upstream speed of 1000kbps. All configuration screens display measurements in kbps (kilobits per second), but this *User's Guide* also uses Mbps (megabits per second) for brevity's sake.

19.2 Bandwidth Classes and Filters

Use bandwidth classes and sub-classes to allocate specific amounts of bandwidth capacity (bandwidth budgets). Configure a bandwidth filter to define a bandwidth class (or sub-class) based on a specific application and/or subnet. Use the **Class Setup** tab (see the Bandwidth Manager Class Configuration section) to set up a bandwidth class's name, bandwidth allotment, and bandwidth filter. You can configure up to one bandwidth filter per bandwidth class. You can also configure bandwidth classes without bandwidth filters. However, it is recommended that you configure sub-classes with filters for any classes that you configure without filters. The ZyWALL leaves the bandwidth budget allocated and unused for a class that does not have a filter itself or sub-classes with filters. View your configured bandwidth classes and sub-classes in the **Class Setup** tab (see the Configuring Class Setup section) for details.

The total of the configured bandwidth budgets for sub-classes cannot exceed the configured bandwidth budget speed of the parent class.

19.3 Proportional Bandwidth Allocation

Bandwidth management allows you to define how much bandwidth each class gets; however, the actual bandwidth allotted to each class decreases or increases in proportion to actual available bandwidth.

19.4 Bandwidth Management Usage Examples

These examples show bandwidth management allotments on a WAN interface that is configured for 10Mbps.

19.4.1 Application-based Bandwidth Management Example

The bandwidth classes in the following example are based solely on application. Each bandwidth class (VoIP, Web, FTP, E-mail and Video) is allotted 128 Kbps.

Figure 156   Application-based Bandwidth Management Example
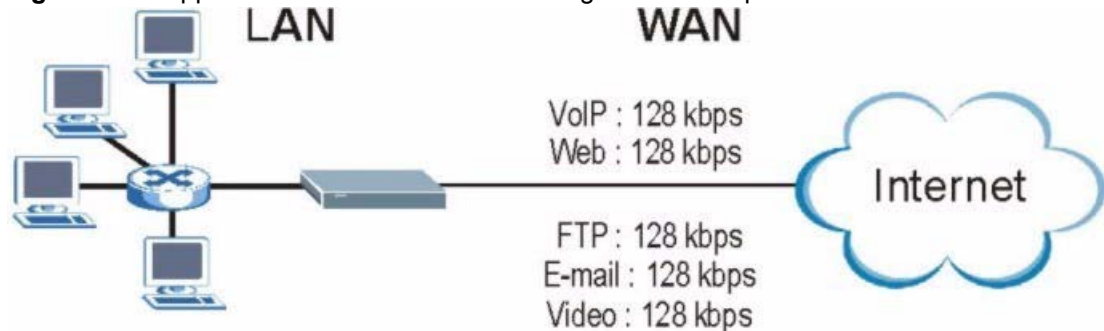
19.4.2 Subnet-based Bandwidth Management Example

The following example uses bandwidth classes based solely on LAN subnets. Each bandwidth class (Subnet A and Subnet B) is allotted 320 Kbps.

Figure 157 Subnet-based Bandwidth Management Example
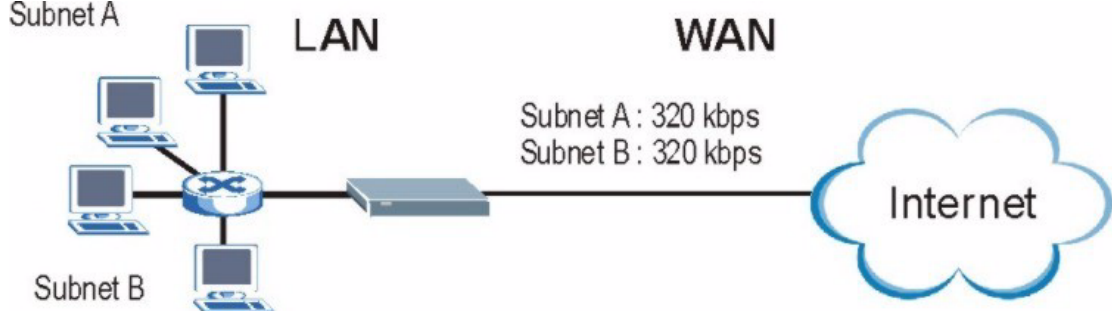
19.4.3 Application and Subnet-based Bandwidth Management Example

The following example uses bandwidth classes based on LAN subnets and applications (specific applications in each subnet are allotted bandwidth).

Table 108 Application and Subnet-based Bandwidth Management Example

TRAFFIC TYPE	FROM SUBNET A	FROM SUBNET B
VoIP	64 Kbps	64 Kbps
Web	64 Kbps	64 Kbps
FTP	64 Kbps	64 Kbps
E-mail	64 Kbps	64 Kbps
Video	64 Kbps	64 Kbps

Figure 158 Application and Subnet-based Bandwidth Management Example
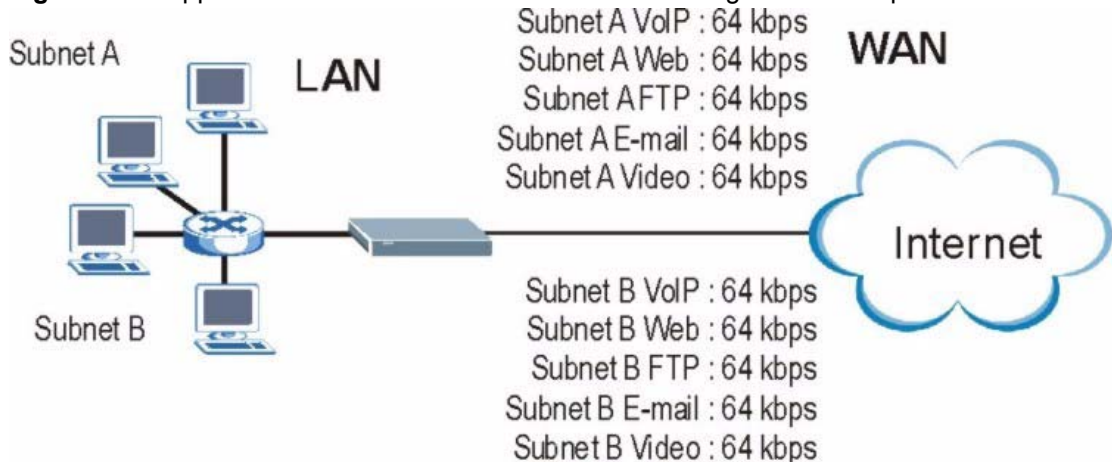
19.5 Scheduler

The scheduler divides up an interface's bandwidth among the bandwidth classes. The ZyWALL has two types of scheduler: fairness-based and priority-based.

19.5.1 Priority-based Scheduler

With the priority-based scheduler, the ZyWALL forwards traffic from bandwidth classes according to the priorities that you assign to the bandwidth classes. The larger a bandwidth class's priority number is, the higher the priority. Assign real-time applications (like those using audio or video) a higher priority number to provide smoother operation.

19.5.2 Fairness-based Scheduler

The ZyWALL divides bandwidth equally among bandwidth classes when using the fairness-based scheduler; thus preventing one bandwidth class from using all of the interface's bandwidth.

19.6 Maximize Bandwidth Usage

The maximize bandwidth usage option (see Figure 162) allows the ZyWALL to divide up any available bandwidth on the interface (including unallocated bandwidth and any allocated bandwidth that a class is not using) among the bandwidth classes that require more bandwidth.

When you enable maximize bandwidth usage, the ZyWALL first makes sure that each bandwidth class gets up to its bandwidth allotment. Next, the ZyWALL divides up an interface's available bandwidth (bandwidth that is unbudgeted or unused by the classes) depending on how many bandwidth classes require more bandwidth and on their priority levels. When only one class requires more bandwidth, the ZyWALL gives extra bandwidth to that class.

When multiple classes require more bandwidth, the ZyWALL gives the highest priority classes the available bandwidth first (as much as they require, if there is enough available bandwidth), and then to lower priority classes if there is still bandwidth available. The ZyWALL distributes the available bandwidth equally among classes with the same priority level.

19.6.1 Reserving Bandwidth for Non-Bandwidth Class Traffic

Do the following three steps to configure the ZyWALL to allow bandwidth for traffic that is not defined in a bandwidth filter.

1 Leave some of the interface's bandwidth unbudgeted.

2 Do not enable the interface's **Maximize Bandwidth Usage** option.

3 Do not enable bandwidth borrowing on the sub-classes that have the root class as their parent (see the Bandwidth Borrowing section).

19.6.2 Maximize Bandwidth Usage Example

Here is an example of a ZyWALL that has maximize bandwidth usage enabled on an interface. The first figure shows each bandwidth class's bandwidth budget and priority. The classes are set up based on subnets. The interface is set to 10 Mbps. Each subnet is allocated 2 Mbps. The unbudgeted 2 Mbps allows traffic not defined in one of the bandwidth filters to go out when you do not select the maximize bandwidth option.

Figure 159 Bandwidth Allotment Example
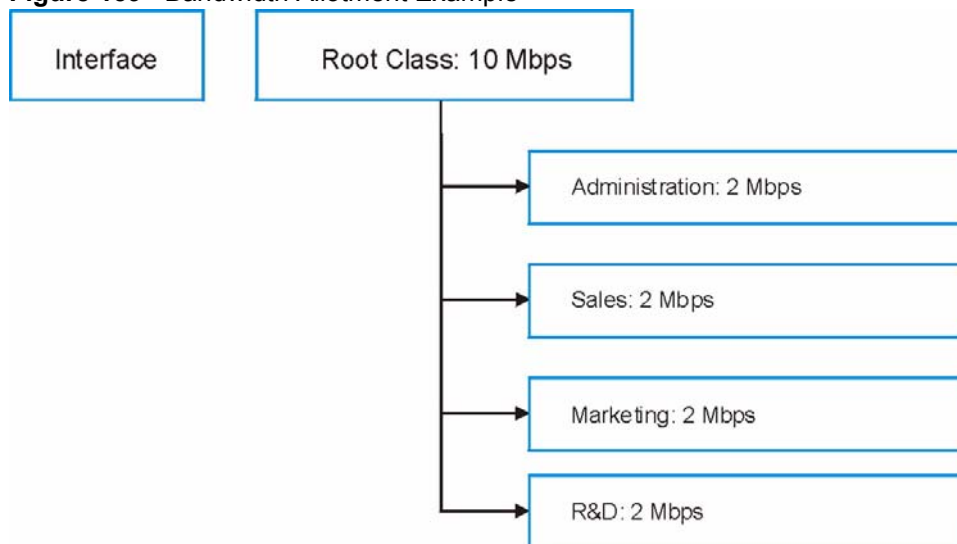
The following figure shows the bandwidth usage with the maximize bandwidth usage option enabled. The ZyWALL divides up the unbudgeted 2 Mbps among the classes that require more bandwidth. If the administration department only uses 1 Mbps of the budgeted 2 Mbps, the ZyWALL also divides the remaining 1 Mbps among the classes that require more bandwidth. Therefore, the ZyWALL divides a total of 3 Mbps total of unbudgeted and unused bandwidth among the classes that require more bandwidth.

In this case, suppose that all of the classes except for the administration class need more bandwidth.

- Each class gets up to its budgeted bandwidth. The administration class only uses 1 Mbps of its budgeted 2 Mbps.
- Sales and Marketing are first to get extra bandwidth because they have the highest priority (6). If they each require 1.5 Mbps or more of extra bandwidth, the ZyWALL divides the total 3 Mbps total of unbudgeted and unused bandwidth equally between the sales and marketing departments (1.5 Mbps extra to each for a total of 3.5 Mbps for each) because they both have the highest priority level.
- R&D requires more bandwidth but only gets its budgeted 2 Mbps because all of the unbudgeted and unused bandwidth goes to the higher priority sales and marketing classes.
- The ZyWALL does not send any traffic that is not defined in the bandwidth filters because all of the unbudgeted bandwidth goes to the classes that need it.

Figure 160 Maximize Bandwidth Usage Example
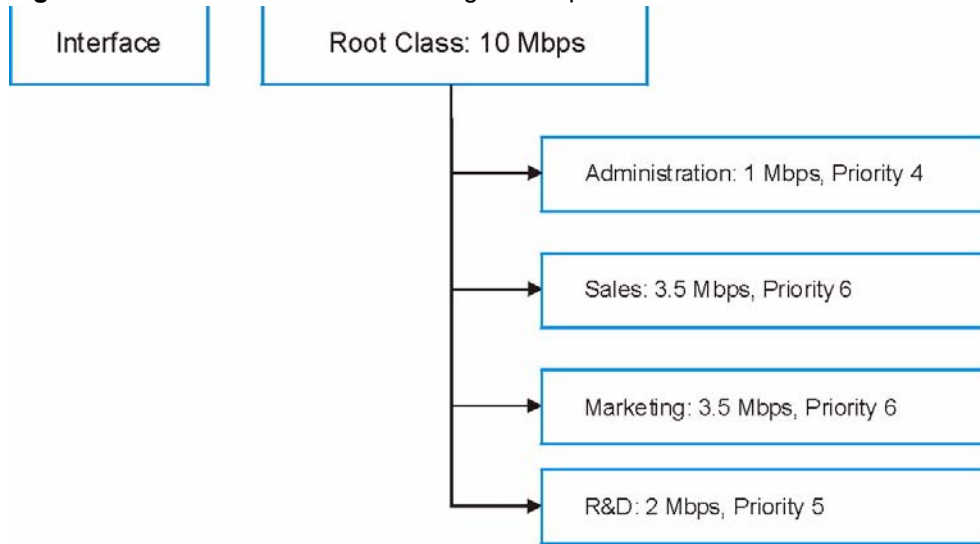
19.7 Bandwidth Borrowing

Bandwidth borrowing allows a sub-class to borrow unused bandwidth from its parent class, whereas maximize bandwidth usage allows bandwidth classes to borrow any unused or unbudgeted bandwidth on the whole interface.

Enable bandwidth borrowing on a sub-class to allow the sub-class to use its parent class's unused bandwidth. A parent class's unused bandwidth is given to the highest priority sub-class first. The sub-class can also borrow bandwidth from a higher parent class (grandparent class) if the sub-class's parent class is also configured to borrow bandwidth from its parent class. This can go on for as many levels as are configured to borrow bandwidth from their parent class (see the Bandwidth Borrowing Example section).

The total of the bandwidth allotments for sub-classes cannot exceed the bandwidth allotment of their parent class. The ZyWALL uses the scheduler to divide a parent class's unused bandwidth among the sub-classes.

19.7.1 Bandwidth Borrowing Example

Here is an example of bandwidth management with classes configured for bandwidth borrowing. The classes are set up based on departments and individuals within certain departments.

Figure 161 Bandwidth Borrowing Example
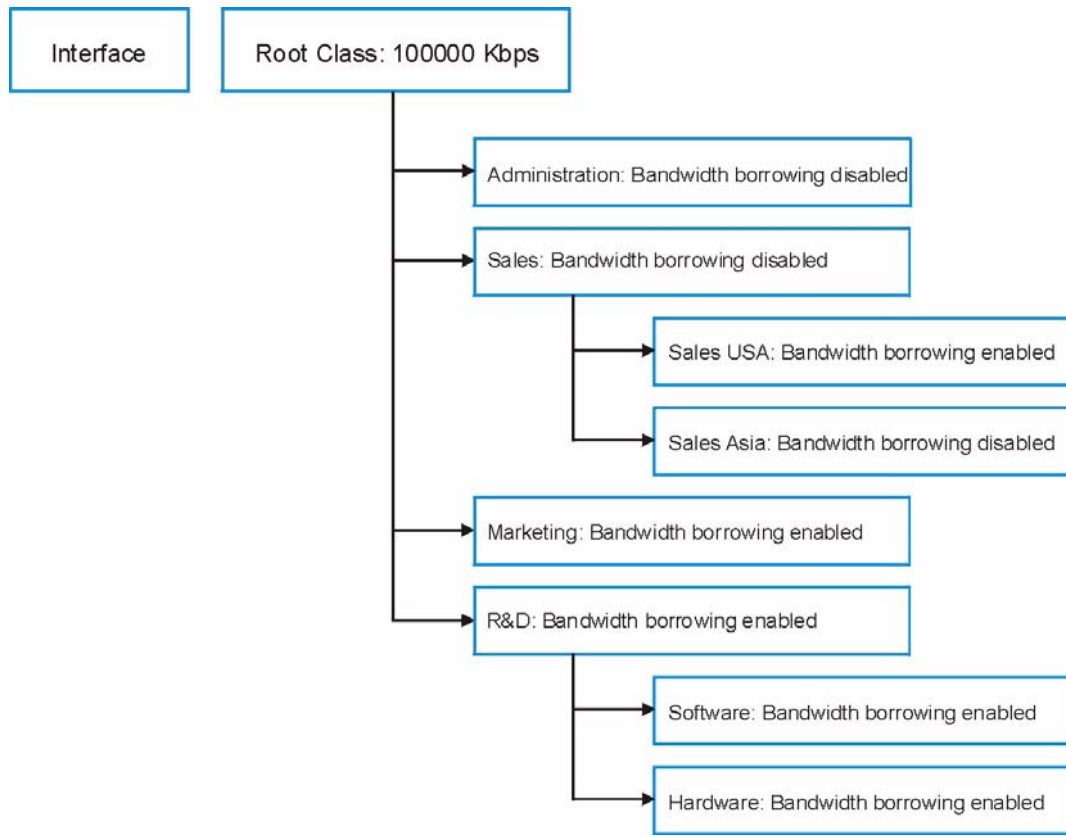
- The Sales USA class can borrow unused bandwidth from the Sales class because the Sales USA class has bandwidth borrowing enabled.
- The Sales USA class cannot borrow unused bandwidth from the Root class because the Sales class has bandwidth borrowing disabled.
- The Sales Asia class cannot borrow unused bandwidth from the Sales class because the Sales Asia class has bandwidth borrowing disabled.
- The R&D Software and Hardware classes can both borrow unused bandwidth from the R&D class because the R&D Software and Hardware classes both have bandwidth borrowing enabled.
- The R&D Software and Hardware classes can also borrow unused bandwidth from the Root class because the R&D class also has bandwidth borrowing enabled.

19.7.2 Maximize Bandwidth Usage With Bandwidth Borrowing

If you configure both maximize bandwidth usage (on the interface) and bandwidth borrowing (on individual sub-classes), the ZyWALL functions as follows.

1 The ZyWALL sends traffic according to each bandwidth class's bandwidth budget.

2 The ZyWALL assigns a parent class's unused bandwidth to its sub-classes that have more traffic than their budgets and have bandwidth borrowing enabled. The ZyWALL gives priority to bandwidth sub-classes of higher priority and treats bandwidth classes of the same priority equally.

3 The ZyWALL assigns any remaining unused or unbudgeted bandwidth on the interface to any bandwidth class that requires it. The ZyWALL gives priority to bandwidth classes of higher priority and treats bandwidth classes of the same level equally.

4 The ZyWALL assigns any remaining unbudgeted bandwidth to traffic that does not match any of the bandwidth classes.

19.8 Configuring Summary

Click **BW MGMT** to open the **Summary** screen.

Enable bandwidth management on an interface and set the maximum allowed bandwidth for that interface.

Figure 162 Bandwidth Manager: Summary

The following table describes the labels in this screen.

Table 109 Bandwidth Manager: Summary

LABEL	DESCRIPTION
WAN1 WAN2 LAN DMZ	These read-only labels represent the physical interfaces. Select an interface's check box to enable bandwidth management on that interface. Bandwidth management applies to all traffic flowing out of the router through the interface, regardless of the traffic's source. Traffic redirect or IP alias may cause LAN-to-LAN or DMZ-to-DMZ traffic to pass through the ZyWALL and be managed by bandwidth management.
Active	Select an interface's check box to enable bandwidth management on that interface.
Speed (kbps)	Enter the amount of bandwidth for this interface that you want to allocate using bandwidth management. This appears as the bandwidth budget of the interface's root class (see the Configuring Class Setup section). The recommendation is to set this speed to match what the device connected to the port can handle. For example, set the WAN interface speed to 1000 kbps if the broadband device connected to the WAN port has an upstream speed of 1000 kbps.

Table 109 Bandwidth Manager: Summary (continued)

LABEL	DESCRIPTION
Scheduler	Select either **Priority-Based** or **Fairness-Based** from the drop-down menu to control the traffic flow. Select **Priority-Based** to give preference to bandwidth classes with higher priorities. Select **Fairness-Based** to treat all bandwidth classes equally. See the Scheduler section.
Maximize Bandwidth Usage	Select this check box to have the ZyWALL divide up all of the interface's unallocated and/or unused bandwidth among the bandwidth classes that require bandwidth. Do not select this if you want to reserve bandwidth for traffic that does not match a bandwidth class (see the Reserving Bandwidth for Non-Bandwidth Class Traffic section) or you want to limit the speed of this interface (see the **Speed** field description).
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

19.9 Configuring Class Setup

The class setup screen displays the configured bandwidth classes by individual interface. Select an interface and click the buttons to perform the actions described next. Click "+" to expand the class tree or click "-" to collapse the class tree. Each interface has a permanent root class. The bandwidth budget of the root class is equal to the speed you configured on the interface (see the Configuring Summary section to configure the speed of the interface). Configure sub-class layers for the root class.

To add or delete child classes on an interface, click **BW MGMT**, then the **Class Setup** tab. The screen appears as shown (with example classes).

The example reserves 15 Mbps of unbudgeted bandwidth for traffic that is not defined in the bandwidth filters (see the Reserving Bandwidth for Non-Bandwidth Class Traffic section). The Administration, Sales USA and Sales Asia bandwidth classes each have bigger bandwidth budgets than the total of the budgets of their sub-classes. The sub-classes can borrow the extra bandwidth as long as they have bandwidth borrowing enabled (see the Bandwidth Borrowing section).

Figure 163 Bandwidth Manager: Class Setup
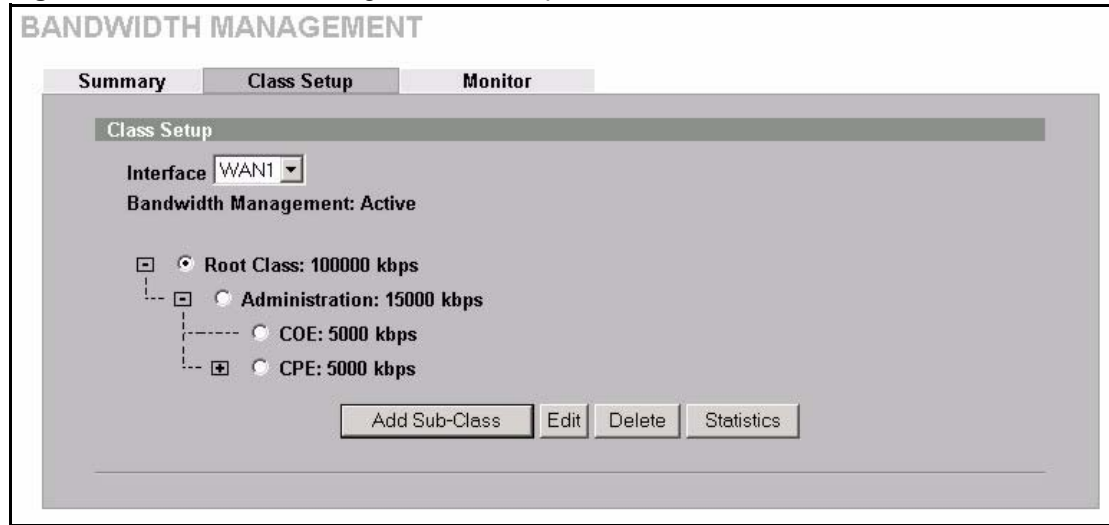
The following table describes the labels in this screen.

Table 110 Bandwidth Manager: Class Setup

LABEL	DESCRIPTION
Interface	Select an interface from the drop-down list box for which you wish to set up classes.
Bandwidth Management	This field displays whether bandwidth management on the interface you selected in the field above is enabled (**Active**) or not (**Inactive**).
Add Sub-Class	Click **Add Sub-class** to add a sub-class.
Edit	Click **Edit** to configure the selected class. You cannot edit the root class.
Delete	Click **Delete** to delete the class and all its sub-classes. You cannot delete the root class.
Statistics	Click **Statistics** to display the status of the selected class.

19.9.1 Bandwidth Manager Class Configuration

Configure a bandwidth management class in the **Class Setup** screen. You must use the **Summary** screen to enable bandwidth management on an interface before you can configure classes for that interface.

To add a child class, click **BW MGMT**, then the **Class Setup** tab. Click the **Add Sub-Class** button to open the following screen.

Figure 164 Bandwidth Manager: Edit Class

The following table describes the labels in this screen.

Table 111 Bandwidth Manager: Edit Class

LABEL	DESCRIPTION
Class Configuration	
Class Name	Use the auto-generated name or enter a descriptive name of up to 20 alphanumeric characters, including spaces.
Bandwidth Budget (kbps)	Specify the maximum bandwidth allowed for the class in kbps. The recommendation is a setting between 20 kbps and 20000 kbps for an individual class.
Priority	Enter a number between 0 and 7 to set the priority of this class. The higher the number, the higher the priority. The default setting is 3.
Borrow bandwidth from parent class	Select this option to allow a sub-class to borrow bandwidth from its parent class if the parent class is not using up its bandwidth budget. Bandwidth borrowing is governed by the priority of the sub-classes. That is, a sub-class with the highest priority (7) is the first to borrow bandwidth from its parent class. Do not select this for the classes directly below the root class if you want to leave bandwidth available for other traffic types (see the Reserving Bandwidth for Non-Bandwidth Class Traffic section) or you want to set the interface's speed to match what the next device in network can handle (see the **Speed** field description in Table 109).
Filter Configuration	

Table 111 Bandwidth Manager: Edit Class (continued)

LABEL	DESCRIPTION
Enable Bandwidth Filter	Select **Enable Bandwidth Filter** to have the ZyWALL use this bandwidth filter when it performs bandwidth management. You must enter a value in at least one of the following fields (other than the **Subnet Mask** fields which are only available when you enter the destination or source IP address).
Service	This field simplifies bandwidth class configuration by allowing you to select a predefined application. When you select a predefined application, you do not configure the rest of the bandwidth filter fields (other than the **Enable Bandwidth Filter** check box). **FTP** (File Transfer Program) is a program to enable fast transfer of files, including large files that may not be possible by e-mail. Select FTP from the drop-down list box to configure the bandwidth filter for FTP traffic. **H.323** is a protocol standard used for multimedia communications over networks, for example NetMeeting. Select H.323 from the drop-down list box to configure the bandwidth filter for H.323 traffic. **SIP** (Session Initiation Protocol) is a signaling protocol used in Internet telephony, instant messaging, events notification and conferencing. The ZyWALL supports SIP traffic pass-through. Select SIP from the drop-down list box to configure this bandwidth filter for SIP traffic. This option makes it easier to manage bandwidth for SIP traffic and is useful for example when there is a VoIP (Voice over Internet Protocol) device on your LAN. Select **Custom** from the drop-down list box if you do not want to use a predefined application for the bandwidth class. When you select **Custom**, you need to configure at least one of the following fields (other than the **Subnet Mask** fields which you only enter if you also enter a corresponding destination or source IP address).
Destination IP Address	Enter the destination IP address in dotted decimal notation.
Destination Subnet Mask	Enter the destination subnet mask. This field is N/A if you do not specify a **Destination IP Address**. Refer to Appendix C IP Subnetting for more information on IP subnetting.
Destination Port	Enter the port number of the destination. See the Predefined Services section in Chapter 10 Firewall Screens for a table of services and port numbers.
Source IP Address	Enter the source IP address.
Source Subnet Mask	Enter the destination subnet mask. This field is N/A if you do not specify a **Source IP Address**. Refer to Appendix C IP Subnetting for more information on IP subnetting.
Source Port	Enter the port number of the source. See the following table for some common services and port numbers.
Protocol ID	Enter the protocol ID (service type) number, for example: 1 for ICMP, 6 for TCP or 17 for UDP.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving.

Table 112 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

19.9.2 Bandwidth Management Statistics

Use the **Bandwidth Management Statistics** screen to view network performance information. Click the **Statistics** button in the **Class Setup** screen to open the **Statistics** screen.

Figure 165 Bandwidth Management Statistics

The following table describes the labels in this screen.

Table 113 Bandwidth Management Statistics

LABEL	DESCRIPTION
Class Name	This field displays the name of the class the statistics page is showing.
Budget (kbps)	This field displays the amount of bandwidth allocated to the class.
Tx Packets	This field displays the total number of packets transmitted.
Tx Bytes	This field displays the total number of bytes transmitted.

Table 113 Bandwidth Management Statistics (continued)

LABEL	DESCRIPTION
Dropped Packets	This field displays the total number of packets dropped.
Dropped Bytes	This field displays the total number of bytes dropped.
Bandwidth Statistics for the Past 8 Seconds (t-8 to t-1)	
This field displays the bandwidth statistics (in bps) for the past one to eight seconds. For example, t-1 means one second ago.	
Update Period (Seconds)	Enter the time interval in seconds to define how often the information should be refreshed.
Set Interval	Click **Set Interval** to apply the new update period you entered in the **Update Period** field above.
Stop Update	Click **Stop Update** to stop the browser from refreshing bandwidth management statistics.
Clear Counter	Click **Clear Counter** to clear all of the bandwidth management statistics.

19.10 Configuring Monitor

To view the device's bandwidth usage and allotments, click **BW MGMT**, then the **Monitor** tab. The screen appears as shown.

Figure 166 Bandwidth Manager Monitor
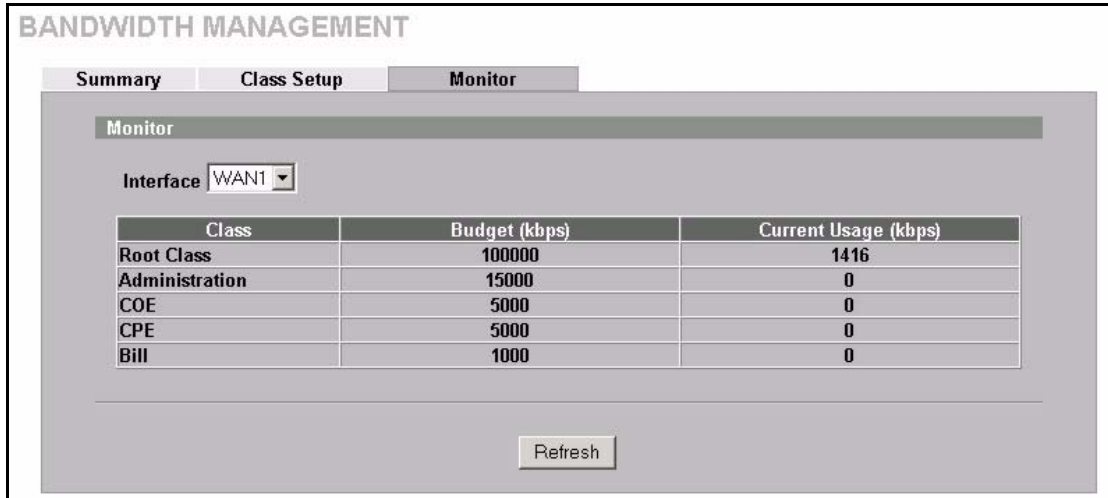
The following table describes the labels in this screen.

Table 114 Bandwidth Manager Monitor

LABEL	DESCRIPTION
Interface	Select an interface from the drop-down list box to view the bandwidth usage of its bandwidth classes.
Class	This field displays the name of the class.

Table 114 Bandwidth Manager Monitor

LABEL	DESCRIPTION
Budget (kbps)	This field displays the amount of bandwidth allocated to the class.
Current Usage (kbps)	This field displays the amount of bandwidth that each class is using.
Refresh	Click **Refresh** to update the page.

Chapter 19 Bandwidth Management

C HAPTER 20
DNS

This chapter shows you how to configure the DNS screens.

20.1 DNS Overview

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it. The ZyWALL uses a system DNS server (in the order you specify in the **DNS System** screen) to resolve domain names, for example, VPN, DDNS and the time server.

20.2 DNS Server Address Assignment

The ZyWALL can get the DNS server addresses in the following ways.

1 The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, manually enter them in the DNS server fields.

2 If your ISP dynamically assigns the DNS server IP addresses (along with the ZyWALL's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.

3 You can manually enter the IP addresses of other DNS servers. These servers can be public or private. A DNS server could even be behind a remote IPSec router (see the Private DNS Server section).

20.3 DNS Servers

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

3 Use the **REMOTE MGMT DNS** screen to configure the ZyWALL (in router mode) to accept or discard DNS queries.

20.4 Address Record

An address record contains the mapping of a fully qualified domain name (FQDN) to an IP address. An FQDN consists of a host and domain name and includes the top-level domain. For example, www.zyxel.com.tw is a fully qualified domain name, where "www" is the host, "zyxel" is the second-level domain, and "com.tw" is the top level domain. mail.myZyXEL.com.tw is also a FQDN, where "mail" is the host, "myZyXEL" is the second-level domain, and "com.tw" is the top level domain.

The ZyWALL allows you to configure address records about the ZyWALL itself or another device. This way you can keep a record of DNS names and addresses that people on your network may use frequently. If the ZyWALL receives a DNS query for an FQDN for which the ZyWALL has an address record, the ZyWALL can send the IP address in a DNS response without having to query a DNS name server.

20.5 Name Server Record

A name server record contains a DNS server's IP address. The ZyWALL can query the DNS server to resolve domain names for features like VPN, DDNS and the time server. A domain zone may also be included. A domain zone is a fully qualified domain name without the host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name.

20.5.1 Private DNS Server

In cases where you want to use domain names to access Intranet servers on a remote private network that has a DNS server, you must identify that DNS server. You cannot use DNS servers on the LAN or from the ISP since these DNS servers cannot resolve domain names to private IP addresses on the remote private network.

The following figure depicts an example where three VPN tunnels are created from ZyWALL A; one to branch office **2**, one to branch office **3** and another to headquarters (**HQ**). In order to access computers that use private domain names on the **HQ** network, the ZyWALL at branch office **1** uses the Intranet DNS server in headquarters.

Figure 167 Private DNS Server Example
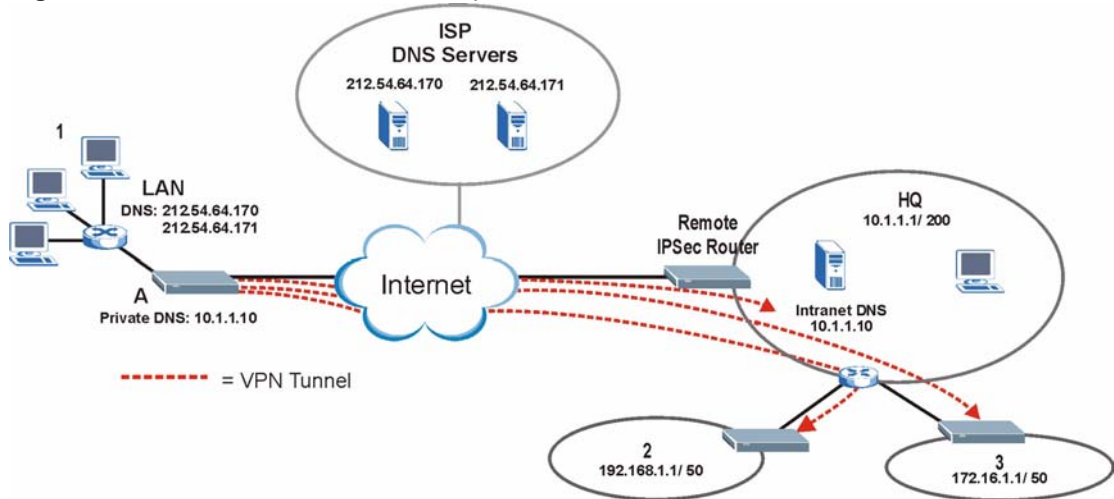
> **Note:** If you do not specify an Intranet DNS server on the remote network, then the VPN host must use IP addresses to access the computers on the remote private network.

20.6 The System Screen

To configure your ZyWALL's DNS address and name server records, click **DNS**. The screen appears as shown.

Figure 168 System
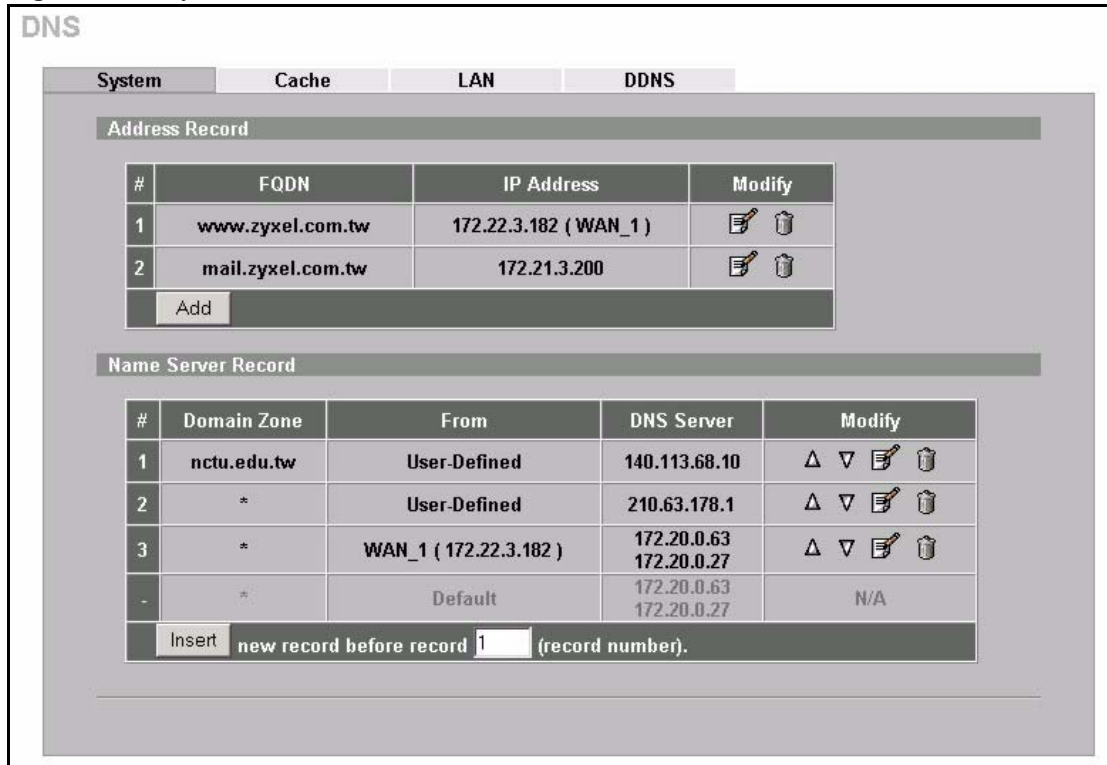
The following table describes the labels in this screen.

Table 115 System

LABEL	DESCRIPTION
Address Record	An address record specifies the mapping of a fully qualified domain name (FQDN) to an IP address. An FQDN consists of a host and domain name and includes the top-level domain. For example, www.zyxel.com.tw is a fully qualified domain name, where "www" is the host, "zyxel" is the second-level domain, and "com.tw" is the top level domain.
#	This is the index number of the address record.
FQDN	This is a host's fully qualified domain name.
IP Address	This is the IP address of a host.
Modify	Click the edit icon to go to the screen where you can edit the record.
	Click the delete icon to remove an existing record. A window display asking you to confirm that you want to delete the record. Note that subsequent records move up by one when you take this action.
Add	Click **Add** to open a screen where you can add a new address record. Refer to Table 116 for information on the fields.
Name Server Record	A name server record contains a DNS server's IP address. The ZyWALL can query the DNS server to resolve domain names for features like VPN, DDNS and the time server.
	When the ZyWALL needs to resolve a domain name, it checks it against the name server record entries in the order that they appear in this list.
	A "*" indicates a name server record without a domain zone. The default record is grayed out. The ZyWALL uses this default record if the domain name that needs to be resolved does not match any of the other name server records.

Table 115 System

LABEL	DESCRIPTION
#	This is the index number of the name server record.
Domain Zone	A domain zone is a fully qualified domain name without the host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name.
From	This field displays whether the IP address of a DNS server is from a WAN interface (and which it is) or specified by the user.
DNS Server	This is the IP address of a DNS server.
Modify	Click a triangle icon to move the record up or down in the list.
	Click the edit icon to go to the screen where you can edit the record.
	Click the delete icon to remove an existing record. A window display asking you to confirm that you want to delete the record. Note that subsequent records move up by one when you take this action.
Insert	Click **Insert** to open a screen where you can insert a new name server record. Refer to Table 117 for information on the fields.

20.6.1 Adding an Address Record

Click **Add** in the **System** screen to add an address record.

Figure 169   System: Add

The following table describes the labels in this screen.

Table 116   System: Add

LABEL	DESCRIPTION
FQDN	Type a fully qualified domain name (FQDN) of a server. An FQDN starts with a host name and continues all the way up to the top-level domain name. For example, www.zyxel.com.tw is a fully qualified domain name, where "www" is the host, "zyxel" is the second-level domain, and "com.tw" is the top level domain.
IP Address	If this entry is for one of the WAN ports, select **WAN Interface** and select WAN 1 or WAN 2 from the drop-down list box.
	For entries that are not for one of the WAN ports, select **Custom** and enter the IP address of the host in dotted decimal notation.

Table 116   System: Add

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

20.6.2 Inserting a Name Server record

Click **Insert** in the **System** screen to insert a name server record.

Figure 170   System: Insert

The following table describes the labels in this screen.

Table 117 System: Insert

LABEL	DESCRIPTION
Domain Zone	This field is optional.
	A domain zone is a fully qualified domain name without the host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name. For example, whenever the ZyWALL receives needs to resolve a zyxel.com.tw domain name, it can send a query to the recorded name server IP address.
	Leave this field blank if all domain zones are served by the specified DNS server(s).
DNS Server	Select the **DNS Server(s) from ISP** radio button if your ISP dynamically assigns DNS server information. The fields below display the (read-only) DNS server IP address(es) that the ISP assigns. **N/A** displays for any DNS server IP address fields for which the ISP does not assign an IP address. **N/A** displays for all of the DNS server IP address fields if the ZyWALL has a fixed WAN IP address.
	Select **Public DNS Server** if you have the IP address of a DNS server. The IP address must be public or a private address on your local LAN. Enter the DNS server's IP address in the field to the right.
	Public DNS Server entries with the IP address set to 0.0.0.0 are not allowed.
	Select **Private DNS Server** if the DNS server has a private IP address and is located behind a VPN peer. Enter the DNS server's IP address in the field to the right.
	With a private DNS server, you must also configure the first DNS server entry in the **DNS LAN** screen to use **DNS Relay**.
	You must also configure a VPN rule since the ZyWALL uses a VPN tunnel when it relays DNS queries to the private DNS server. The rule must include the LAN IP address of the ZyWALL as a local IP address and the IP address of the DNS server as a remote IP address.
	Private DNS Server entries with the IP address set to 0.0.0.0 are not allowed.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Cancel	Click **Cancel** to exit this screen without saving.

20.7 DNS Cache

DNS cache is the temporary storage area where a router stores responses from DNS servers. When the ZyWALL receives a positive or negative response for a DNS query, it records the response in the DNS cache. A positive response means that the ZyWALL received the IP address for a domain name that it checked with a DNS server within the five second DNS timeout period. A negative response means that the ZyWALL did not receive a response for a query it sent to a DNS server within the five second DNS timeout period.

When the ZyWALL receives DNS queries, it compares them against the DNS cache before querying a DNS server. If the DNS query matches a positive entry, the ZyWALL responses with the IP address from the entry. If the DNS query matches a negative entry, the ZyWALL replies that the DNS query failed.

20.8 Configure DNS Cache

To configure your ZyWALL's DNS caching, click **DNS**, then the **Cache** tab. The screen appears as shown.

Figure 171   Cache

The following table describes the labels in this screen.

Table 118   Cache

LABEL	DESCRIPTION
DNS Cache Setup	
Cache Positive DNS Resolutions	Select the check box to record the positive DNS resolutions in the cache. Caching positive DNS resolutions helps speed up the ZyWALL's processing of commonly queried domain names and reduces the amount of traffic that the ZyWALL sends out to the WAN.
Maximum TTL	Type the maximum time to live (TTL) (60 to 3600 seconds). This sets how long the ZyWALL is to allow a positive resolution entry to remain in the DNS cache before discarding it.
Cache Negative DNS Resolutions	Caching negative DNS resolutions helps speed up the ZyWALL's processing of commonly queried domain names (for which DNS resolution has failed) and reduces the amount of traffic that the ZyWALL sends out to the WAN.
Negative Cache Period	Type the time (60 to 3600 seconds) that the ZyWALL is to allow a negative resolution entry to remain in the DNS cache before discarding it.
Apply	Click **Apply** to save your changes back to the ZyWALL.

Table 118 Cache

LABEL	DESCRIPTION
Reset	Click **Reset** to begin configuring this screen afresh.
DNS Cache Entry	
Flush	Click this button to clear the cache manually. After you flush the cache, the ZyWALL must query the DNS servers again for any domain names that had been previously resolved.
Refresh	Click this button to reload the cache.
#	This is the index number of a record.
Cache Type	This displays whether the response for the DNS request is positive or negative.
Domain Name	This is the domain name of a host.
IP Address	This is the (resolved) IP address of a host. This field displays **0.0.0.0** for negative DNS resolution entries.
Remaining Time (sec)	This is the number of seconds left before the DNS resolution entry is discarded from the cache.
Modify	Click the delete icon to remove the DNS resolution entry from the cache.

20.9 Configuring LAN DNS

Click **DNS** and then the **LAN** tab to open the **LAN DNS** screen shown next. Use this screen to configure the DNS server information that the ZyWALL sends to its LAN DHCP clients.

Figure 172 LAN DNS

The following table describes the labels in this screen.

Table 119 LAN

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 clients. The ZyWALL only passes this information to the LAN DHCP clients 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 clients 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.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

20.10 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.

20.10.1 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.

20.10.2 High Availability

A DNS server maps a domain name to a port's IP address. If that WAN port loses its connection, high availability allows the router to substitute another port's IP address for the domain name mapping.

20.11 Configuring Dynamic DNS

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

Figure 173 DDNS

The following table describes the labels in this screen.

Table 120 DDNS

LABEL	DESCRIPTION
Account Setup	
Active	Select this check box to use dynamic DNS.
Service Provider	This is the name of your Dynamic DNS service provider.
Username	Enter your user name. You can use up to 31 alphanumeric characters (and the underscore). Spaces are not allowed.
Password	Enter the password associated with the user name above. You can use up to 31 alphanumeric characters (and the underscore). Spaces are not allowed.
My Domain Names	
Domain Name 1~5	Enter the host names in these fields.
DDNS Type	Select the type of service that you are registered for from your Dynamic DNS service provider. Select **Dynamic** if you have the Dynamic DNS service. Select **Static** if you have the Static DNS service. Select **Custom** if you have the Custom DNS service.
Offline	This option is available when **Custom** is selected in the **DDNS Type** field. Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line.
Wildcard	Select the check box to enable DYNDNS Wildcard.
WAN Interface	Select the WAN port to use for updating the IP address of the domain name.
IP Address Update Policy	Select **Use WAN IP Address** to have the ZyWALL update the domain name with the WAN port's IP address. Select **Use User-Defined** and enter the IP address if you have a static IP address. Select **Let DDNS Server Auto Detect** only when there are one or more NAT routers between the ZyWALL and the DDNS server. This feature has the DDNS server automatically detect and use the IP address of the NAT router that has a public IP address. **Note:** The DDNS server may not be able to detect the proper IP address if there is an HTTP proxy server between the ZyWALL and the DDNS server.
HA	Select this check box to enable the high availability (HA) feature. High availability has the ZyWALL update a domain name with another port's IP address when the normal WAN port does not have a connection. If the WAN port specified in the **WAN Interface** field does not have a connection, the ZyWALL will attempt to use the IP address of another WAN port to update the domain name. When the WAN ports are in the active/passive operating mode, the ZyWALL will update the domain name with the IP address of whichever WAN port has a connection, regardless of the setting in the **WAN Interface** field. Disable this feature and the ZyWALL will only update the domain name with an IP address of the WAN port specified in the **WAN Interface** field. If that WAN port does not have a connection, the ZyWALL will not update the domain name with another port's IP address. **Note:** If you enable high availability, DDNS can also function when the ZyWALL uses the dial backup port. DDNS does not function when the ZyWALL uses traffic redirect.

Table 120   DDNS

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

CHAPTER 21
Remote Management

This chapter provides information on the Remote Management screens.

21.1 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 10 Firewall Screens 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&DMZ)
- DMZ only,

> **Note:** When you choose **WAN only** or **ALL** (LAN & WAN& DMZ), 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 Console port

2 SSH

3 Telnet

4 HTTPS and HTTP

21.1.1 Remote Management Limitations

1 Remote management over LAN or WAN will not work when:

2 A filter in SMT menu 3.1 (LAN) or in menu 11.5 (WAN) 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.

21.1.2 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.

21.1.3 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.

21.2 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 15 Certificates 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 174 HTTPS Implementation
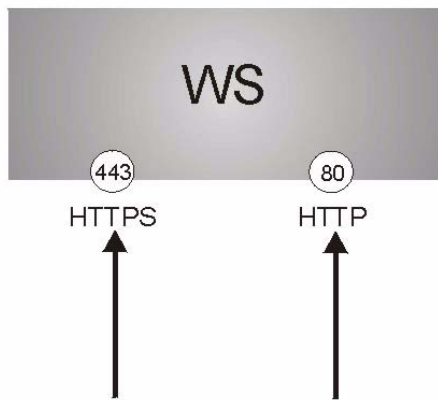
> **Note:** If you disable **HTTP Server Access** (**Disable**) in the **REMOTE MGMT WWW** screen, then the ZyWALL blocks all HTTP connection attempts.

21.3 Configuring WWW

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

Figure 175 WWW

The following table describes the labels in this screen.

Table 121 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 L Importing Certificates 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	

Table 121 WWW (continued)

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 changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

21.4 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.

21.4.1 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 176   Security Alert Dialog Box (Internet Explorer)
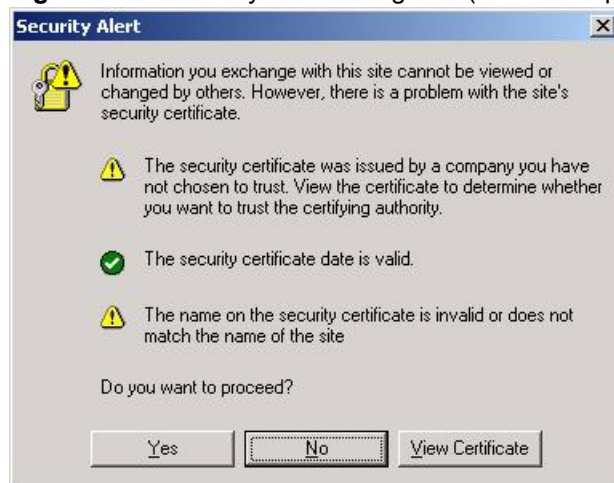
21.4.2 Netscape Navigator Warning Messages

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 ZyWALL's certificate into the SSL client.

Figure 177   Figure 18-4 Security Certificate 1 (Netscape)

Figure 178   Security Certificate 2 (Netscape)

21.4.3 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 L Importing Certificates 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 (see Figure 182 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 192.168.1.1, create a certificate that uses 192.168.1.1 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**.

21.4.4 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 179   Login Screen (Internet Explorer)

Figure 180   Login Screen (Netscape)

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

The factory default certificate is a common default certificate for all ZyWALL models.

Figure 181   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 182   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 183 Common ZyWALL Certificate
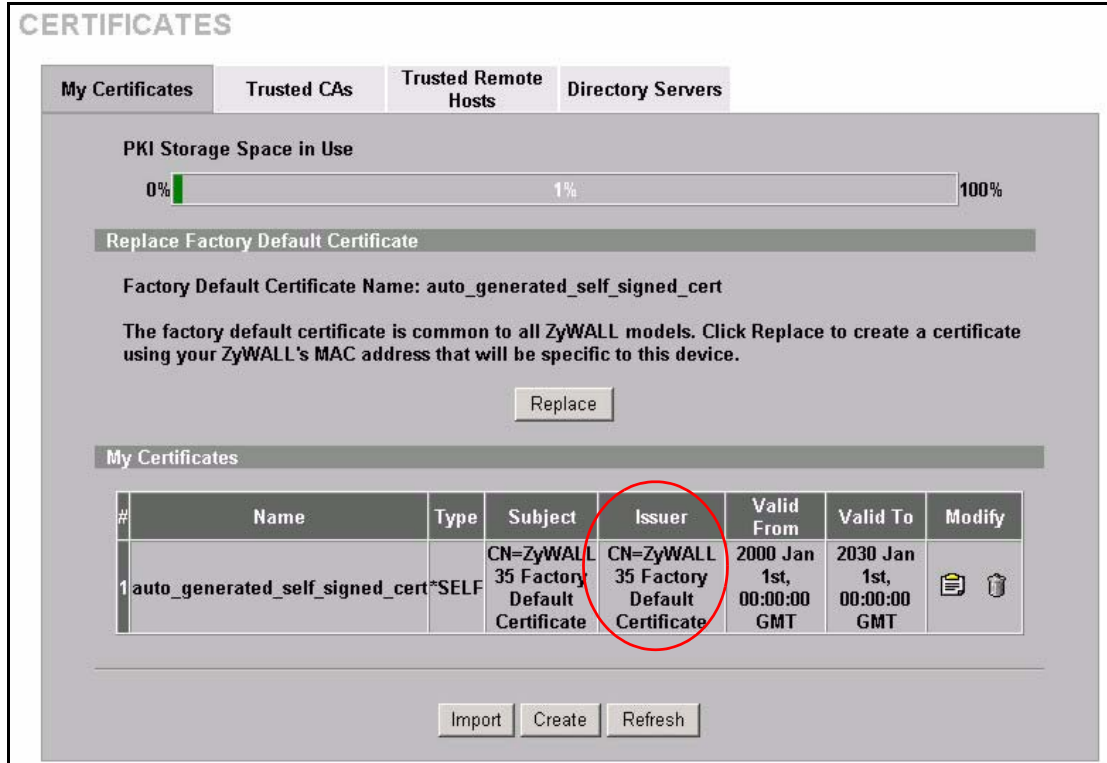
21.5 SSH Overview

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 184 SSH Communication Example

21.6 How SSH works

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

Figure 185 How SSH Works
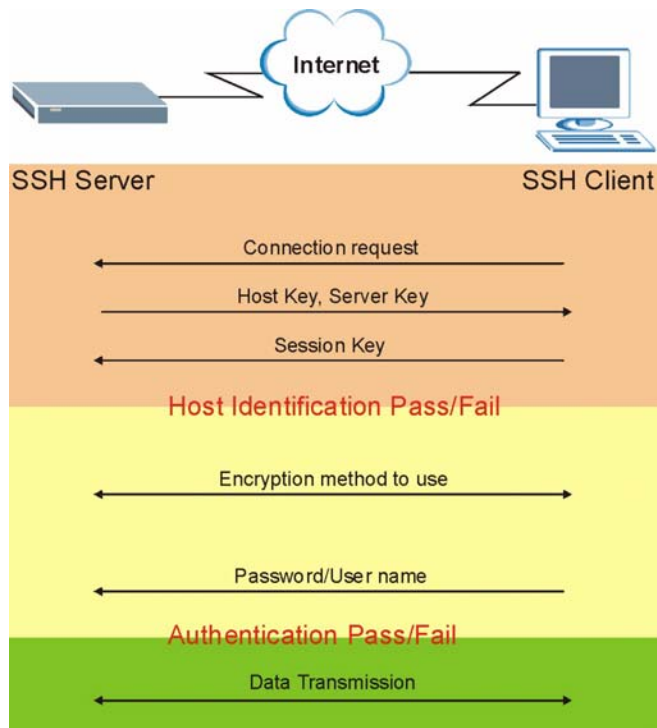
1 **Host Identification**

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.

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

21.7.1 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.

21.8 Configuring SSH

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

Figure 186 SSH

The following table describes the labels in this screen.

Table 122 SSH

LABEL	DESCRIPTION
Server Host Key	Select the certificate whose corresponding private key is to be used to identify the ZyWALL for SSH connections. You must have certificates already configured in the **My Certificates** screen (Click **My Certificates** and see Chapter 15 Certificates 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 changes back to the ZyWALL.
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.

21.9 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.

21.9.1 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 187   SSH Example 1: Store Host Key

Enter the password to log in to the ZyWALL. The SMT main menu displays next.

21.9.2 Example 2: Linux

This section describes how to access the ZyWALL using the OpenSSH client program that comes with most Linux distributions.

1 Test whether the SSH service is available on the ZyWALL.

Enter "`telnet 192.168.1.1 22`" at a terminal prompt and press [ENTER]. The computer attempts to connect to port 22 on the ZyWALL (using the default IP address of 192.168.1.1).

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

Figure 188 SSH Example 2: Test

```
$ telnet 192.168.1.1 22
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.
SSH-1.5-1.0.0
```

2 Enter "`ssh -1 192.168.1.1`". This command forces your computer to connect to the ZyWALL using SSH version 1. If this is the first time you are connecting to the ZyWALL using SSH, a message displays prompting you to save the host information of the ZyWALL. Type "`yes`" and press [ENTER].

Then enter the password to log in to the ZyWALL.

Figure 189 SSH Example 2: Log in

```
$ ssh -1 192.168.1.1
The authenticity of host '192.168.1.1 (192.168.1.1)' can't be
established.
RSA1 key fingerprint is
21:6c:07:25:7e:f4:75:80:ec:af:bd:d4:3d:80:53:d1.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.1' (RSA1) to the list of known
hosts.
Administrator@192.168.1.1's password:
```

3 The SMT main menu displays next.

21.10 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 -1 192.168.1.1`". This command forces your computer to connect to the ZyWALL for secure file transfer using SSH version 1. If this is the first time you are connecting to the ZyWALL using SSH, a message displays prompting you to save the host information of the ZyWALL. Type "`yes`" and press [ENTER].

2 Enter the password to login to the ZyWALL.

3 Use the "`put`" command to upload a new firmware to the ZyWALL.

Figure 190 Secure FTP: Firmware Upload Example

```
$ sftp -1 192.168.1.1
Connecting to 192.168.1.1...
The authenticity of host '192.168.1.1 (192.168.1.1)' can't be
established.
RSA1 key fingerprint is
21:6c:07:25:7e:f4:75:80:ec:af:bd:d4:3d:80:53:d1.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.1' (RSA1) to the list of known
hosts.
Administrator@192.168.1.1's password:
sftp> put firmware.bin ras
Uploading firmware.bin to /ras
Read from remote host 192.168.1.1: Connection reset by peer
Connection closed
$
```

21.11 Telnet

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

Figure 191 Telnet Configuration on a TCP/IP Network
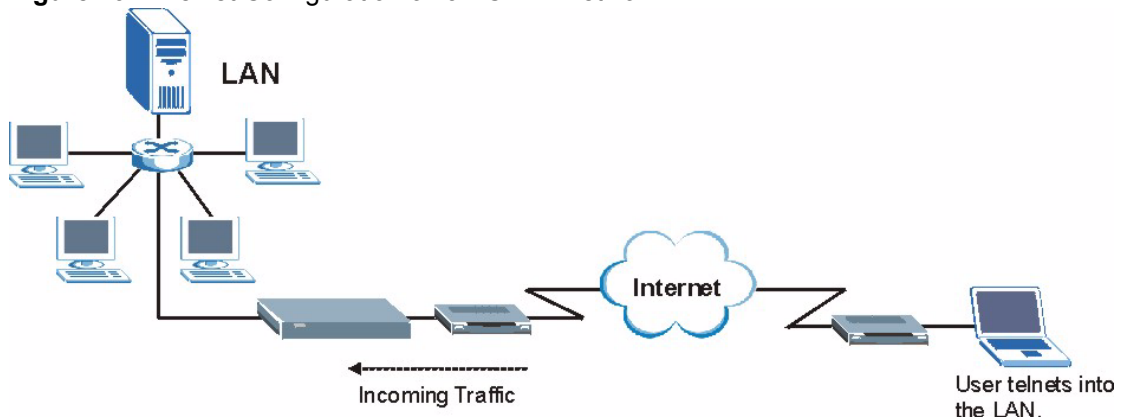
21.12 Configuring TELNET

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

Figure 192 Telnet

The following table describes the labels in this screen.

Table 123 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 changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

21.13 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 193 FTP

The following table describes the labels in this screen.

Table 124 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 changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

21.14 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 194   SNMP Management Model

Managed Device   Managed Device   Managed Device
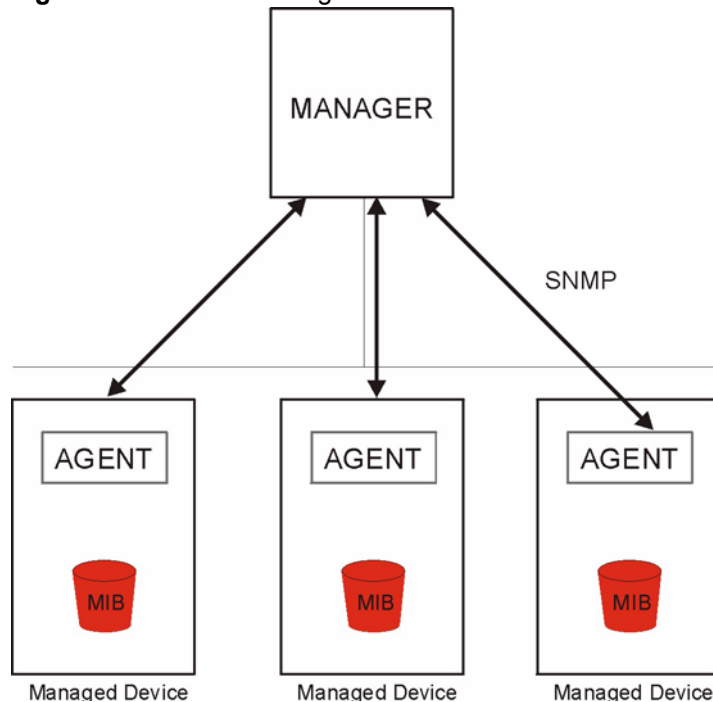
An SNMP managed network consists of two main types of component: agents and a manager.

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.

21.14.1 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.

21.14.2 SNMP Traps

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

Table 125   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.

21.14.3 REMOTE MANAGEMENT: SNMP

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

Figure 195 SNMP

The following table describes the labels in this screen.

Table 126 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 changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

21.15 Configuring DNS

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa. Refer to Chapter 7 WAN Screens 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 196 DNS

The following table describes the labels in this screen.

Table 127 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 changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

21.16 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 ZyXEL devices located worldwide. See the *Vantage CNM User's Guide* for details.

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

21.17 Configuring CNM

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

Figure 197   CNM
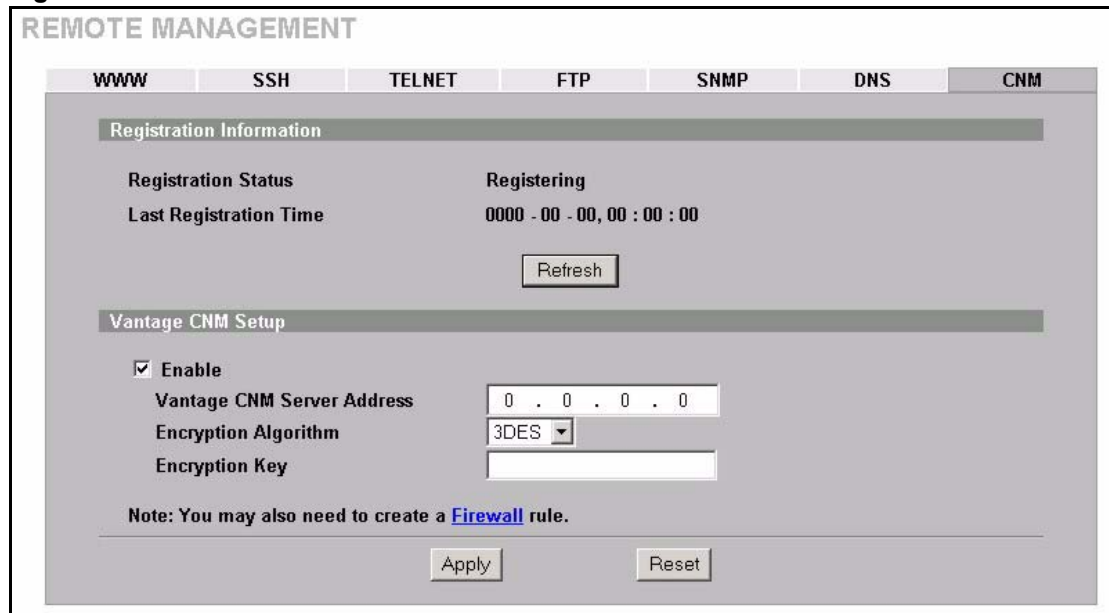
The following table describes the labels in this screen.

Table 128   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. It 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 128 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.

C HAPTER 22
UPnP

This chapter introduces the Universal Plug and Play feature. This chapter is only applicable when the ZyWALL is in router mode.

22.1 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.

22.1.1 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.

22.1.2 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 16 Network Address Translation (NAT) for further information about NAT.

22.1.3 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.

22.2 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.

22.3 Configuring UPnP

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

Figure 198   Configuring UPnP
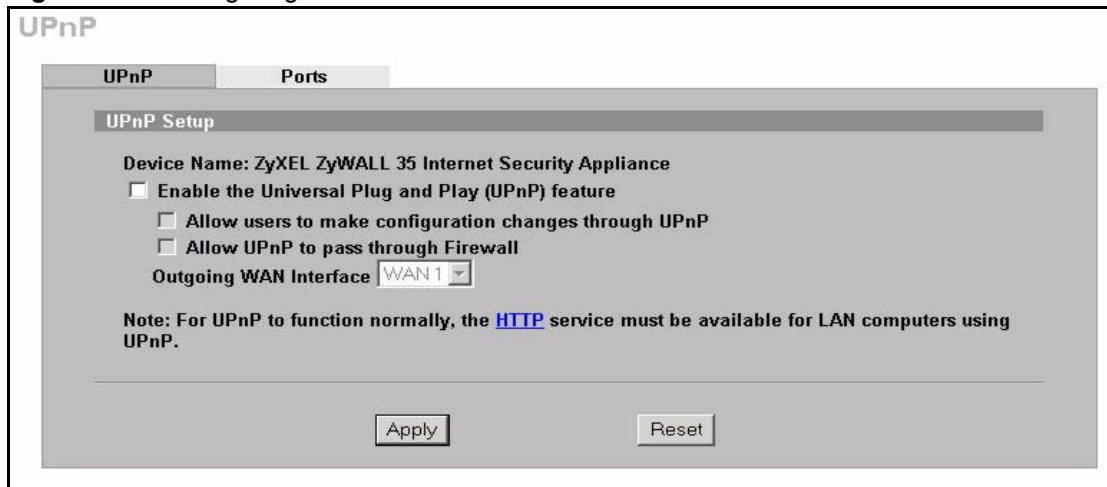
The following table describes the fields in this screen.

Table 129   Configuring UPnP

LABEL	DESCRIPTION
UPnP Setup	
Device Name	This identifies the ZyXEL device in UPnP applications.

Table 129 Configuring UPnP

LABEL	DESCRIPTION
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).
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).
Outgoing WAN Interface	Select through which WAN port you want to send out traffic from UPnP-enabled applications. If the WAN port you select loses its connection, the ZyWALL attempts to use the other WAN port. If the other WAN port also does not work, the ZyWALL drops outgoing packets from UPnP-enabled applications.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

22.4 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 199 UPnP Ports
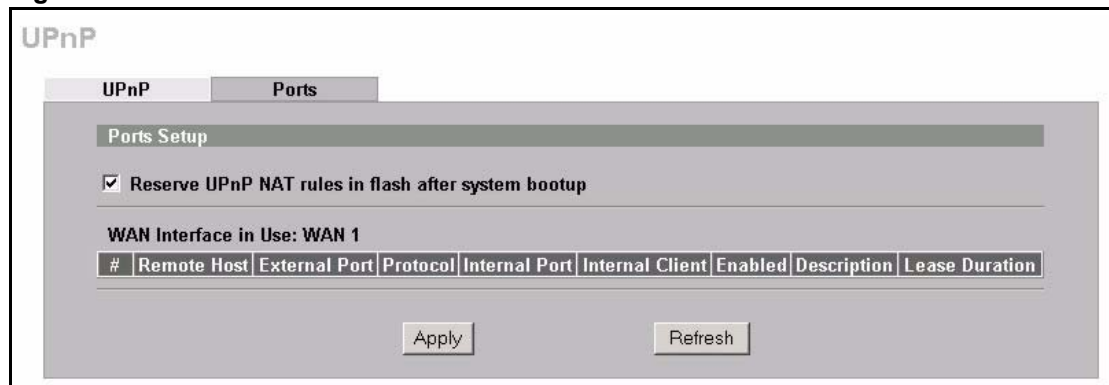
The following table describes the labels in this screen.

Table 130 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.	
#	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.

22.5 Installing UPnP in Windows Example

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

22.5.1 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.
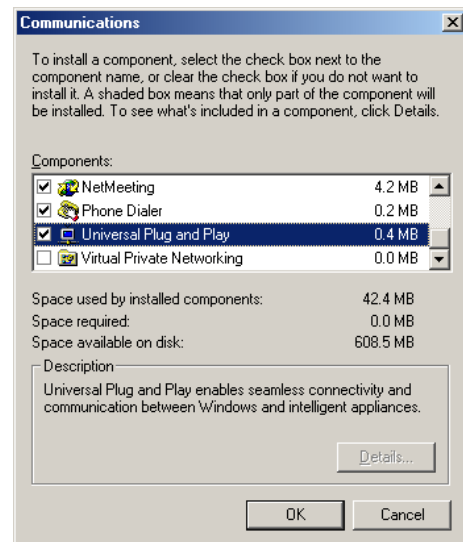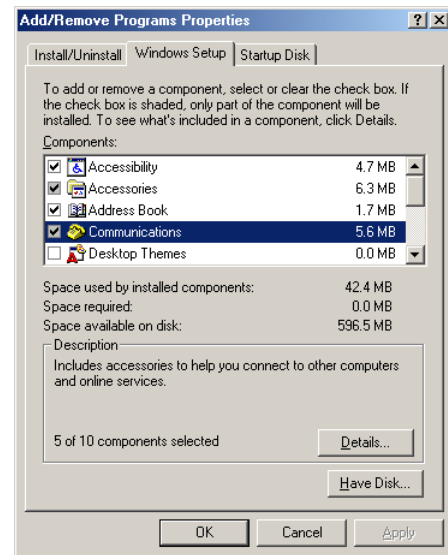
22.5.2 Installing UPnP in Windows XP

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**.
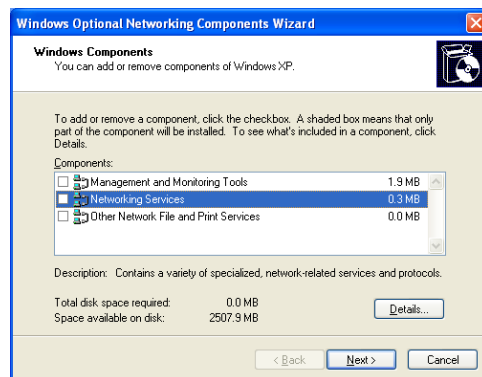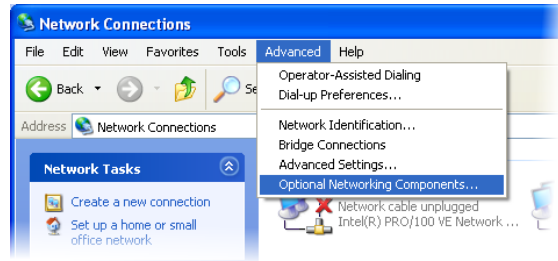
5 In the **Networking Services** window, select the **Universal Plug and Play** check box.

6 Click **OK** to go back to the **Windows Optional Networking Component Wizard** window and click **Next**.
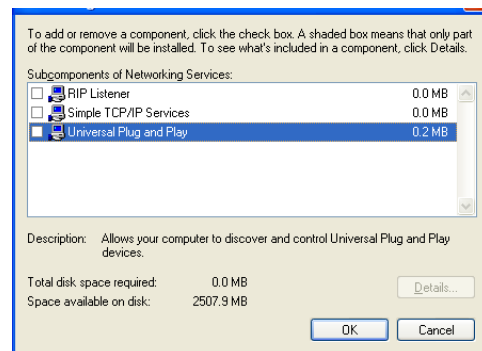
22.6 Using UPnP in Windows XP Example

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.

22.6.1 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**.
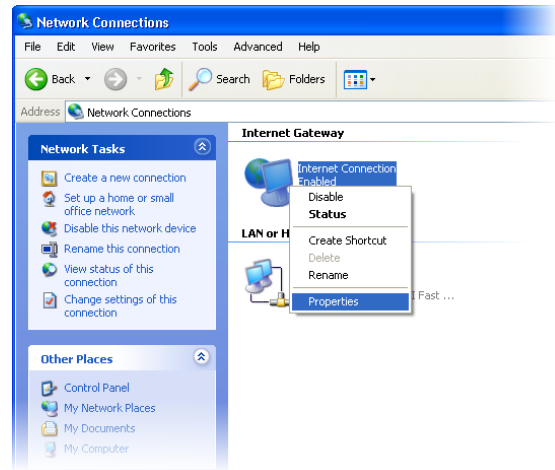
3 In the **Internet Connection Properties** window, click **Settings** to see the port mappings that were automatically created.

You may edit or delete the port mappings or click **Add** to manually add port mappings.
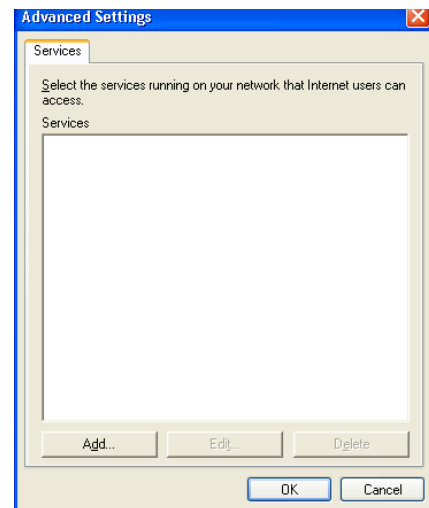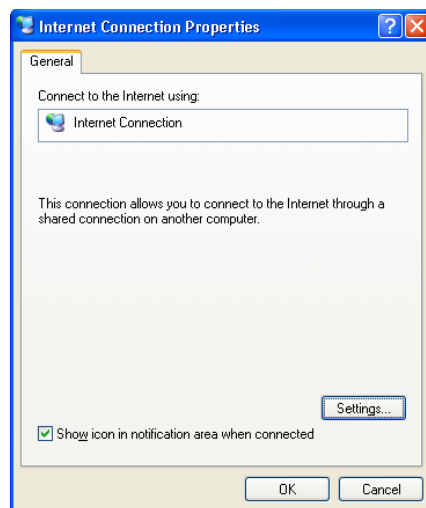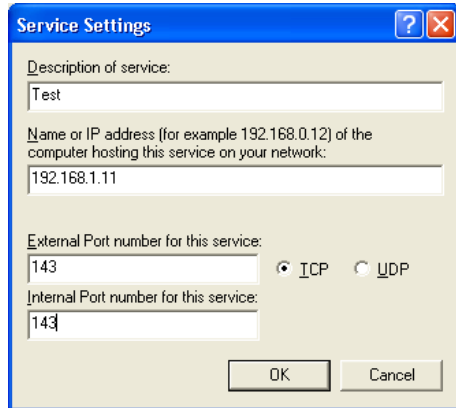
>
>
> **Note:** When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

4 Select the **Show icon in notification area when connected** check box and click **OK**. An icon displays in the system tray.
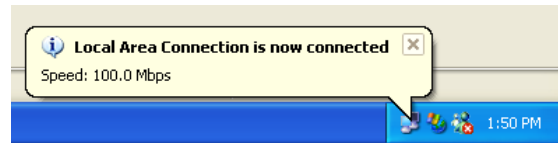
5 Double-click the icon to display your current Internet connection status.
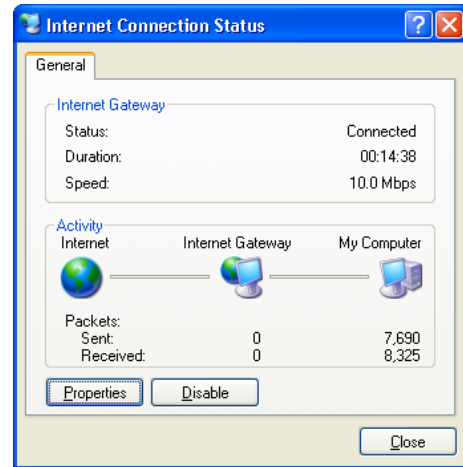
22.6.2 Web Configurator Easy Access

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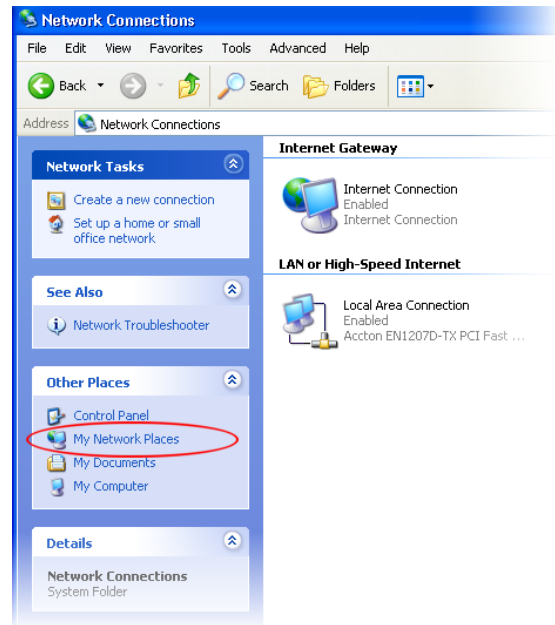
4 An icon with the description for each UPnP-enabled device displays under **Local Network**.

5 Right-click the icon for your ZyXEL device and select **Invoke**. The web configurator login screen displays.
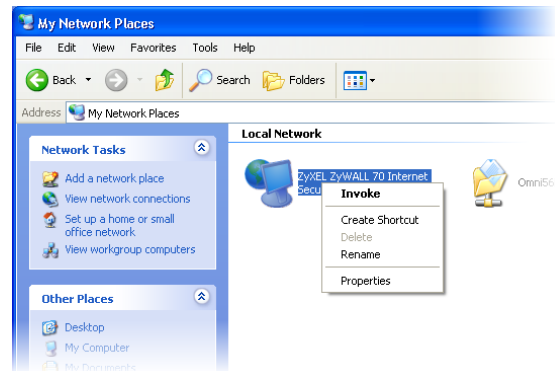
6 Right-click the icon for your ZyXEL device and select **Properties**. A properties window displays with basic information about the ZyXEL device.
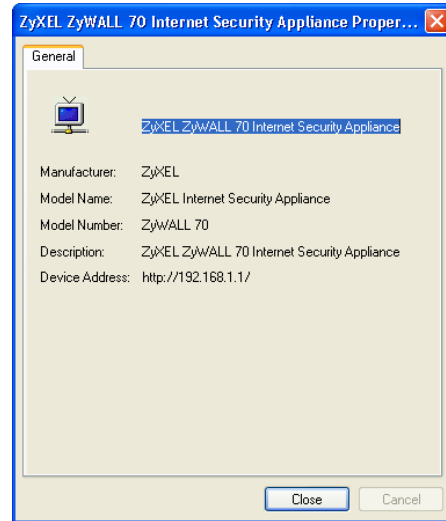
C HAPTER 23
Logs Screens

This chapter contains information about configuring general log settings and viewing the ZyWALL's logs. Refer to Appendix S Log Descriptions for example log message explanations.

23.1 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 the Configuring Log Settings section). 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 200 View Log
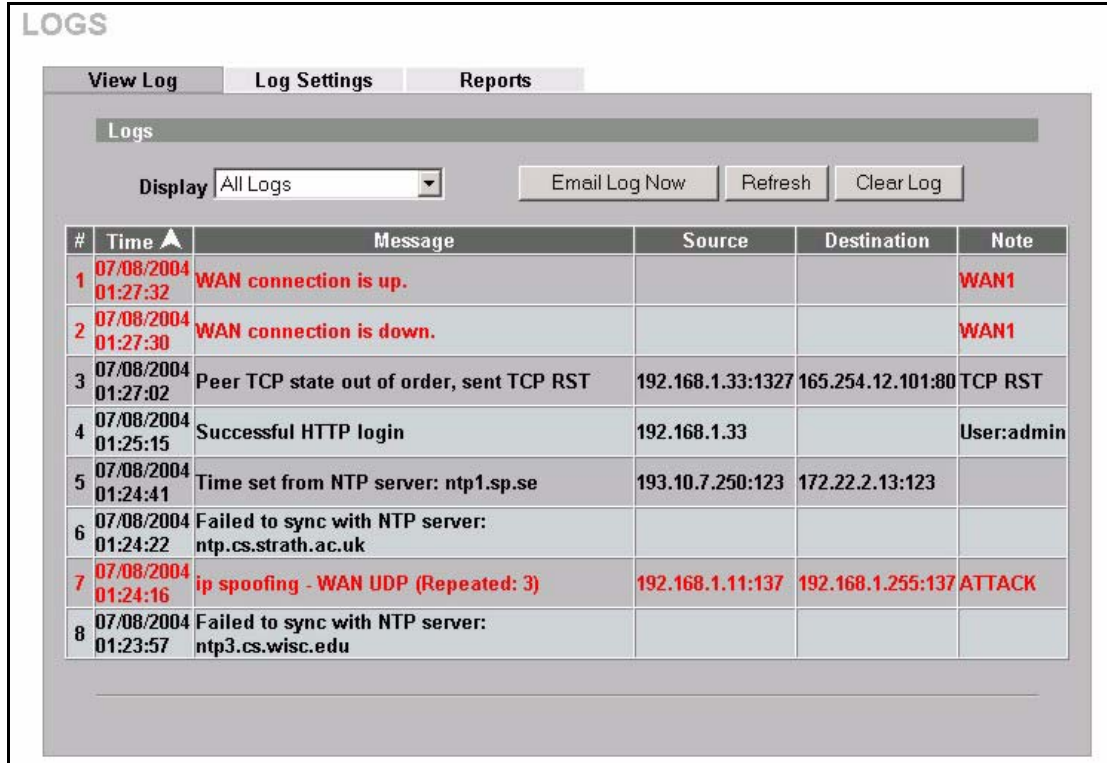
The following table describes the labels in this screen.

Table 131 View Log

LABEL	DESCRIPTION
Display	The categories that you select in the **Log Settings** page (see the Configuring Log Settings section) 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 the Configuring Time and Date section 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 the Configuring Log Settings section).
Refresh	Click **Refresh** to renew the log screen.
Clear Log	Click **Clear Log** to delete all the logs.

23.2 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.

```
#  .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 132   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.
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.

23.3 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 201 Log Settings

The following table describes the labels in this screen.

Table 133 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 menu 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 133 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. You can use the `sys log consolidate msglist` command to see what log messages will be consolidated.
Log Consolidation Period	Specify the time interval during which the ZyWALL merges logs with identical messages into one log.
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

23.4 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 202 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 134 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.
Interface	Select on which interface (**LAN** or **DMZ**) the logs will be collected. The logs on the DMZ or LAN IP alias 1 and 2 are also recorded.
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.

23.4.1 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 203   Web Site Hits Report Example
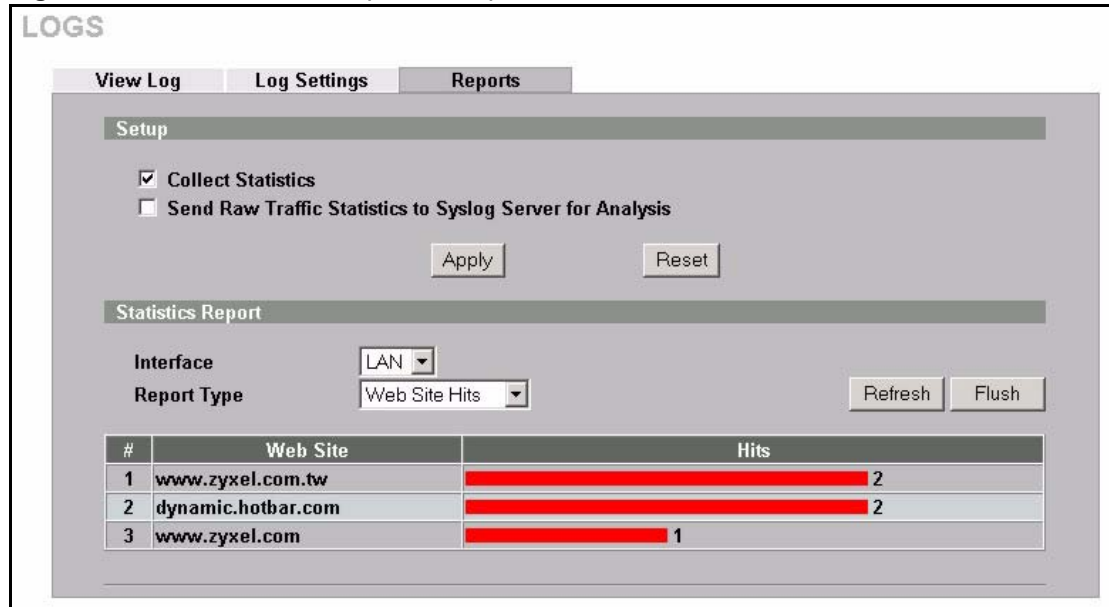
The following table describes the label in this screen.

Table 135   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 138).

23.4.2 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 204 Protocol/Port Report Example
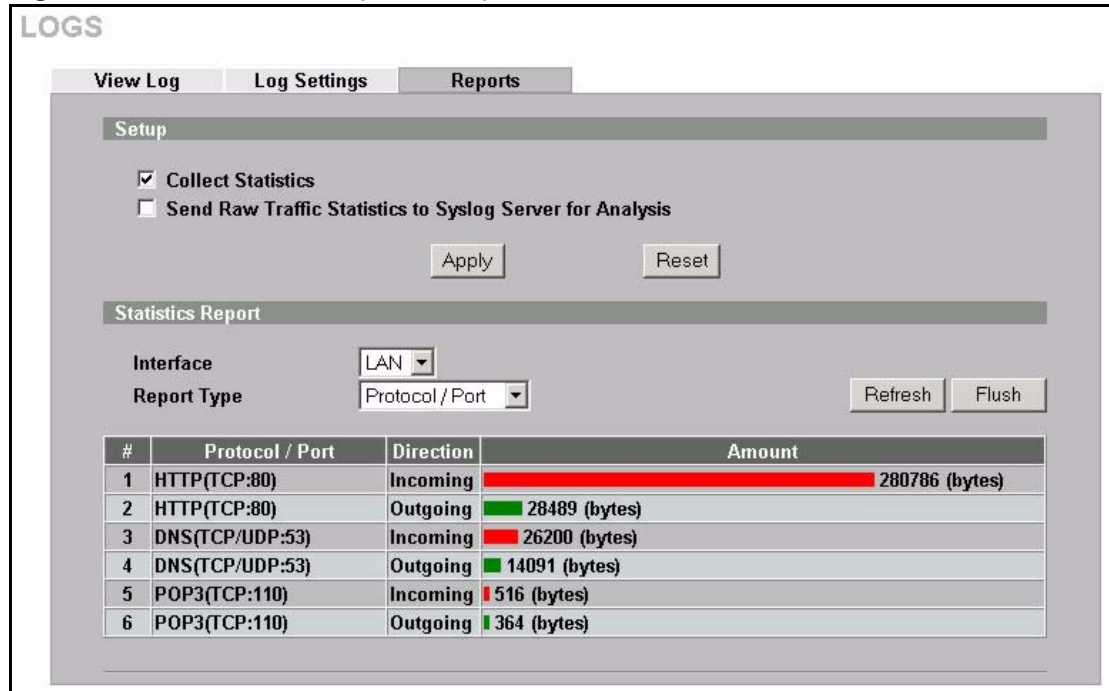
The following table describes the labels in this screen.

Table 136 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 or DMZ. This field displays **Outgoing** to denote traffic that is going out from the LAN or DMZ 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 138).

23.4.3 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 205 LAN IP Address Report Example
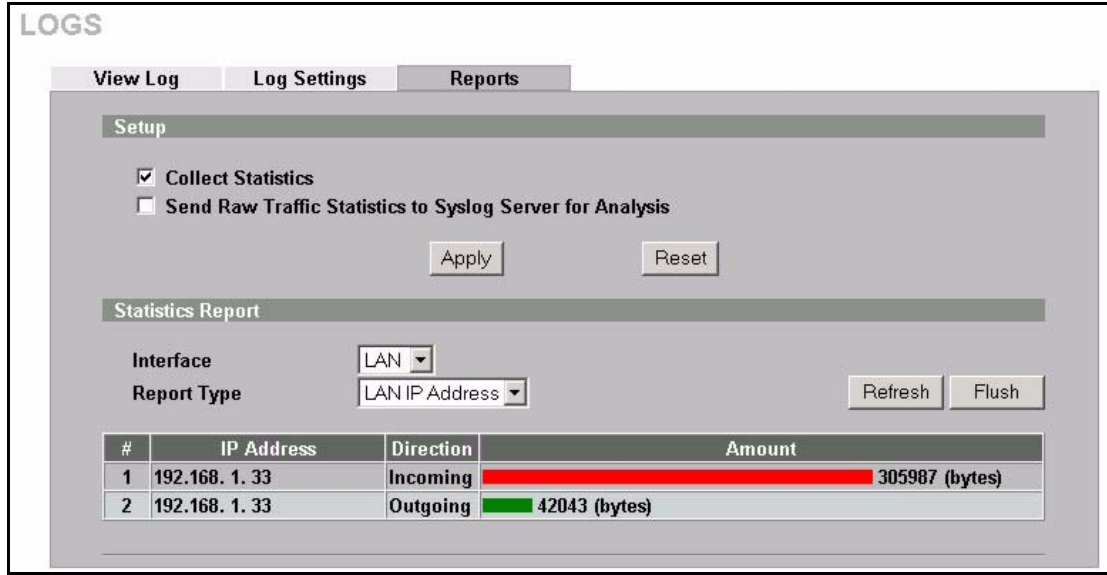
The following table describes the labels in this screen.

Table 137 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 or DMZ. This field displays **Outgoing** to denote traffic that is going out from the LAN or DMZ 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 138).

23.4.4 Reports Specifications

The following table lists detailed specifications on the reports feature.

Table 138 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.

C H A P T E R **24**
Maintenance

This chapter displays information on the maintenance screens.

24.1 Maintenance Overview

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

24.2 General Setup

24.2.1 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**.

24.2.2 Domain Name

The **Domain Name** entry is what is propagated to the DHCP clients on the LAN. If you leave this blank, the domain name obtained by DHCP from the ISP is used. While you must enter the host name (System Name), the domain name can be assigned from the ZyWALL via DHCP.

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

Figure 206 General Setup

The following table describes the labels in this screen.

Table 139 General Setup

LABEL	DESCRIPTION
General Setup	
System Name	Choose a descriptive name for identification purposes. It is recommended you enter your computer's "Computer name" in this field. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	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 SMT) can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
Apply	Click **Apply** to save your changes back to the ZyWALL.
Reset	Click **Reset** to begin configuring this screen afresh.

24.3 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 207 Password Setup

The following table describes the labels in this screen.

Table 140 Password Setup

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.

24.4 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:** 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 141 Default Time Servers

ntp1.cs.wisc.edu
ntp1.gbg.netnod.se
ntp2.cs.wisc.edu
tock.usno.navy.mil

Table 141 Default Time Servers

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

24.5 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 208   Time and Date

The following table describes the labels in this screen.

Table 142   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 142 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.

24.5.1 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 209   Synchronization in Process
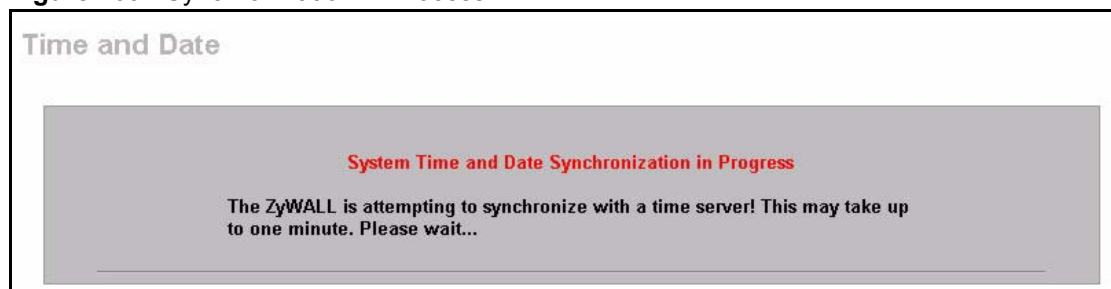
Click the **Return** button to go back to the **Time and Date** screen after the time and date is updated successfully.

Figure 210 Synchronization is Successful
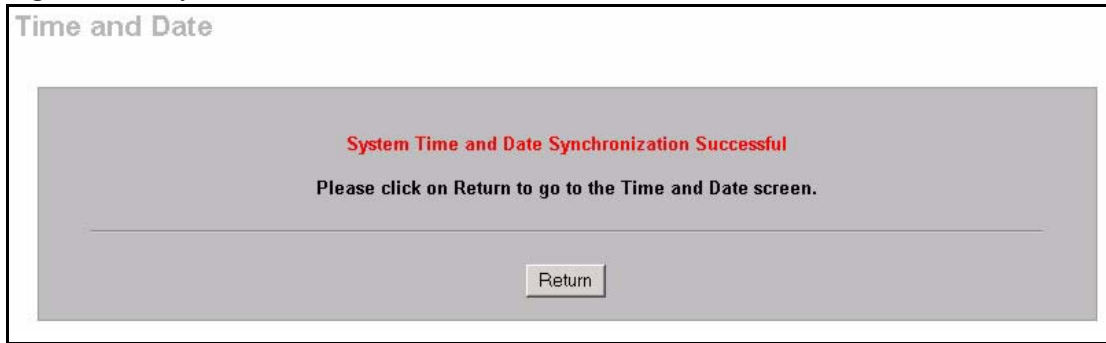
If the update was not successful, the following screen appears. Click **Return** to go back to the **Time and Date** screen.

Figure 211 Synchronization Fail
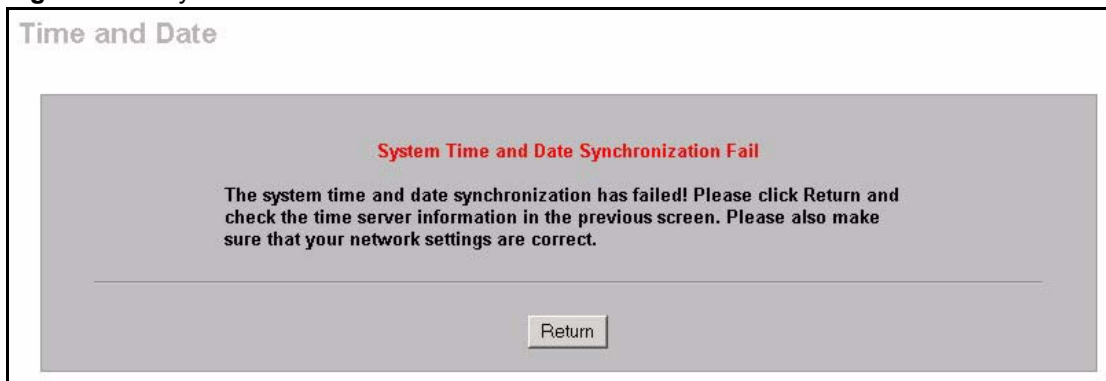
24.6 Configuring Device Mode

To configure and have your ZyWALL work as a router or a bridge, click **MAINTENANCE**, then the **Device Mode** tab. When the ZyWALL is in router mode, the screen appears as shown next.

Figure 212 Device Mode (Router Mode)
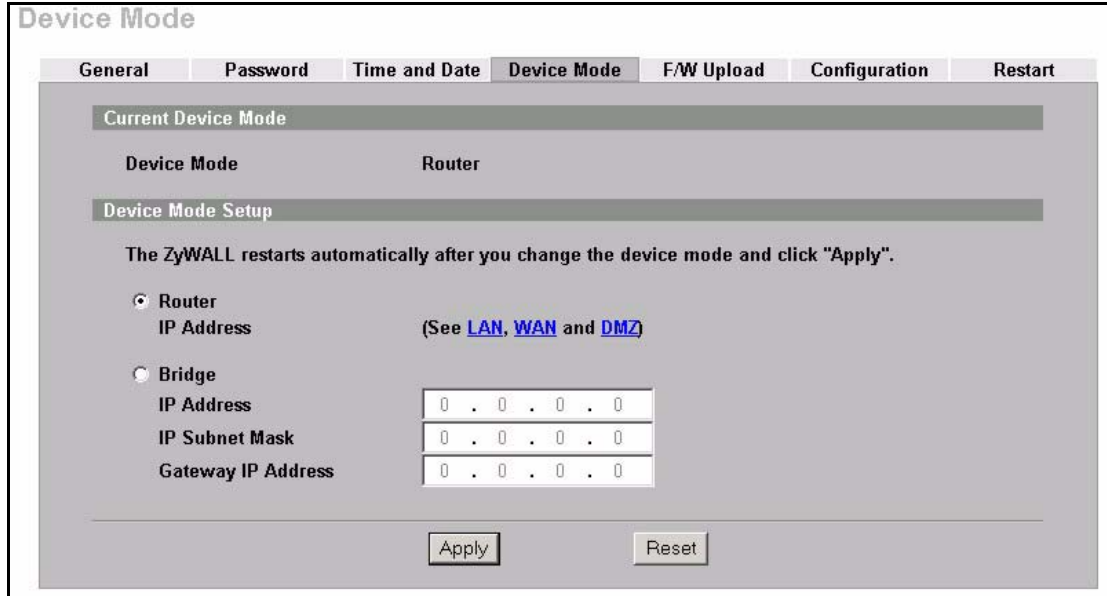
The following table describes the labels in this screen.

Table 143 Device Mode (Router Mode)

LABEL	DESCRIPTION
Current Device Mode	
Device Mode	This displays whether the ZyWALL is functioning as a router or a bridge.
Device Mode Setup	
Router	When the ZyWALL is in router mode, there is no need to select or clear this radio button.
IP Address	Click **LAN**, **WAN** or **DMZ** to go to the **LAN**, **WAN** or **DMZ** screen where you can view and/or change the corresponding settings.
Bridge	Select this radio button and configure the following fields, then click **Apply** to set the ZyWALL to bridge mode.
IP Address	Enter the IP address of your ZyWALL in dotted decimal notation.
Subnet Mask	Enter the IP subnet mask of the ZyWALL.
Gateway IP Address	Enter the gateway IP address.
Apply	Click **Apply** to save your changes back to the ZyWALL. After you click **Apply**, please wait for one minute and use the IP address you configured in the **IP Address** field to access the ZyWALL again.
Reset	Click **Reset** to begin configuring this screen afresh.

When the ZyWALL is in bridge mode, the screen appears as shown next

Figure 213 Device Mode (Bridge Mode)

The following table describes the labels in this screen.

Table 144 Device Mode (Bridge Mode)

LABEL	DESCRIPTION
Current Device Mode	
Device Mode	This displays whether the ZyWALL is functioning as a router or a bridge.
Device Mode Setup	
Router	Select this radio button and click **Apply** to set the ZyWALL to router mode.
LAN Interface IP Address	Enter the IP address of your ZyWALL' s LAN port in dotted decimal notation. 192.168.1.1 is the factory default.
LAN Interface Subnet Mask	Enter the IP subnet mask of the ZyWALL's LAN port.
DHCP Server	DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (computers) to obtain TCP/IP configuration at startup from a server. Unless you are instructed by your ISP, leave the **DHCP Server** check box selected. Clear it to stop the ZyWALL from acting as a DHCP server. When configured as a server, the ZyWALL provides TCP/IP configuration for the clients. If not, DHCP service is disabled and you must have another DHCP server on your LAN, or else the computers must be manually configured. When set as a server, fill in the rest of the DHCP setup fields.
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Pool Size	This field specifies the size, or count of the IP address pool.
Bridge	When the ZyWALL is in bridge mode, there is no need to select or clear this radio button.
IP Address	Click **Bridge** to go to the **Bridge** screen where you can view and/or change the bridge settings.

Table 144 Device Mode (Bridge Mode) (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the ZyWALL. After you click **Apply**, please wait for one minute and use the IP address you configured in the **LAN Interface IP Address** field to access the ZyWALL again.
Reset	Click **Reset** to begin configuring this screen afresh.

24.7 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 uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot. See the Uploading Firmware and Configuration Files section 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 214   Firmware Upload
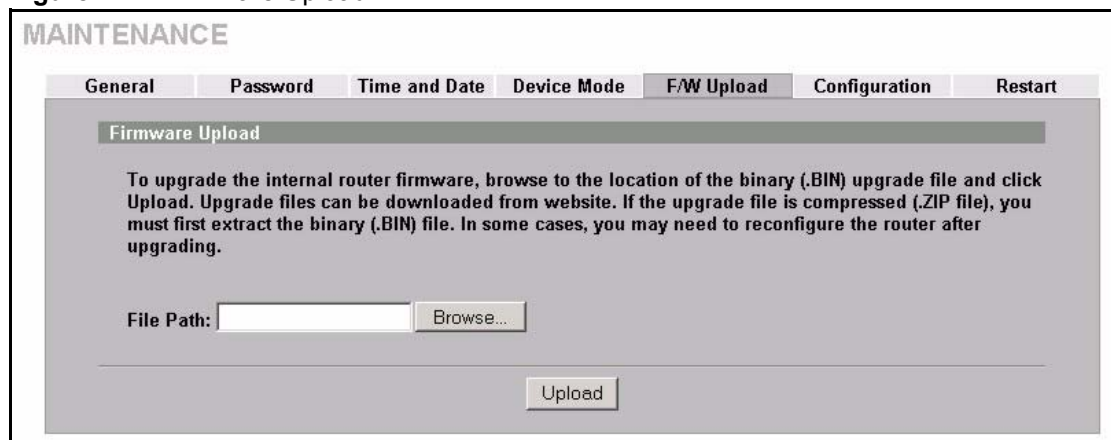
The following table describes the labels in this screen.

Table 145   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 215 Firmware Upload In Process
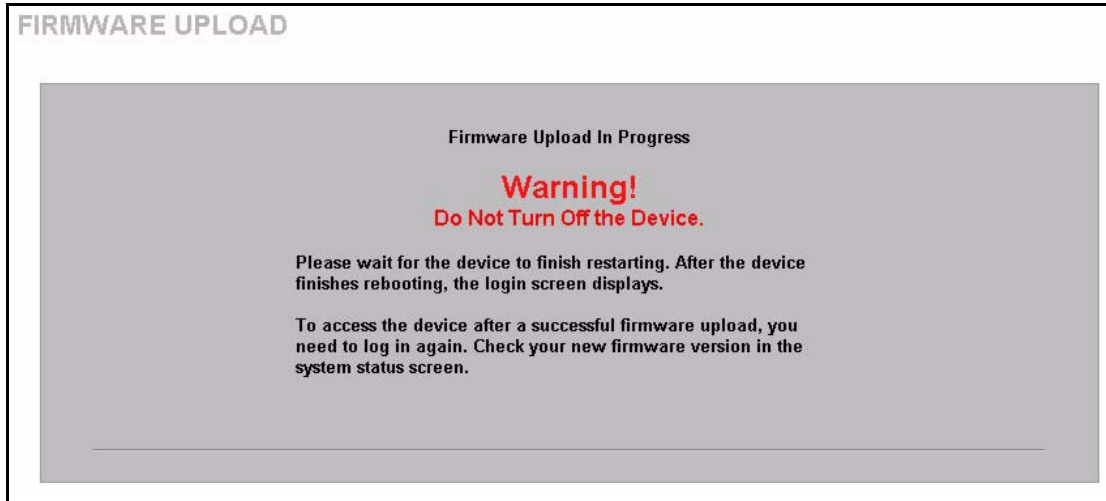
The ZyWALL automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 216 Network Temporarily Disconnected

After 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 217 Firmware Upload Error

24.8 Configuration Screen

See the Uploading Firmware and Configuration Files section 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 218   Configuration
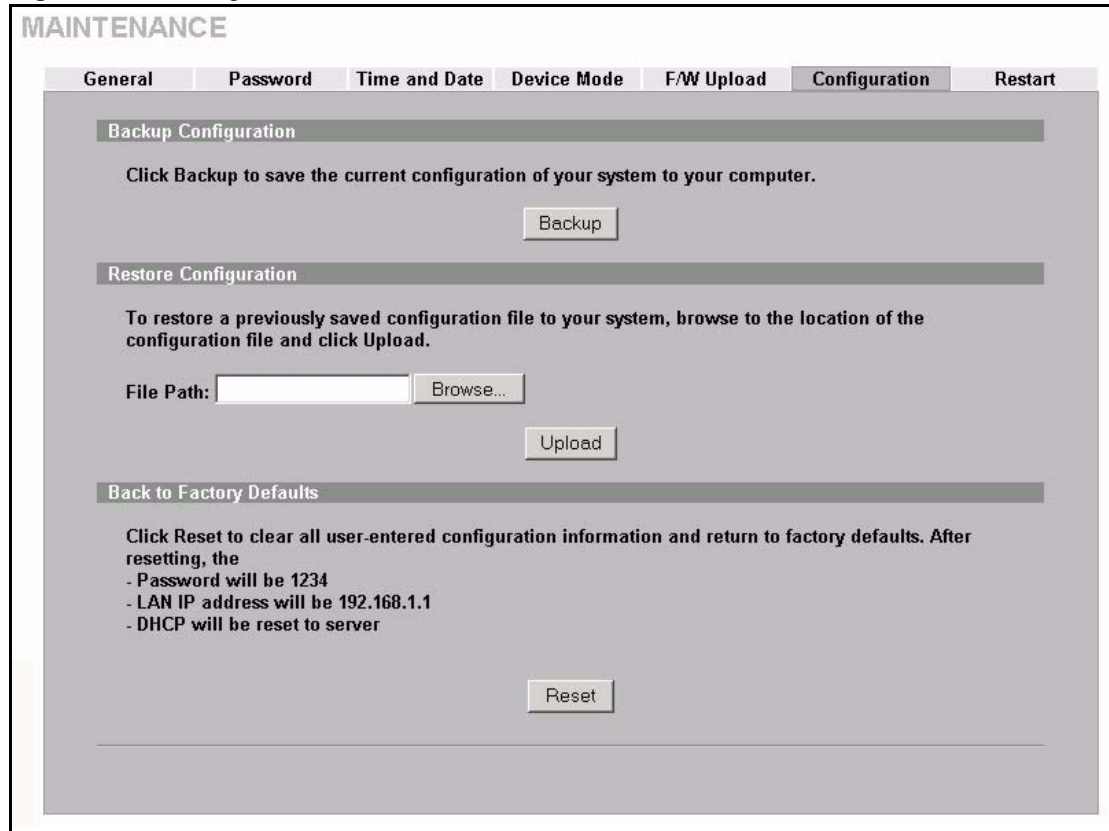
24.8.1 Backup Configuration

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.

24.8.2 Restore Configuration

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

Table 146   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 219   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 220   Network Temporarily Disconnected

If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.1). See your *Quick Start Guide* for details on how to set up your computer's IP address.

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **Configuration** screen.

Figure 221   Configuration Upload Error

24.8.3 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 222   Reset Warning Message
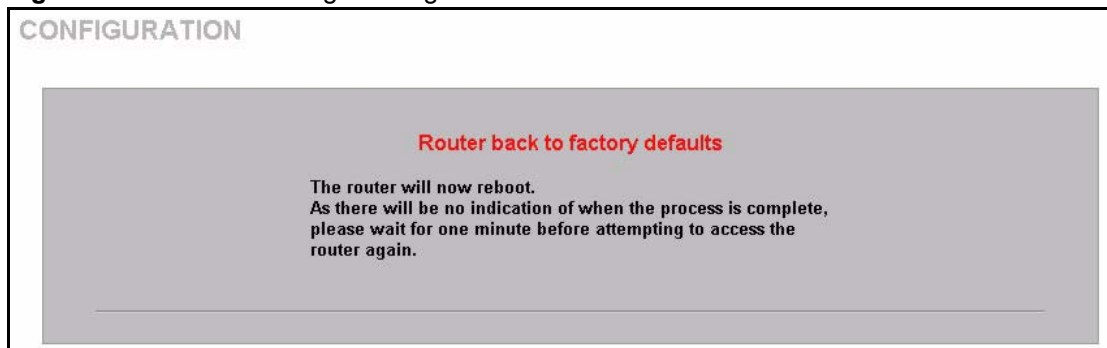
You can also press the **RESET** button on the rear panel to reset the factory defaults of your ZyWALL. Refer to the Resetting the ZyWALL section for more information on the **RESET** button.

24.9 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 223   Restart Screen

CHAPTER 25
Introducing the SMT

This chapter explains how to access the System Management Terminal and gives an overview of its menus.

25.1 Introduction to the SMT

The ZyWALL's SMT (System Management Terminal) is a menu-driven interface that you can access from a terminal emulator through the console port or over a telnet connection. This chapter shows you how to access the SMT (System Management Terminal) menus via console port, how to navigate the SMT and how to configure SMT menus.

25.2 Accessing the SMT via the Console Port

Make sure you have the physical connection properly set up as described in the *Quick Start Guide*.

When configuring using the console port, you need a computer equipped with communications software configured to the following parameters:

- VT100 terminal emulation.
- 9600 Baud.
- No parity, 8 data bits, 1 stop bit, flow control set to none.

25.2.1 Initial Screen

When you turn on your ZyWALL, it performs several internal tests as well as line initialization.

After the tests, the ZyWALL asks you to press [ENTER] to continue, as shown next.

Figure 224 Initial Screen

```
            Copyright (c) 1994 - 2004 ZyXEL Communications Corp.

            initialize ch =0, ethernet address: 00:A0:C5:01:23:45
            initialize ch =1, ethernet address: 00:A0:C5:01:23:46
            initialize ch =2, ethernet address: 00:A0:C5:01:23:47
            initialize ch =3, ethernet address: 00:A0:C5:01:23:48
            initialize ch =4, ethernet address: 00:00:00:00:00:00
            AUX port init . done
            Modem init . inactive

            Press ENTER to continue...
```

25.2.2 Entering the Password

The login screen appears after you press [ENTER], prompting you to enter the password, as shown below.

For your first login, enter the default password "1234". As you type the password, the screen displays an "X" for each character you type.

Please note that if there is no activity for longer than five minutes after you log in, your ZyWALL will automatically log you out and display a blank screen. If you see a blank screen, press [ENTER] to bring up the login screen again.

Figure 225 Password Screen

```
            Enter Password : XXXX
```

25.3 Navigating the SMT Interface

The SMT is an interface that you use to configure your ZyWALL.

Several operations that you should be familiar with before you attempt to modify the configuration are listed in the table below.

Table 147 Main Menu Commands

OPERATION	KEYSTROKES	DESCRIPTION
Move down to another menu	[ENTER]	To move forward to a submenu, type in the number of the desired submenu and press [ENTER].
Move up to a previous menu	[ESC]	Press the [ESC] key to move back to the previous menu.

Table 147   Main Menu Commands

OPERATION	KEYSTROKES	DESCRIPTION
Move to a "hidden" menu	Press [SPACE BAR] to change No to Yes then press [ENTER].	Fields beginning with "Edit" lead to hidden menus and have a default setting of No. Press [SPACE BAR] to change No to Yes, and then press [ENTER] to go to a "hidden" menu.
Move the cursor	[ENTER] or [UP]/ [DOWN] arrow keys	Within a menu, press [ENTER] to move to the next field. You can also use the [UP]/[DOWN] arrow keys to move to the previous and the next field, respectively.
Entering information	Fill in, or press [SPACE BAR], then press [ENTER] to select from choices.	You need to fill in two types of fields. The first requires you to type in the appropriate information. The second allows you to cycle through the available choices by pressing [SPACE BAR].
Required fields	<? >	All fields with the symbol <?> must be filled in order be able to save the new configuration.
N/A fields	<N/A>	Some of the fields in the SMT will show a <N/A>. This symbol refers to an option that is Not Applicable.
Save your configuration	[ENTER]	Save your configuration by pressing [ENTER] at the message "Press ENTER to confirm or ESC to cancel". Saving the data on the screen will take you, in most cases to the previous menu.
Exit the SMT	Type 99, then press [ENTER].	Type 99 at the main menu prompt and press [ENTER] to exit the SMT interface.

25.3.1 Main Menu

After you enter the password, the SMT displays the **ZyWALL Main Menu**, as shown next.

Figure 226 Main Menu (Router Mode)

```
            Copyright (c) 1994 - 2004 ZyXEL Communications Corp.

                        ZyWALL 35 Main Menu

    Getting Started                    Advanced Management
      1. General Setup                   21. Filter and Firewall Setup
      2. WAN Setup                       22. SNMP Configuration
      3. LAN Setup                       23. System Password
      4. Internet Access Setup           24. System Maintenance
      5. DMZ Setup                       25. IP Routing Policy Setup
      6. Route Setup                     26. Schedule Setup
    Advanced Applications                27. VPN/IPSec Setup
      11. Remote Node Setup
      12. Static Routing Setup
      15. NAT Setup


                                               99. Exit


                  Enter Menu Selection Number:
```

Figure 227 Main Menu (Bridge Mode)

```
      Copyright (c) 1994 - 2004 ZyXEL Communications Corp.

                        ZyWALL 35 Main Menu

    Getting Started                Advanced Management
      1. General Setup               21. Filter and Firewall Setup
                                      22. SNMP Configuration
                                      23. System Password
                                      24. System Maintenance


                                      99. Exit



                  Enter Menu Selection Number:
```

The following table describes the fields in this menu.

Table 148 Main Menu Summary

NO.	MENU TITLE	FUNCTION
1	General Setup	Use this menu to set up device mode, dynamic DNS and administrative information.
2	WAN Setup	Use this menu to clone a MAC address from a computer on your LAN and configure the backup WAN dial-up connection.

Table 148 Main Menu Summary

NO.	MENU TITLE	FUNCTION
3	LAN Setup	Use this menu to apply LAN filters, configure LAN DHCP and TCP/IP settings and configure the wireless LAN port.
4	Internet Access Setup	Configure your Internet Access setup (Internet address, gateway, login, etc.) with this menu.
5	DMZ Setup	Use this menu to configure your public servers connected to the DMZ port.
6	Route Setup	Use this menu to configure your WAN route assessment, traffic redirect properties and failover parameters.
11	Remote Node Setup	Use this menu to configure detailed remote node settings (your ISP is also a remote node) as well as apply WAN filters.
12	Static Routing Setup	Configure IP static routes in this menu.
15	NAT Setup	Use this menu to configure Network Address Translation.
21	Filter and Firewall Setup	Configure filters, activate/deactivate the firewall and view the firewall log.
22	SNMP Configuration	Use this menu to configure SNMP-related parameters.
23	System Password	Change your password in this menu (recommended).
24	System Maintenance	From displaying system status to uploading firmware, this menu provides comprehensive system maintenance.
25	IP Routing Policy Setup	From displaying system status to uploading firmware, this menu provides comprehensive system maintenance.
26	Schedule Setup	Use this menu to schedule outgoing calls.
27	VPN /IPSec Setup	Use this menu to configure VPN connections.
99	Exit	Use this menu to exit (necessary for remote configuration).

25.3.2 SMT Menus at a Glance

The following figure gives you an example overview of the various SMT menu screens for your ZyWALL.

Figure 228 ZyWALL SMT Menu Overview Example
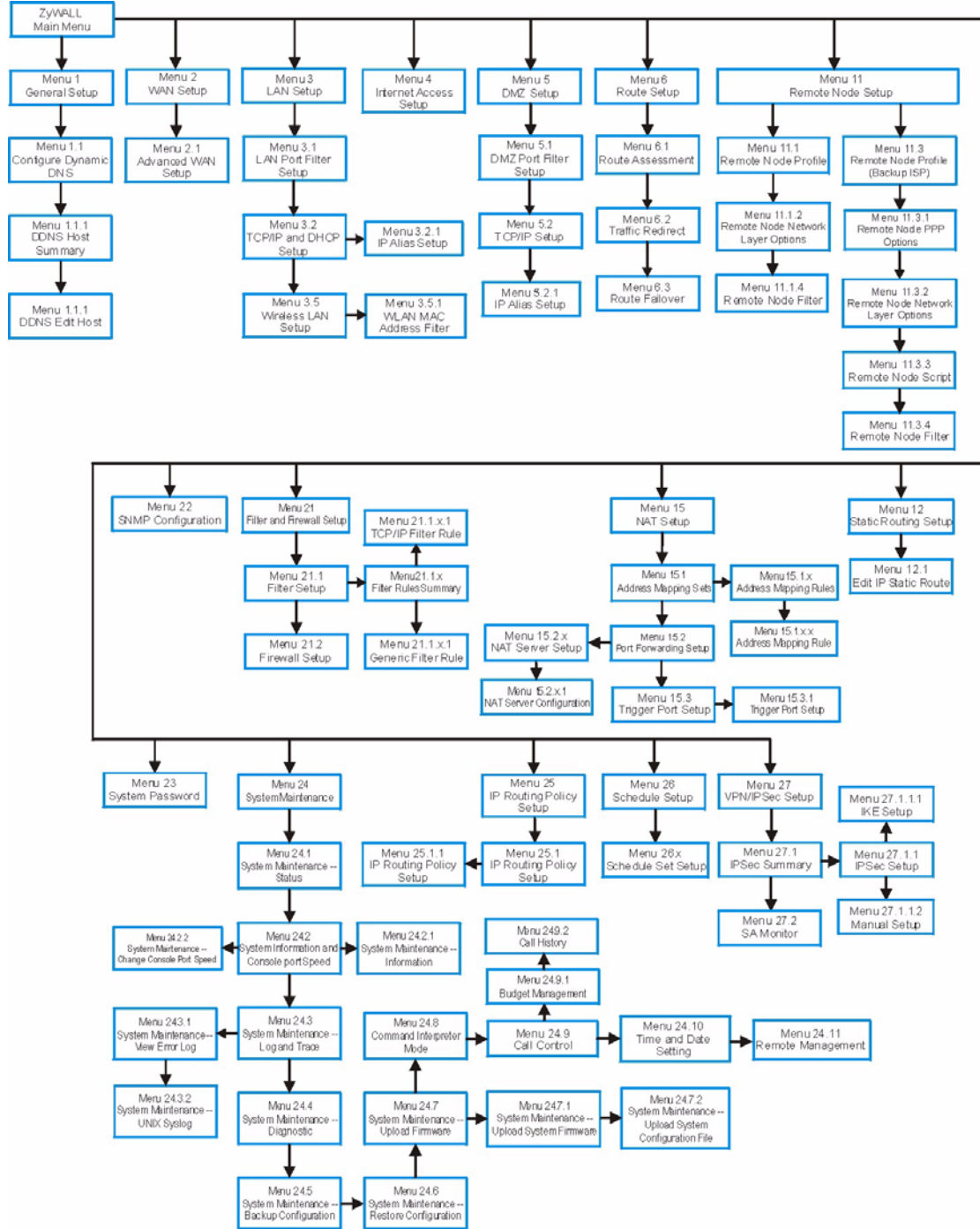
25.4 Changing the System Password

Change the system password by following the steps shown next.

1 Enter 23 in the main menu to open **Menu 23 - System Password** as shown next.

Figure 229 Menu 23: System Password

```
                          Menu 23 - System Password

                  Old Password= ?
                  New Password= ?
                  Retype to confirm= ?




                   Enter here to CONFIRM or ESC to CANCEL:
```

2 Type your existing password and press [ENTER].

3 Type your new system password and press [ENTER].

4 Re-type your new system password for confirmation and press [ENTER].

Note that as you type a password, the screen displays an "x" for each character you type.

25.5 Resetting the ZyWALL

See Chapter 2 Introducing the Web Configurator for directions on resetting the ZyWALL.

Chapter 25 Introducing the SMT

C HAPTER 26
SMT Menu 1 - General Setup

Menu 1 - General Setup contains administrative and system-related information.

26.1 Introduction to General Setup

Menu 1 - General Setup contains administrative and system-related information.

26.2 Configuring General Setup

1 Enter 1 in the main menu to open **Menu 1 - General Setup**.

2 The **Menu 1 - General Setup** screen appears, as shown next. Fill in the required fields.

Figure 230   Menu 1: General Setup (Router Mode)

```
                 Menu 1 - General Setup

          System Name= ZyWALL35
          Domain Name= zyxel.com.tw

          Device Mode= Router Mode


          Edit Dynamic DNS= No

          Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

Table 149   Menu 1: General Setup (Router Mode)

FIELD	DESCRIPTION
System Name	Choose a descriptive name for identification purposes. It is recommended you enter your computer's "Computer name" in this field. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. You can go to menu 24.8 and type "sys domain name" to see the current domain name used by your router.
	The domain name entered by you is given priority over the ISP assigned domain name. If you want to clear this field just press [SPACE BAR] and then [ENTER].
Device Mode	Press [SPACE BAR] and then [ENTER] to select **Router Mode**.

Table 149 Menu 1: General Setup (Router Mode) (continued)

FIELD	DESCRIPTION
Edit Dynamic DNS	Press [SPACE BAR] and then [ENTER] to select **Yes** or **No** (default). Select **Yes** to configure **Menu 1.1: Configure Dynamic DNS** discussed next.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

Figure 231 Menu 1: General Setup (Bridge Mode)

```
                     Menu 1 - General Setup

        System Name= Zy35
        Domain Name= zyxel.com.tw

        Device Mode= Bridge Mode

        IP Address= 172.21.5.22
        Network Mask= 255.255.0.0
        Gateway= 172.21.0.254
        First System DNS Server
          IP Address= 0.0.0.0
        Second System DNS Server
          IP Address= 0.0.0.0
        Third System DNS Server
          IP Address= 0.0.0.0


                    Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields not previously discussed (see Table 149).

Table 150 Menu 1: General Setup (Bridge Mode)

FIELD	DESCRIPTION
Device Mode	Press [SPACE BAR] and then [ENTER] to select **Bridge Mode**.
IP Address	Enter the IP address of your ZyWALL in dotted decimal notation.
Network Mask	Enter the subnet mask of your ZyWALL.
Gateway	Enter the gateway IP address.
First System DNS Server Second System DNS Server Third System DNS Server	Enter the DNS server's IP address(es) in the **IP Address** field(s) if you have the IP address(es) of the DNS server(s).

26.2.1 Configuring Dynamic DNS

To configure Dynamic DNS, set the ZyWALL to router mode in menu 1 or in the **MAINTENANCE Device Mode** screen and go to **Menu 1 - General Setup** and press [SPACE BAR] to select **Yes** in the **Edit Dynamic DNS** field. Press [ENTER] to display **Menu 1.1 - Configure Dynamic DNS** (shown next).

Figure 232 Menu 1.1: Configure Dynamic DNS

```
         Menu 1.1 - Configure Dynamic DNS

             Service Provider= WWW.DynDNS.ORG
             Active= No
             Username=
             Password= ********
             Edit Host= No


             Press ENTER to Confirm or ESC to Cancel:
```

Follow the instructions in the next table to configure Dynamic DNS parameters.

Table 151 Menu 1.1: Configure Dynamic DNS

FIELD	DESCRIPTION
Service Provider	This is the name of your Dynamic DNS service provider.
Active	Press [SPACE BAR] to select **Yes** and then press [ENTER] to make dynamic DNS active.
Username	Enter your user name.
Password	Enter the password assigned to you.
Edit Host	Press [SPACE BAR] and then [ENTER] to select **Yes** if you want to configure a DDNS host.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

The IP address updates when you reconfigure menu 1 or perform DHCP client renewal.

26.2.1.1 Editing DDNS Host

To configure a DDNS host, follow the procedure below.

1 Configure your ZyWALL as a router in menu 1 or the **MAINTENANCE Device Mode** screen.

2 Enter 1 in the main menu to open **Menu 1 - General Setup**.

3 press [SPACE BAR] to select **Yes** in the **Edit Dynamic DNS** field. Press [ENTER] to display **Menu 1.1 - Configure Dynamic DNS**.

4 Press [SPACE BAR] and then [ENTER] to select **Yes** in the **Edit Host** field. Press [ENTER] to display **Menu 1.1.1 - DDNS Host Summary**.

Figure 233 Menu 1.1.1: DDNS Host Summary

```
            Menu 1.1.1 DDNS Host Summary

  #                      Summary
  --- - -------------------------------------------------------
  01    Hostname=ZyWALL,
          Type=Dynamic,WC=Yes,Offline=No,Policy=DDNS Server
        Detect, WAN1, HA=Yes
  02     _____
         _____
  03     _____
         _____
  04     _____
         _____
  05     _____
         _____
         _____


            Select Command= None          Select Rule= N/A
                  Press ENTER to Confirm or ESC to Cancel:
```
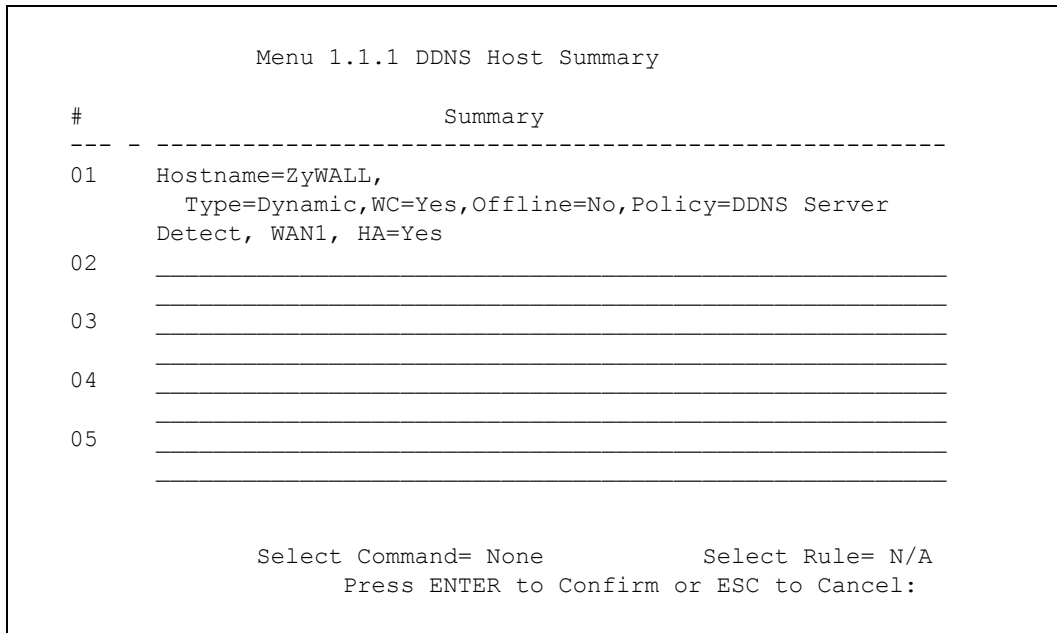
The following table describes the fields in this screen.

Table 152 Menu 1.1.1: DDNS Host Summary

FIELD	DESCRIPTION
#	This is the DDNS host index number.
Summary	This displays the details about the DDNS host.
Select Command	Press [SPACE BAR] to choose from **None**, **Edit**, **Delete**, **Next Page** or **Previous Page** and then press [ENTER]. You must select a DDNS host in the next field when you choose the **Edit** or **Delete** commands.
	Select **None** and then press [ENTER] to go to the "Press ENTER to Confirm…" prompt.
	Use **Edit** to create or edit a rule. Use **Delete** to remove a rule. To edit or delete a DDNS host, first make sure you are on the correct page. When a rule is deleted, subsequent rules do not move up in the page list.
	Select **Next Page** or **Previous Page** to view the next or previous page of DDNS hosts (respectively).
Select Rule	Type the DDNS host index number you wish to edit or delete and then press [ENTER].
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

5 Select **Edit** in the **Select Command** field; type the index number of the DDNS host you want to configure in the **Select Rule** field and press [ENTER] to open **Menu 1.1.1 - DDNS Edit Host** (see the next figure).

Figure 234 Menu 1.1.1: DDNS Edit Host

```
                       Menu 1.1.1 - DDNS Edit Host

            Hostname= ZyWALL
            DDNS Type= DynamicDNS
            Enable Wildcard Option= Yes
            Enable Off Line Option= N/A
            Bind WAN= 1
            HA= Yes
            IP Address Update Policy:
              DDNS Server Auto Detect IP Address= Yes
              Use Specified IP Address= N/A
              Use IP Address= N/A



                        Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this screen.

Table 153 Menu 1.1.1: DDNS Edit Host

FIELD	DESCRIPTION
Host Name	Enter your host name in this field.
DDNS Type	Press [SPACE BAR] and then [ENTER] to select **DynamicDNS** if you have a dynamic IP address(es). Select **StaticDNS** if you have a static IP address(s).
	Select **CustomDNS** to have dyns.org provide DNS service for a domain name that you already have from a source other than dyndns.org.
Enable Wildcard Option	Your ZyWALL supports DYNDNS Wildcard. Press [SPACE BAR] and then [ENTER] to select **Yes** or **No**. This field is **N/A** when you choose DDNS client as your service provider.
Enable Off Line Option	This field is only available when **CustomDNS** is selected in the **DDNS Type** field. Press [SPACE BAR] and then [ENTER] to select **Yes**. When **Yes** is selected, http://www.dyndns.org/ traffic is redirected to a URL that you have previously specified (see www.dyndns.org for details).
Bind WAN	Enter the WAN port to use for updating the IP address of the domain name.
HA	Press [SPACE BAR] and then [ENTER] to select **Yes** to enable the high availability (HA) feature.
	If the WAN port specified in the **Bind WAN** field does not have a connection, the ZyWALL will attempt to use the IP address of another WAN port to update the domain name.
	When the WAN ports are in the active/passive operating mode, the ZyWALL will update the domain name with the IP address of whichever WAN port has a connection, regardless of the setting in the **Bind WAN** field.
	Clear this check box and the ZyWALL will not update the domain name with an IP address if the WAN port specified in the **Bind WAN** field does not have a connection.
	Note: If you enable high availability, DDNS can also function when the ZyWALL uses the dial backup port. DDNS does not function when the ZyWALL uses traffic redirect.
	Refer to the High Availability section in Chapter 20 DNS for detailed information.

Table 153   Menu 1.1.1: DDNS Edit Host (continued)

FIELD	DESCRIPTION
IP Address Update Policy:	You can select **Yes** in either the **DDNS Server Auto Detect IP Address** field (recommended) or the **Use Specified IP Address** field, but not both.
	With the **DDNS Server Auto Detect IP Address** and **Use Specified IP Address** fields both set to **No**, the DDNS server automatically updates the IP address of the host name(s) with the ZyWALL's WAN IP address.
	DDNS does not work with a private IP address. When both fields are set to **No**, the ZyWALL must have a public WAN IP address in order for DDNS to work.
DDNS Server Auto Detect IP Address	Only select this option when there are one or more **NAT** routers between the ZyWALL and the DDNS server. Press [SPACE BAR] to select **Yes** and then press [ENTER] to have the DDNS server automatically detect and use the IP address of the NAT router that has a public IP address.
	Note: The DDNS server may not be able to detect the proper IP address if there is an HTTP proxy server between the ZyWALL and the DDNS server.
Use Specified IP Address	Press [SPACE BAR] to select **Yes** and then press [ENTER] to update the IP address of the host name(s) to the IP address specified below.
	Only select **Yes** if the ZyWALL uses or is behind a static public IP address.
Use IP Address	Enter the static public IP address if you select **Yes** in the **Use Specified IP Address** field.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

CHAPTER 27
WAN and Dial Backup Setup

This chapter describes how to configure the WAN using menu 2 and dial-backup using menus 2.1 and 11.1.

27.1 Introduction to WAN and Dial Backup Setup

This chapter explains how to configure settings for your WAN port and how to configure the ZyWALL for a dial backup connection.

27.2 WAN Setup

From the main menu, enter 2 to open menu 2.

Figure 235 MAC Address Cloning in WAN Setup

```
                    Menu 2 - WAN Setup

          WAN 1 MAC Address:
            Assigned By= Factory default
            IP Address= N/A
          WAN 2 MAC Address:
            Assigned By= Factory default
            IP Address= N/A

          Dial-Backup:
            Active= No
            Port Speed= 115200
            AT Command String:
              Init= at&fs0=0
            Edit Advanced Setup= No


        Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this screen.

Table 154   MAC Address Cloning in WAN Setup

FIELD	DESCRIPTION
WAN 1/2 MAC Address	
Assigned By	Press [SPACE BAR] and then [ENTER] to choose one of two methods to assign a MAC Address. Choose **Factory Default** to select the factory assigned default MAC Address. Choose **IP address attached on LAN** to use the MAC Address of that computer whose IP you give in the following field.
IP Address	This field is applicable only if you choose the **IP address attached on LAN** method in the **Assigned By** field. Enter the IP address of the computer on the LAN whose MAC you are cloning.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

27.3 Dial Backup

The Dial Backup port can be used in reserve, as a traditional dial-up connection should the broadband connection to the WAN port fail. To set up the auxiliary port (Dial Backup) for use in the event that the regular WAN connection is dropped, first make sure you have set up the switch and port connection (see the *Quick Start Guide*), then configure

1 Menu 2 - WAN Setup,

2 Menu 2.1 - Advanced WAN Setup and

3 Menu 11.1 - Remote Node Profile (Backup ISP) as shown next

Refer also to the section about traffic redirect for information on an alternate backup WAN connection.

27.4 Configuring Dial Backup in Menu 2

From the main menu, enter 2 to open menu 2.

Figure 236 Menu 2: Dial Backup Setup

```
         Menu 2 - WAN Setup

    WAN 1 MAC Address:
      Assigned By= Factory default
      IP Address= N/A
    WAN 2 MAC Address:
      Assigned By= Factory default
      IP Address= N/A


    Dial-Backup:
      Active= No
      Port Speed= 115200
      AT Command String:
        Init= at&fs0=0
      Edit Advanced Setup= No



    Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

Table 155 Menu 2: Dial Backup Setup

FIELD	DESCRIPTION
Dial-Backup:	
Active	Use this field to turn the dial-backup feature on (**Yes**) or off (**No**).
Port Speed	Press [SPACE BAR] and then press [ENTER] to select the speed of the connection between the Dial Backup port and the external device. Available speeds are: **9600**, **19200**, **38400**, **57600**, **115200** or **230400** bps.
AT Command String:	
Init	Enter the AT command string to initialize the WAN device. Consult the manual of your WAN device connected to your Dial Backup port for specific AT commands.
Edit Advanced Setup	To edit the advanced setup for the Dial Backup port, move the cursor to this field; press the [SPACE BAR] to select **Yes** and then press [ENTER] to go to **Menu 2.1 - Advanced Setup**.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

27.5 Advanced WAN Setup

> **Note:** Consult the manual of your WAN device connected to your Dial Backup port for specific AT commands.

To edit the advanced setup for the Dial Backup port, move the cursor to the **Edit Advanced Setup** field in **Menu 2 - WAN Setup**, press the [SPACE BAR] to select **Yes** and then press [ENTER].

Figure 237   Menu 2.1: Advanced WAN Setup

```
      Menu 2.1 - Advanced WAN Setup

    AT Command Strings:                  Call Control:
      Dial= atdt                          Dial Timeout(sec)= 60
      Drop= ~~+++~~ath                    Retry Count= 0
      Answer= ata                         Retry Interval(sec)= N/A
                                          Drop Timeout(sec)= 20
    Drop DTR When Hang Up= Yes            Call Back Delay(sec)= 15

    AT Response Strings:
      CLID= NMBR =
      Called Id=
      Speed= CONNECT

            Press ENTER to Confirm or ESC to Cancel:
```

The following table describes fields in this menu.

Table 156   Advanced WAN Port Setup: AT Commands Fields

FIELD	DESCRIPTION
AT Command Strings:	
Dial	Enter the AT Command string to make a call.
Drop	Enter the AT Command string to drop a call. "~" represents a one second wait, e.g., "~~+++~~ath" can be used if your modem has a slow response time.
Answer	Enter the AT Command string to answer a call.
Drop DTR When Hang Up	Press the [SPACE BAR] to choose either **Yes** or **No**. When **Yes** is selected (the default), the DTR (Data Terminal Ready) signal is dropped after the "AT Command String: Drop" is sent out.
AT Response Strings:	
CLID (Calling Line Identification)	Enter the keyword that precedes the CLID (Calling Line Identification) in the AT response string. This lets the ZyWALL capture the CLID in the AT response string that comes from the WAN device. CLID is required for CLID authentication.
Called Id	Enter the keyword preceding the dialed number.
Speed	Enter the keyword preceding the connection speed.

Table 157 Advanced WAN Port Setup: Call Control Parameters

FIELD	DESCRIPTION
Call Control	
Dial Timeout (sec)	Enter a number of seconds for the ZyWALL to keep trying to set up an outgoing call before timing out (stopping). The ZyWALL times out and stops if it cannot set up an outgoing call within the timeout value.
Retry Count	Enter a number of times for the ZyWALL to retry a busy or no-answer phone number before blacklisting the number.
Retry Interval (sec)	Enter a number of seconds for the ZyWALL to wait before trying another call after a call has failed. This applies before a phone number is blacklisted.
Drop Timeout (sec)	Enter a number of seconds for the ZyWALL to wait before dropping the DTR signal if it does not receive a positive disconnect confirmation.
Call Back Delay (sec)	Enter a number of seconds for the ZyWALL to wait between dropping a callback request call and dialing the co-responding callback call.

27.6 Remote Node Profile (Backup ISP)

Enter **3** in **Menu 11 - Remote Node Setup** to open **Menu 11.3 - Remote Node Profile (Backup ISP)** (shown below) and configure the setup for your Dial Backup port connection.

Figure 238   Menu 11.3: Remote Node Profile (Backup ISP)

```
        Menu 11.3 - Remote Node Profile (Backup ISP)

   Rem Node Name= Dial                    Edit PPP Options= No
   Active= No                             Rem IP Addr= 0.0.0.0
                                          Edit IP= No
   Outgoing:                              Edit Script Options= No
     My Login= ChangeMe
     My Password= ********               Telco Option:
     Retype to Confirm= ********           Allocated Budget(min)= 0
     Authen= CHAP/PAP                       Period(hr)= 0
     Pri Phone #= 0                        Schedules=
     Sec Phone #=                          Nailed-Up Connection= No

                                         Session Options:
                                           Edit Filter Sets= No
                                           Idle Timeout(sec)= 100


   Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

Table 158 Menu 11.3: Remote Node Profile (Backup ISP)

FIELD	DESCRIPTION
Rem Node Name	Enter a descriptive name for the remote node. This field can be up to eight characters.
Active	Press [SPACE BAR] and then [ENTER] to select **Yes** to enable the remote node or **No** to disable the remote node.
Outgoing	
My Login	Enter the login name assigned by your ISP for this remote node.
My Password	Enter the password assigned by your ISP for this remote node.
Retype to Confirm	Enter your password again to make sure that you have entered is correctly.
Authen	This field sets the authentication protocol used for outgoing calls. Options for this field are: **CHAP/PAP** - Your ZyWALL will accept either **CHAP** or **PAP** when requested by this remote node. **CHAP** - accept CHAP only. **PAP** - accept PAP only.
Pri Phone # Sec Phone #	Enter the first (primary) phone number from the ISP for this remote node. If the Primary Phone number is busy or does not answer, your ZyWALL dials the Secondary Phone number if available. Some areas require dialing the pound sign # before the phone number for local calls. Include a # symbol at the beginning of the phone numbers as required.
Edit PPP Options	Move the cursor to this field and use the space bar to select [Yes] and press [Enter] to edit the PPP options for this remote node. This brings you to **Menu 11.3.1 - Remote Node PPP Options** (see the Editing PPP Options section).
Rem IP Addr	Leave the field set to 0.0.0.0 (default) if the remote gateway has a dynamic IP address. Enter the remote gateway's IP address here if it is static.
Edit IP	This field leads to a "hidden" menu. Press [SPACE BAR] to select **Yes** and press [ENTER] to go to **Menu 11.3.2 - Remote Node Network Layer Options**. See the Editing TCP/IP Options section for more information.
Edit Script Options	Press [SPACE BAR] to select **Yes** and press [ENTER] to edit the AT script for the dial backup remote node (**Menu 11.3.3 - Remote Node Script**). See the Editing Login Script section for more information.
Telco Option	
Allocated Budget	Enter the maximum number of minutes that this remote node may be called within the time period configured in the **Period** field. The default for this field is 0 meaning there is no budget control and no time limit for accessing this remote node.
Period(hr)	Enter the time period (in hours) for how often the budget should be reset. For example, to allow calls to this remote node for a maximum of 10 minutes every hour, set the **Allocated Budget** to 10 (minutes) and the **Period** to 1 (hour).
Schedules	You can apply up to four schedule sets here. For more details please refer to Chapter 43 Call Scheduling.
Nailed-Up Connection	Press [SPACE BAR] to select **Yes** to set this connection to always be on, regardless of whether or not there is any traffic. Select **No** to have this connection act as a dial-up connection.
Session Options	

Table 158   Menu 11.3: Remote Node Profile (Backup ISP) (continued)

FIELD	DESCRIPTION
Edit Filter sets	This field leads to another "hidden" menu. Use [SPACE BAR] to select **Yes** and press [ENTER] to open menu 11.3.4 to edit the filter sets. See the Remote Node Filter section for more details.
Idle Timeout	Enter the number of seconds of idle time (when there is no traffic from the ZyWALL to the remote node) that can elapse before the ZyWALL automatically disconnects the PPP connection. This option only applies when the ZyWALL initiates the call.
Once you have configured this menu, press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.	

27.7 Editing PPP Options

The ZyWALL's dial back-up feature uses PPP. To edit the remote node PPP Options, move the cursor to the **Edit PPP Options** field in **Menu 11.3 - Remote Node Profile (Backup ISP)**, and use the space bar to select **Yes**. Press [Enter] to open **Menu 11.3.1 - Remote Node PPP Options** as shown next.

Figure 239   Menu 11.3.1: Remote Node PPP Options

```
                Menu 11.3.1 - Remote Node PPP Options

            Encapsulation= Standard PPP
            Compression= No


                Enter here to CONFIRM or ESC to CANCEL:
```

This table describes the Remote Node PPP Options Menu, and contains instructions on how to configure the PPP options fields.

Table 159   Menu 11.3.1: Remote Node PPP Options

FIELD	DESCRIPTION
Encapsulation	Press [SPACE BAR] and then [ENTER] to select **CISCO PPP** if your Dial Backup WAN device uses Cisco PPP encapsulation, otherwise select **Standard PPP**.
Compression	Press [SPACE BAR] and then [ENTER] to select **Yes** to enable or **No** to disable Stac compression.
Once you have configured this menu, press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.	

27.8 Editing TCP/IP Options

Move the cursor to the **Edit IP** field in menu 11.3, then press [SPACE BAR] to select **Yes**. Press [ENTER] to open **Menu 11.3.2 - Remote Node Network Layer Options**.

Figure 240   Menu 11.3.2: Remote Node Network Layer Options

```
            Menu 11.3.2 - Remote Node Network Layer Options

         IP Address Assignment= Static
         Rem IP Addr= 0.0.0.0
         Rem Subnet Mask= 0.0.0.0
         My WAN Addr= 0.0.0.0

         Network Address Translation= SUA Only
         NAT Lookup Set= 255
         Metric= 15
         Private= No
         RIP Direction= None
           Version= N/A
         Multicast= None

          Enter here to CONFIRM or ESC to CANCEL:
```

The following table describes the fields in this menu.

Table 160   Menu 11.3.2: Remote Node Network Layer Options

FIELD	DESCRIPTION
IP Address Assignment	If your ISP did not assign you a fixed IP address, press [SPACE BAR] and then [ENTER] to select **Dynamic**, otherwise select **Static** and enter the IP address and subnet mask in the following fields.
Rem IP Address	Enter the (fixed) IP address assigned to you by your ISP (static IP address assignment is selected in the previous field).
Rem Subnet Mask	Enter the subnet mask associated with your static IP.
My WAN Addr	Leave the field set to 0.0.0.0 to have the ISP or other remote router dynamically (automatically) assign your WAN IP address if you do not know it. Enter your WAN IP address here if you know it (static).
	This is the address assigned to your local ZyWALL, not the remote router.
Network Address Translation	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet).
	Press [SPACE BAR] and then [ENTER] to select either **Full Feature**, **None** or **SUA Only.**
	Choose **None** to disable NAT.
	Choose **SUA Only** if you have a single public IP address. SUA (Single User Account) is a subset of NAT that supports two types of mapping: **Many-to-One** and **Server**.
	Choose **Full Feature** if you have multiple public IP addresses. **Full Feature** mapping types include: **One-to-One**, **Many-to-One** (SUA/PAT), **Many-to-Many Overload**, **Many- One-to-One** and **Server**. When you select **Full Feature** you must configure at least one address mapping set.
	See Chapter 16 Network Address Translation (NAT) for a full discussion on this feature.

Table 160   Menu 11.3.2: Remote Node Network Layer Options

FIELD	DESCRIPTION
NAT Lookup Set	If you select **SUA Only** in the **Network Address Translation** field, it displays **255** and indicates the SMT will use the pre-configured **Set 255** (read only) in menu 15.1.
	If you select **Full Feature** or **None** in the **Network Address Translation** field, it displays **1**, **2** or **3** and indicates the SMT will use the pre-configured **Set 1** in menu 15.1 for the first WAN port, **Set 2** in menu 15.1 for the second WAN port and **Set 3** for the Backup port.
	Refer to the NAT Setup section in Chapter 34 Network Address Translation (NAT) for more information.
Metric	Enter a number from 1 to 15 to set this route's priority among the ZyWALL's routes. The smaller the number, the higher priority the route has.
Private	This parameter determines if the ZyWALL will include the route to this remote node in its RIP broadcasts. If set to **Yes**, this route is kept private and not included in RIP broadcasts. If **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts.
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the **RIP Direction** from **Both**, **None**, **In Only**, **Out Only** and **None**.
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version from **RIP-1**, **RIP-2B** and **RIP-2M**.
Multicast	IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group. The ZyWALL supports both IGMP version 1 (**IGMP-v1**) and version 2 (**IGMP-v2**). Press the [SPACE BAR] to enable IP Multicasting or select **None** to disable it. See Chapter 4 LAN Screens for more information on this feature.
Once you have completed filling in **Menu 11.3.2 Remote Node Network Layer Options**, press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration and return to menu 11.3, or press [ESC] at any time to cancel.	

27.9 Editing Login Script

For some remote gateways, text login is required before PPP negotiation is started. The ZyWALL provides a script facility for this purpose. The script has six programmable sets; each set is composed of an 'Expect' string and a 'Send' string. After matching a message from the server to the 'Expect' field, the ZyWALL returns the set's 'Send' string to the server.

For instance, a typical login sequence starts with the server printing a banner, a login prompt for you to enter the user name and a password prompt to enter the password:

```
Welcome to Acme, Inc.
Login: myLogin
Password:
```

To handle the first prompt, you specify "`ogin:` " as the 'Expect' string and "`myLogin`" as the 'Send' string in set 1. The reason for leaving out the leading "`L`" is to avoid having to know exactly whether it is upper or lower case. Similarly, you specify "`word:` " as the 'Expect' string and your password as the 'Send' string for the second prompt in set 2.

You can use two variables, $USERNAME and $PASSWORD (all UPPER case), to represent the actual user name and password in the script, so they will not show in the clear. They are replaced with the outgoing login name and password in the remote node when the ZyWALL sees them in a 'Send' string. Please note that both variables must been entered exactly as shown. No other characters may appear before or after, either, i.e., they must be used alone in response to login and password prompts.

Please note that the ordering of the sets is significant, i.e., starting from set 1, the ZyWALL will wait until the 'Expect' string is matched before it proceeds to set 2, and so on for the rest of the script. When both the 'Expect' and the 'Send' fields of the current set are empty, the ZyWALL will terminate the script processing and start PPP negotiation. This implies two things: first, the sets must be contiguous; the sets after an empty one are ignored. Second, the last set should match the final message sent by the server. For instance, if the server prints:

```
login successful.
Starting PPP...
```

after you enter the password, then you should create a third set to match the final "PPP..." but without a "Send" string. Otherwise, the ZyWALL will start PPP prematurely right after sending your password to the server.

If there are errors in the script and it gets stuck at a set for longer than the "Dial Timeout" in menu 2 (default 60 seconds), the ZyWALL will timeout and drop the line. To debug a script, go to Menu 24.4 to initiate a manual call and watch the trace display to see if the sequence of messages and prompts from the server differs from what you expect.

Figure 241 Menu 11.3.3: Remote Node Script

```
                  Menu 11.3.3 - Remote Node Script

           Active= No

           Set 1:                                Set 5:
             Expect=                               Expect=
             Send=                                 Send=
           Set 2:                                Set 6:
             Expect=                               Expect=
             Send=                                 Send=
           Set 3:
             Expect=
             Send=
           Set 4:
             Expect=
             Send=

         Enter here to CONFIRM or ESC to CANCEL:
```

The following table describes the fields in this menu.

Table 161 Menu 11.3.3: Remote Node Script

FIELD	DESCRIPTION
Active	Press [SPACE BAR] and then [ENTER] to select either **Yes** to enable the AT strings or **No** to disable them.
Set 1-6: Expect	Enter an Expect string to match. After matching the Expect string, the ZyWALL returns the string in the **Send** field.
Set 1-6: Send	Enter a string to send out after the Expect string is matched.

27.10 Remote Node Filter

Move the cursor to the field **Edit Filter Sets** in menu 11.3, and then press [SPACE BAR] to set the value to **Yes**. Press [ENTER] to open **Menu 11.3.4** - **Remote Node Filter**.

Use menu 11.3.4 to specify the filter set(s) to apply to the incoming and outgoing traffic between this remote node and the ZyWALL to prevent certain packets from triggering calls. You can specify up to four filter sets separated by commas, for example, 1, 5, 9, 12, in each filter field. Note that spaces are accepted in this field. Please refer to Chapter 36 Filter Configuration for more information on defining the filters.

Figure 242   Menu 11.3.4: Remote Node Filter

```
                    Menu 11.3.4 - Remote Node Filter

            Input Filter Sets:
              protocol filters=
                 device filters=
            Output Filter Sets:
              protocol filters=
                 device filters=
            Call Filter Sets:
              protocol filters=
                 device filters=



                   Enter here to CONFIRM or ESC to CANCEL:
```

C HAPTER 28
LAN Setup

This chapter describes how to configure the LAN using **Menu 3 - LAN Setup**.

28.1 Introduction to LAN Setup

This chapter describes how to configure the ZyWALL for LAN and wireless LAN connections.

28.2 Accessing the LAN Menus

From the main menu, enter 3 to open **Menu 3 - LAN Setup**.

Figure 243 Menu 3: LAN Setup

```
                    Menu 3 - LAN Setup

              1. LAN Port Filter Setup
              2. TCP/IP and DHCP Setup


              5. Wireless LAN Setup




                    Enter Menu Selection Number:
```
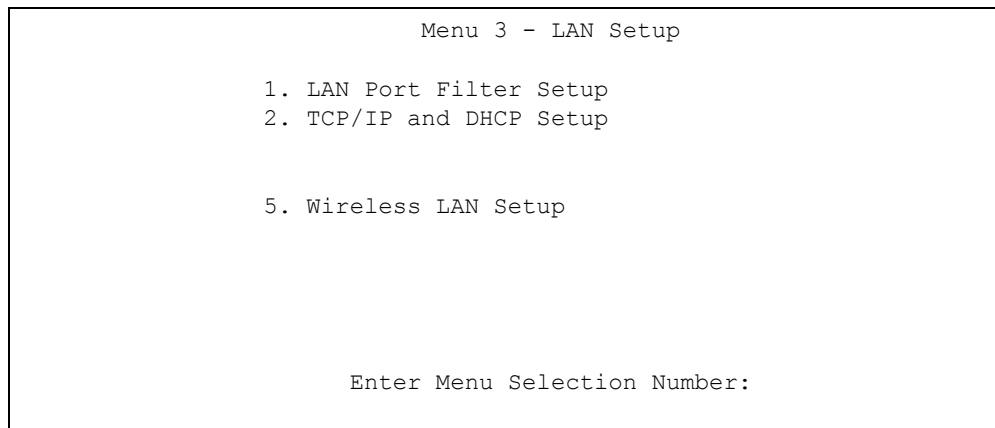
28.3 LAN Port Filter Setup

This menu allows you to specify the filter sets that you wish to apply to the LAN traffic. You seldom need to filter the LAN traffic, however, the filter sets may be useful to block certain packets, reduce traffic and prevent security breaches.

Figure 244 Menu 3.1: LAN Port Filter Setup

```
              Menu 3.1 - LAN Port Filter Setup

         Input Filter Sets:
           protocol filters=
              device filters=
         Output Filter Sets:
           protocol filters=
              device filters=


         Press ENTER to Confirm or ESC to Cancel:
```

28.4 TCP/IP and DHCP Ethernet Setup Menu

From the main menu, enter 3 to open **Menu 3 - LAN Setup** to configure TCP/IP (RFC 1155) and DHCP Ethernet setup.

Figure 245   Menu 3: TCP/IP and DHCP Setup

```
             Menu 3 - LAN Setup

         1. LAN Port Filter Setup
         2. TCP/IP and DHCP Setup


         5. Wireless LAN Setup


                 Enter Menu Selection Number:
```

From menu 3, select the submenu option **TCP/IP and DHCP Setup** and press [ENTER]. The screen now displays **Menu 3.2 - TCP/IP and DHCP Ethernet Setup**, as shown next.

Figure 246 Menu 3.2: TCP/IP and DHCP Ethernet Setup

```
          Menu 3.2 - TCP/IP and DHCP Ethernet Setup


    DHCP= Server                      TCP/IP Setup:
    Client IP Pool:
      Starting Address= 192.168.1.33  IP Address= 192.168.1.1
      Size of Client IP Pool= 128     IP Subnet Mask= 255.255.255.0
                                      RIP Direction= Both
                                        Version= RIP-1
                                      Multicast= None
                                      Edit IP Alias= No


    DHCP Server Address= N/A


                      Press ENTER to Confirm or ESC to Cancel:
```

Follow the instructions in the next table on how to configure the DHCP fields.

Table 162 Menu 3.2: DHCP Ethernet Setup Fields

FIELD	DESCRIPTION
DHCP	This field enables/disables the DHCP server. If set to **Server**, your ZyWALL will act as a DHCP server. If set to **None**, the DHCP server will be disabled. If set to **Relay**, the ZyWALL acts as a surrogate DHCP server and relays requests and responses between the remote server and the clients. When set to **Server**, the following items need to be set:
Client IP Pool:	
Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Size of Client IP Pool	This field specifies the size, or count of the IP address pool.
DHCP Server Address	If **Relay** is selected in the **DHCP** field above, then type the IP address of the actual, remote DHCP server here.

Use the instructions in the following table to configure TCP/IP parameters for the LAN port.

> **Note:** LAN and DMZ IP addresses must be on separate subnets.

Table 163 Menu 3.2: LAN TCP/IP Setup Fields

FIELD	DESCRIPTION
TCP/IP Setup:	
IP Address	Enter the IP address of your ZyWALL in dotted decimal notation

Table 163 Menu 3.2: LAN TCP/IP Setup Fields (continued)

FIELD	DESCRIPTION
IP Subnet Mask	Your ZyWALL will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyWALL.
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP direction. Options are: **Both**, **In Only**, **Out Only** or **None**.
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version. Options are: **RIP-1**, **RIP-2B** or **RIP-2M**.
Multicast	IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group. The ZyWALL supports both IGMP version 1 (**IGMP-v1**) and version 2 (**IGMP-v2**). Press [SPACE BAR] and then [ENTER] to enable IP Multicasting or select **None** (default) to disable it.
Edit IP Alias	The ZyWALL supports three logical LAN interfaces via its single physical Ethernet interface with the ZyWALL itself as the gateway for each LAN network. Press [SPACE BAR] to select **Yes** and then press [ENTER] to display menu 3.2.1
When you have completed this menu, press [ENTER] at the prompt [Press ENTER to Confirm…] to save your configuration, or press [ESC] at any time to cancel.	

28.4.1 IP Alias Setup

IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The ZyWALL supports three logical LAN interfaces via its single physical Ethernet interface with the ZyWALL itself as the gateway for each LAN network.

You must use menu 3.2 to configure the first network. Move the cursor to the **Edit IP Alias** field, press [SPACE BAR] to choose **Yes** and press [ENTER] to configure the second and third network.

Press [ENTER] to open **Menu 3.2.1 - IP Alias Setup**, as shown next.

Figure 247 Menu 3.2.1: IP Alias Setup

```
              Menu 3.2.1 - IP Alias Setup

        IP Alias 1= Yes
          IP Address= 192.168.2.1
          IP Subnet Mask= 255.255.255.0
          RIP Direction= None
            Version= RIP-1
          Incoming protocol filters=
          Outgoing protocol filters=
        IP Alias 2= No
          IP Address= N/A
          IP Subnet Mask= N/A
          RIP Direction= N/A
            Version= N/A
          Incoming protocol filters= N/A
          Outgoing protocol filters= N/A



                Enter here to CONFIRM or ESC to CANCEL:
```

Use the instructions in the following table to configure IP alias parameters.

Table 164 Menu 3.2.1: IP Alias Setup

FIELD	DESCRIPTION
IP Alias 1, 2	Choose **Yes** to configure the LAN network for the ZyWALL.
IP Address	Enter the IP address of your ZyWALL in dotted decimal notation.
IP Subnet Mask	Your ZyWALL will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyWALL.
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP direction. Options are **Both**, **In Only**, **Out Only** or **None**.
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version. Options are **RIP-1**, **RIP-2B** or **RIP-2M**.
Incoming Protocol Filters	Enter the filter set(s) you wish to apply to the incoming traffic between this node and the ZyWALL.
Outgoing Protocol Filters	Enter the filter set(s) you wish to apply to the outgoing traffic between this node and the ZyWALL.
When you have completed this menu, press [ENTER] at the prompt [Press ENTER to Confirm…] to save your configuration, or press [ESC] at any time to cancel.	

28.5 Wireless LAN Setup

Use menu 3.5 to set up your ZyWALL as the wireless access point.

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

From the main menu, enter 3 to open **Menu 3 - LAN Setup** to configure the Wireless LAN setup. To edit the wireless LAN configuration, enter 5 to open **Menu 3.5 - Wireless LAN Setup** as shown next.

Figure 248   Menu 3.5: Wireless LAN Setup

```
              Menu 3.5 - Wireless LAN Setup

              Enable Wireless LAN= No
              ESSID= Wireless
              Hide ESSID= No
              Channel ID= CH06 2437MHz
              RTS Threshold= 2432
              Frag. Threshold= 2432
              WEP= Disable
                Default Key= N/A
                Key1= N/A
                Key2= N/A
                Key3= N/A
                Key4= N/A
              Edit MAC Address Filter= No

              Press ENTER to Confirm or ESC to Cancel:
```

> **Note:** The settings of all client stations on the wireless LAN must match those of the ZyWALL.

Follow the instructions in the next table on how to configure the wireless LAN parameters.

Table 165 Menu 3.5: Wireless LAN Setup

FIELD	DESCRIPTION
Enable Wireless LAN	Press [SPACE BAR] to select **Yes** to turn on the wireless LAN. The wireless LAN is off by default. Configure wireless LAN security features such as Mac filters and 802.1X before you turn on the wireless LAN.
ESSID	(Extended Service Set IDentification) The ESSID identifies the AP to which the wireless stations associate. Wireless stations associating to the Access Point must have the same ESSID. Enter a descriptive name (up to 32 characters) for the wireless LAN.
Hide ESSID	Press [SPACE BAR] to select **Yes** to hide the ESSID in the outgoing beacon frame so a station cannot obtain the ESSID through passive scanning.
Channel ID	This allows you to set the operating frequency/channel depending on your particular region. Use the [SPACE BAR] to select a channel.
RTS Threshold	(Request To Send) The threshold (number of bytes) for enabling RTS/CTS handshake. Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this attribute to be larger than the maximum MSDU (MAC service data unit) size turns off the RTS/CTS handshake. Setting this attribute to zero turns on the RTS/CTS handshake. Enter a value between **0** and **2432**.
Frag. Threshold	The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter a value between **256** and **2432**.
WEP	Select **Disable** to allow wireless stations to communicate with the access points without any data encryption. Select **64-bit WEP** or **128-bit WEP** to enable data encryption.
Default Key	Enter the key number (1 to 4) in this field. Only one key can be enabled at any one time. This key must be the same on the ZyWALL and the wireless stations to communicate.
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the ZyWALL and the wireless stations must use the same WEP key for data transmission. If you chose **64-bit WEP** in the **WEP Encryption** field, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bit WEP** in the **WEP Encryption** field, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). **Note:** Enter "0x" before the key to denote a hexadecimal key. Don't enter "0x" before the key to denote an ASCII key.
Edit MAC Address Filter	Press [SPACE BAR] to select **Yes** and then press [ENTER] to display menu 3.5.1.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

> **Note:** The ZyWALL LAN Ethernet and wireless ports can transparently communicate with each other (transparent bridge).

28.5.1 MAC Address Filter Setup

Your ZyWALL checks the MAC address of the wireless station device against a list of allowed or denied MAC addresses. However, intruders could fake allowed MAC addresses so MAC-based authentication is less secure than EAP authentication.

Follow the steps below to create the MAC address table on your ZyWALL.

1 From the main menu, enter 3 to open **Menu 3 - LAN Setup**.

2 Enter 5 to display **Menu 3.5 - Wireless LAN Setup**.

3 In the **Edit MAC Address Filter** field, press [SPACE BAR] to select **Yes** and press [ENTER]. **Menu 3.5.1 - WLAN MAC Address Filter** displays as shown next.

Figure 249 Menu 3.5.1: WLAN MAC Address Filter

```
             Menu 3.5.1 - WLAN MAC Address Filter

             Active= No
             Filter Action= Allowed Association
             MAC Address Filter
               Address  1= 00:00:00:00:00:00
               Address  2= 00:00:00:00:00:00
               Address  3= 00:00:00:00:00:00
               Address  4= 00:00:00:00:00:00
               Address  5= 00:00:00:00:00:00
               Address  6= 00:00:00:00:00:00
               Address  7= 00:00:00:00:00:00
               Address  8= 00:00:00:00:00:00
               Address  9= 00:00:00:00:00:00
               Address 10= 00:00:00:00:00:00
               Address 11= 00:00:00:00:00:00
               Address 12= 00:00:00:00:00:00

             Enter here to CONFIRM or ESC to CANCEL:
```

The following table describes the fields in this menu.

Table 166 Menu 3.5.1: WLAN MAC Address Filter

FIELD	DESCRIPTION
Active	To enable MAC address filtering, press [SPACE BAR] to select **Yes** and press [ENTER].
Filter Action	Define the filter action for the list of MAC addresses in the MAC address filter table.
	To deny access to the ZyWALL, press [SPACE BAR] to select **Deny Association** and press [ENTER]. MAC addresses not listed will be allowed to access the router.
	The default action, **Allowed Association**, permits association with the ZyWALL. MAC addresses not listed will be denied access to the router.
MAC Address Filter	
Address 1..12	Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the client computers that are allowed or denied access to the ZyWALL in these address fields.
When you have completed this menu, press [ENTER] at the prompt [Press ENTER to Confirm…] to save your configuration, or press [ESC] at any time to cancel.	

CHAPTER 29
Internet Access

This chapter shows you how to configure your ZyWALL for Internet access.

29.1 Introduction to Internet Access Setup

Use information from your ISP along with the instructions in this chapter to set up your ZyWALL to access the Internet. There are three different menu 4 screens depending on whether you chose **Ethernet**, **PPTP** or **PPPoE** Encapsulation. Contact your ISP to determine what encapsulation type you should use.

29.2 Ethernet Encapsulation

If you choose **Ethernet** in menu 4 you will see the next menu.

Figure 250 Menu 4: Internet Access Setup (Ethernet)

```
                Menu 4 - Internet Access Setup

           ISP's Name= WAN_1
           Encapsulation= Ethernet
             Service Type= Standard
             My Login= N/A
             My Password= N/A
             Retype to Confirm= N/A
             Login Server= N/A
             Relogin Every (min)=  N/A
           IP Address Assignment= Dynamic
             IP Address= N/A
             IP Subnet Mask= N/A
             Gateway IP Address= N/A
           Network Address Translation= SUA Only

           Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

Table 167 Menu 4: Internet Access Setup (Ethernet)

FIELD	DESCRIPTION
ISP's Name	This is the descriptive name of your ISP for identification purposes. You can only configure the WAN 2 port in **Menu 11.2 - Remote Node Profile** or in the **WAN WAN 2** screen via the web configurator.
Encapsulation	Press [SPACE BAR] and then press [ENTER] to choose **Ethernet**. The encapsulation method influences your choices for the **IP Address** field.
Service Type	Press [SPACE BAR] and then [ENTER] to select **Standard**, **RR-Toshiba** (RoadRunner Toshiba authentication method), **RR-Manager** (RoadRunner Manager authentication method), **RR-Telstra** or **Telia Login**. Choose a RoadRunner flavor if your ISP is Time Warner's RoadRunner; otherwise choose **Standard**.
Note: DSL users must choose the **Standard** option only. The **My Login**, **My Password** and **Login Server** fields are not applicable in this case.	
My Login	Enter the login name given to you by your ISP.
My Password	Type your password again for confirmation.
Retype to Confirm	Enter your password again to make sure that you have entered is correctly.
Login Server	The ZyWALL will find the RoadRunner Server IP if this field is left blank. If it does not, then you must enter the authentication server IP address.
Relogin Every (min)	This field is available when you select **Telia Login** in the **Service Type** field. The Telia server logs the ZyWALL out if the ZyWALL does not log in periodically. Type the number of minutes from 1 to 59 (30 recommended) for the ZyWALL to wait between logins.
IP Address Assignment	If your ISP did not assign you a fixed IP address, press [SPACE BAR] and then [ENTER] to select **Dynamic**, otherwise select **Static** and enter the IP address and subnet mask in the following fields.
IP Address	Enter the (fixed) IP address assigned to you by your ISP (static IP address assignment is selected in the previous field).
IP Subnet Mask	Enter the subnet mask associated with your static IP.
Gateway IP Address	Enter the gateway IP address associated with your static IP.
Network Address Translation	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet). Choose **None** to disable NAT. Choose **SUA Only** if you have a single public IP address. SUA (Single User Account) is a subset of NAT that supports two types of mapping: **Many-to-One** and **Server**. Choose **Full Feature** if you have multiple public IP addresses. **Full Feature** mapping types include: **One-to-One**, **Many-to-One** (SUA/PAT), **Many-to-Many Overload**, **Many- One-to-One** and **Server**. When you select **Full Feature** you must configure at least one address mapping set! Please see Chapter 16 Network Address Translation (NAT) for a more detailed discussion on the Network Address Translation feature.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

29.3 Configuring the PPTP Client

> **Note:** The ZyWALL supports only one PPTP server connection at any given time.

To configure a PPTP client, you must configure the **My Login** and **Password** fields for a PPP connection and the PPTP parameters for a PPTP connection.

After configuring **My Login** and **Password** for PPP connection, press [SPACE BAR] and then [ENTER] in the **Encapsulation** field in **Menu 4 -Internet Access Setup** to choose **PPTP** as your encapsulation option. This brings up the following screen.

Figure 251   Internet Access Setup (PPTP)

```
             Menu 4 - Internet Access Setup

        ISP's Name= WAN_1
        Encapsulation= PPTP
          Service Type= N/A
          My Login=
          My Password= ********
          Retype to Confirm= ********
          Idle Timeout= 100

        IP Address Assignment= Dynamic
          IP Address= N/A
          IP Subnet Mask= N/A
          Gateway IP Address= N/A
        Network Address Translation= SUA Only

        Press ENTER to Confirm or ESC to Cancel:
```

The following table contains instructions about the new fields when you choose **PPTP** in the **Encapsulation** field in menu 4.

Table 168   New Fields in Menu 4 (PPTP) Screen

FIELD	DESCRIPTION
Encapsulation	Press [SPACE BAR] and then press [ENTER] to choose **PPTP**. The encapsulation method influences your choices for the **IP Address** field.
Idle Timeout	This value specifies the time, in seconds, that elapses before the ZyWALL automatically disconnects from the PPTP server.

29.4 Configuring the PPPoE Client

If you enable PPPoE in menu 4, you will see the next screen. For more information on PPPoE, please see Appendix D PPPoE.

```
          Menu 4 - Internet Access Setup

ISP's Name= WAN_1
Encapsulation= PPPoE
  Service Type= N/A
  My Login=
  My Password= ********
  Retype to Confirm= ********
  Idle Timeout= 100

IP Address Assignment= Dynamic
  IP Address= N/A
  IP Subnet Mask= N/A
  Gateway IP Address= N/A
Network Address Translation= SUA Only

Press ENTER to Confirm or ESC to Cancel:
```

The following table contains instructions about the new fields when you choose **PPPoE** in the **Encapsulation** field in menu 4.

Table 169 New Fields in Menu 4 (PPPoE) screen

FIELD	DESCRIPTION
Encapsulation	Press [SPACE BAR] and then press [ENTER] to choose **PPPoE**. The encapsulation method influences your choices in the **IP Address** field.
Idle Timeout	This value specifies the time in seconds that elapses before the ZyWALL automatically disconnects from the PPPoE server.

If you need a PPPoE service name to identify and reach the PPPoE server, please go to menu 11 and enter the PPPoE service name provided to you in the **Service Name** field.

29.5 Basic Setup Complete

Well done! You have successfully connected, installed and set up your ZyWALL to operate on your network as well as access the Internet.

> **Note:** When the firewall is activated, the default policy allows all communications to the Internet that originate from the LAN, and blocks all traffic to the LAN that originates from the Internet.

You may deactivate the firewall in menu 21.2 or via the ZyWALL embedded web configurator. You may also define additional firewall rules or modify existing ones but please exercise extreme caution in doing so. See the chapters on firewall for more information on the firewall.

CHAPTER 30
DMZ Setup

This chapter describes how to configure the ZyWALL's DMZ using **Menu 5 - DMZ Setup**.

30.1 Configuring DMZ Setup

From the main menu, enter 5 to open **Menu 5 – DMZ Setup**.

Figure 253   Menu 5: DMZ Setup

```
              Menu 5 - DMZ Setup

              1. DMZ Port Filter Setup
              2. TCP/IP Setup

              Enter Menu Selection Number:
```

30.2 DMZ Port Filter Setup

This menu allows you to specify the filter sets that you wish to apply to your public server(s) traffic.

Figure 254   Menu 5.1: DMZ Port Filter Setup

```
              Menu 5.1 - DMZ Port Filter Setup

              Input Filter Sets:
                protocol filters=
                  device filters=
              Output Filter Sets:
                protocol filters=
                  device filters=

              Press ENTER to Confirm or ESC to Cancel:
```

30.3 TCP/IP Setup

For more detailed information about RIP setup, IP Multicast and IP alias, please refer to Chapter 4 LAN Screens.

30.3.1 IP Address

From the main menu, enter 5 to open **Menu 5 - DMZ Setup** to configure TCP/IP (RFC 1155).

Figure 255   Menu 5: TCP/IP Setup

```
              Menu 5 - DMZ Setup

              1. DMZ Port Filter Setup
              2. TCP/IP Setup

                    Enter Menu Selection Number:
```

From menu 5, select the submenu option **2. TCP/IP Setup** and press [ENTER]. The screen now displays **Menu 5.2 - TCP/IP Setup**, as shown next.

Figure 256   Menu 5.2: TCP/IP Setup

```
              Menu 5.2 - TCP/IP Ethernet Setup

              TCP/IP Setup:
                IP Address= 0.0.0.0
                IP Subnet Mask= 0.0.0.0
                RIP Direction= Both
                  Version= RIP-1
                Multicast= None
                Edit IP Alias= No

              Press ENTER to Confirm or ESC to Cancel:
```

The TCP/IP setup fields are the same as the ones in **Menu 3.2 - TCP/IP Ethernet Setup**. Each public server will need a unique IP address. Refer to the TCP/IP and DHCP Ethernet Setup Menu section for information on how to configure these fields.

> **Note:** DMZ and LAN IP addresses must be on separate subnets. You must also configure NAT for the DMZ port (see Chapter 34 Network Address Translation (NAT)) in menus 15.1 and 15.2.

30.3.2 IP Alias Setup

You must use menu 5.2 to configure the first network. Move the cursor to the **Edit IP Alias** field, press [SPACE BAR] to choose **Yes** and press [ENTER] to configure the second and third network.

Pressing [ENTER] opens **Menu 5.2.1 - IP Alias Setup**, as shown next.

Figure 257 Menu 5.2.1: IP Alias Setup

```
                   Menu 5.2.1 - IP Alias Setup

             IP Alias 1= No
               IP Address= N/A
               IP Subnet Mask= N/A
               RIP Direction= N/A
                 Version= N/A
               Incoming protocol filters= N/A
               Outgoing protocol filters= N/A
             IP Alias 2= No
               IP Address= N/A
               IP Subnet Mask= N/A
               RIP Direction= N/A
                 Version= N/A
               Incoming protocol filters= N/A
               Outgoing protocol filters= N/A

             Enter here to CONFIRM or ESC to CANCEL:
```

Refer to Table 164 for instructions on configuring IP alias parameters.

CHAPTER 31
Route Setup

This chapter describes how to configure the ZyWALL's traffic redirect.

31.1 Configuring Route Setup

From the main menu, enter 6 to open **Menu 6 - Route Setup**.

Figure 258   Menu 6: Route Setup

```
          Menu 6 - Route Setup

     1. Route Assessment
     2. Traffic Redirect
     3. Route Failover



            Enter Menu Selection Number:
```

31.2 Route Assessment

This menu allows you to configure traffic redirect properties.

Figure 259   Menu 6.1: Route Assessment

```
          Menu 6.1 - Route Assessment


     Probing WAN 1 Check Point= Yes
       Use Default Gateway as Check Point= Yes
       Check Point= N/A
     Probing WAN 2 Check Point= Yes
       Use Default Gateway as Check Point= Yes
       Check Point= N/A
     Probing Traffic Redirection Check Point= No
       Use Default Gateway as Check Point= N/A
       Check Point= N/A



     Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

Table 170   Menu 6.1: Route Assessment

FIELD	DESCRIPTION
Probing WAN 1/2 Check Point	Press [SPACE BAR] and then press [ENTER] to choose **Yes** to test your ZyWALL's WAN accessibility.
	If you do not select **No** in the **Use Default Gateway as Check Point** field and enter a domain name or IP address of a reliable nearby computer (for example, your ISP's DNS server address) in the **Check Point** field, the ZyWALL will use the default gateway IP address.
Probing Traffic Redirection Check Point	Press [SPACE BAR] and then press [ENTER] to choose **Yes** to test your ZyWALL's traffic redirect connection.
	If you do not select **No** in the **Use Default Gateway as Check Point** field and enter a domain name or IP address of a reliable nearby computer (for example, your ISP's DNS server address) in the **Check Point** field, the ZyWALL will use the default gateway IP address.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

31.3 Traffic Redirect

To configure the parameters for traffic redirect, enter **2** in **Menu 6 - Route Setup** to open **Menu 6.2 - Traffic Redirect** as shown next.

Figure 260   Menu 6.2: Traffic Redirect

```
        Menu 6.2 - Traffic Redirect

     Active= No
     Configuration:
       Backup Gateway IP Address= 0.0.0.0
       Metric= 14




     Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

Table 171   Menu 6.2: Traffic Redirect

FIELD	DESCRIPTION
Active	Press [SPACE BAR] and select Yes (to enable) or No (to disable) traffic redirect setup. The default is No.
Backup Gateway IP Address	Enter the IP address of your backup gateway in dotted decimal notation.
	The ZyWALL automatically forwards traffic to this IP address if the ZyWALL's Internet connection terminates.

Table 171 Menu 6.2: Traffic Redirect

FIELD	DESCRIPTION
Metric	This field sets this route's priority among the routes the ZyWALL uses. Enter a number from 1 to 15 to set this route's priority among the ZyWALL's routes (see the TCP/IP Priority (Metric) section in the Chapter 7 WAN Screens) The smaller the number, the higher priority the route has.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

31.4 Route Failover

This menu allows you to configure how the ZyWALL uses the route assessment ping check function.

Figure 261   Menu 6.3: Route Failover

```
            Menu 6.3 - Route Failover

            Period= 5
            Timeout=: 3
            Fail Tolerance= 3



            Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

Table 172   Menu 6.3: Route Failover

FIELD	DESCRIPTION
Period	Type the number of seconds for the ZyWALL to wait between checks to see if it can connect to the WAN IP address (in the **Check Point** field of menu 6.1) or the default gateway. Allow more time if your destination IP address handles lots of traffic.
Timeout	Type the number of seconds for your ZyWALL to wait for a ping response from the IP address in the **Check Point** field of menu 6.1 before it times out. The WAN connection is considered "down" after the ZyWALL times out the number of times specified in the **Fail Tolerance** field. Use a higher value in this field if your network is busy or congested.
Fail Tolerance	Type the number of times your ZyWALL may attempt and fail to connect to the Internet before traffic is forwarded to the backup gateway.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

C H A P T E R   3 2

Remote Node Setup

This chapter shows you how to configure a remote node.

32.1 Introduction to Remote Node Setup

A remote node is required for placing calls to a remote gateway. A remote node represents both the remote gateway and the network behind it across a WAN connection. Note that when you use menu 4 to set up Internet access, you are actually configuring a remote node. The following describes how to configure **Menu 11.x (where x is 1 or 2) - Remote Node Profile**, **Menu 11.x.2 - Remote Node Network Layer Options** and **Menu 11.x.4 - Remote Node Filter**.

32.2 Remote Node Setup

From the main menu, select menu option 11 to open **Menu 11 - Remote Node Setup** (shown below).

Then enter **1** or **2** to open **Menu 11.x - Remote Node Profile** and configure the setup for your first or second WAN port. Enter **3** to open **Menu 11.3 Remote Node Profile (Backup ISP)** and configure the setup for your Dial Backup port connection (see).

Figure 262   Menu 11: Remote Node Setup

```
              Menu 11 - Remote Node Setup

          1. WAN_1 (ISP, SUA)
          2. WAN_2 (ISP, NAT)
          3. -Dial (BACKUP_ISP, SUA)




              Enter Node # to Edit:
```

32.3 Remote Node Profile Setup

The following explains how to configure the remote node profile menu.

32.3.1 Ethernet Encapsulation

There are three variations of menu 11.x depending on whether you choose **Ethernet Encapsulation**, **PPPoE Encapsulation** or **PPTP Encapsulation**. You must choose the **Ethernet** option when the WAN port is used as a regular Ethernet. The first menu 11.x screen you see is for Ethernet encapsulation shown next.

Figure 263 Menu 11.1: Remote Node Profile for Ethernet Encapsulation

```
        Menu 11.1 - Remote Node Profile

        Rem Node Name= WAN_1                  Route= IP
        Active= Yes

        Encapsulation= Ethernet              Edit IP= No
        Service Type= Standard               Session Options:
                                               Edit Filter Sets= No
        Outgoing:
          My Login= N/A
          My Password= N/A
          Retype to Confirm= N/A
          Server= N/A
          Relogin Every (min)=  N/A


        Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

Table 173 Menu 11.1: Remote Node Profile for Ethernet Encapsulation

FIELD	DESCRIPTION
Rem Node Name	Enter a descriptive name for the remote node. This field can be up to eight characters.
Active	Press [SPACE BAR] and then [ENTER] to select **Yes** (activate remote node) or **No** (deactivate remote node).
Encapsulation	**Ethernet** is the default encapsulation. Press [SPACE BAR] and then [ENTER] to change to **PPPoE** or **PPTP** encapsulation.
Service Type	Press [SPACE BAR] and then [ENTER] to select from **Standard**, **RR-Toshiba** (RoadRunner Toshiba authentication method), **RR-Manager** (RoadRunner Manager authentication method), **RR-Telstra** or **Telia Login**. Choose one of the RoadRunner methods if your ISP is Time Warner's RoadRunner; otherwise choose **Standard**.
Outgoing	
My Login	This field is applicable for **PPPoE** encapsulation only. Enter the login name assigned by your ISP when the ZyWALL calls this remote node. Some ISPs append this field to the **Service Name** field above (e.g., jim@poellc) to access the PPPoE server.
My Password	Enter the password assigned by your ISP when the ZyWALL calls this remote node. Valid for **PPPoE** encapsulation only.

Table 173   Menu 11.1: Remote Node Profile for Ethernet Encapsulation (continued)

FIELD	DESCRIPTION
Retype to Confirm	Type your password again to make sure that you have entered it correctly.
Server	This field is valid only when **RoadRunner** is selected in the **Service Type** field. The ZyWALL will find the RoadRunner Server IP automatically if this field is left blank. If it does not, then you must enter the authentication server IP address here.
Relogin Every (min)	This field is available when you select **Telia Login** in the **Service Type** field. The Telia server logs the ZyWALL out if the ZyWALL does not log in periodically. Type the number of minutes from 1 to 59 (30 recommended) for the ZyWALL to wait between logins.
Route	This field refers to the protocol that will be routed by your ZyWALL – IP is the only option for the ZyWALL.
Edit IP	This field leads to a "hidden" menu. Press [SPACE BAR] to select **Yes** and press [ENTER] to go to **Menu 11.x.2 - Remote Node Network Layer Options**.
Session Options	
Edit Filter Sets	This field leads to another "hidden" menu. Use [SPACE BAR] to select **Yes** and press [ENTER] to open menu 11.x.4 to edit the filter sets. See the Remote Node Filter section for more details.
Once you have configured this menu, press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.	

32.3.2 PPPoE Encapsulation

The ZyWALL supports PPPoE (Point-to-Point Protocol over Ethernet). You can only use PPPoE encapsulation when you're using the ZyWALL with a DSL modem as the WAN device. If you change the Encapsulation to **PPPoE,** then you will see the next screen. Please see Appendix D PPPoE for more information on PPPoE.

Figure 264 Menu 11.1: Remote Node Profile for PPPoE Encapsulation

```
       Menu 11.1 - Remote Node Profile

    Rem Node Name= ChangeMe              Route= IP
    Active= Yes

    Encapsulation= PPPoE                 Edit IP= No
    Service Type= Standard               Telco Option:
    Service Name=                          Allocated Budget(min)= 0
    Outgoing:                              Period(hr)= 0
      My Login=                            Schedules=
      My Password= ********                Nailed-Up Connection= No
      Retype to Confirm= ********
      Authen= CHAP/PAP
                                           Session Options:
                                           Edit Filter Sets= No
                                           Idle Timeout(sec)= 0


                  Press ENTER to Confirm or ESC to Cancel:
```

32.3.2.1 Outgoing Authentication Protocol

Generally speaking, you should employ the strongest authentication protocol possible, for obvious reasons. However, some vendor's implementation includes a specific authentication protocol in the user profile. It will disconnect if the negotiated protocol is different from that in the user profile, even when the negotiated protocol is stronger than specified. If you encounter a case where the peer disconnects right after a successful authentication, please make sure that you specify the correct authentication protocol when connecting to such an implementation.

32.3.2.2 Nailed-Up Connection

A nailed-up connection is a dial-up line where the connection is always up regardless of traffic demand. The ZyWALL does two things when you specify a nailed-up connection. The first is that idle timeout is disabled. The second is that the ZyWALL will try to bring up the connection when turned on and whenever the connection is down. A nailed-up connection can be very expensive for obvious reasons.

Do not specify a nailed-up connection unless your telephone company offers flat-rate service or you need a constant connection and the cost is of no concern.

The following table describes the fields not already described in Table 173.

32.3.2.3 Metric

See the TCP/IP Priority (Metric) section in Chapter 7 WAN Screens for details on the **Metric** field.

Table 174 Fields in Menu 11.1 (PPPoE Encapsulation Specific)

FIELD	DESCRIPTION
Service Name	If you are using **PPPoE** encapsulation, then type the name of your PPPoE service here. Only valid with **PPPoE** encapsulation.
Authen	This field sets the authentication protocol used for outgoing calls. Options for this field are: **CHAP/PAP** - Your ZyWALL will accept either **CHAP** or **PAP** when requested by this remote node. **CHAP** - accept CHAP only. **PAP** - accept PAP only.
Telco Option	
Allocated Budget	The field sets a ceiling for outgoing call time for this remote node. The default for this field is 0 meaning no budget control.
Period(hr)	This field is the time period that the budget should be reset. For example, if we are allowed to call this remote node for a maximum of 10 minutes every hour, then the **Allocated Budget** is (10 minutes) and the **Period(hr)** is 1 (hour).
Schedules	You can apply up to four schedule sets here. For more details please refer to Chapter 43 Call Scheduling.
Nailed-Up Connection	This field specifies if you want to make the connection to this remote node a nailed-up connection. More details are given earlier in this section.
Session Options	
Idle Timeout	Type the length of idle time (when there is no traffic from the ZyWALL to the remote node) in seconds that can elapse before the ZyWALL automatically disconnects the PPPoE connection. This option only applies when the ZyWALL initiates the call.

32.3.3 PPTP Encapsulation

If you change the Encapsulation to **PPTP** in menu 11.1, then you will see the next screen. Please see Appendix E PPTP for information on PPTP.

Figure 265 Menu 11.1: Remote Node Profile for PPTP Encapsulation

```
                   Menu 11.1 - Remote Node Profile

     Rem Node Name= ChangeMe              Route= IP
     Active= Yes

     Encapsulation= PPTP                 Edit IP= No
     Service Type= Standard              Telco Option:
                                           Allocated Budget(min)= 0
     Outgoing:                           Period(hr)= 0
       My Login=                         Schedules=
       My Password= ********             Nailed-Up Connection= No
       Retype to Confirm= ********
       Authen= CHAP/PAP
     PPTP:                               Session Options:
       My IP Addr= 10.0.0.140             Edit Filter Sets= No
       My IP Mask= 255.255.255.0          Idle Timeout(sec)= 100
       Server IP Addr= 10.0.0.138
       Connection ID/Name=

                     Press ENTER to Confirm or ESC to Cancel:
```

The next table shows how to configure fields in menu 11.1 not previously discussed.

Table 175 Menu 11.1: Remote Node Profile for PPTP Encapsulation

FIELD	DESCRIPTION
Encapsulation	Press [SPACE BAR] and then [ENTER] to select **PPTP**. You must also go to menu 11.3 to check the IP Address setting once you have selected the encapsulation method.
My IP Addr	Enter the IP address of the WAN Ethernet port.
My IP Mask	Enter the subnet mask of the WAN Ethernet port.
Server IP Addr	Enter the IP address of the ANT modem.
Connection ID/ Name	Enter the connection ID or connection name in the ANT. It must follow the "c:id" and "n:name" format.
	This field is optional and depends on the requirements of your DSL modem.
Schedules	You can apply up to four schedule sets here. For more details refer to Chapter 43 Call Scheduling.
Nailed-Up Connections	Press [SPACE BAR] and then [ENTER] to select **Yes** if you want to make the connection to this remote node a nailed-up connection.

32.4 Edit IP

Move the cursor to the **Edit IP** field in menu 11.1, then press [SPACE BAR] to select **Yes**. Press [ENTER] to open **Menu 11.1.2 - Remote Node Network Layer Options**.

Figure 266   Menu 11.1.2: Remote Node Network Layer Options for Ethernet Encapsulation

```
          Menu 11.1.2 - Remote Node Network Layer Options

      IP Address Assignment= Dynamic
      Rem IP Addr= N/A
      Rem Subnet Mask= N/A
      My WAN Addr= N/A

      Network Address Translation= SUA Only
      NAT Lookup Set= 255
      Metric= 1
      Private= No
      RIP Direction= None
        Version= N/A
      Multicast= None

       Enter here to CONFIRM or ESC to CANCEL:
```

This menu displays the **My WAN Addr** field for **PPPoE** and **PPTP** encapsulations and **Gateway IP Addr** field for **Ethernet** encapsulation. The following table describes the fields in this menu.

Table 176   Remote Node Network Layer Options Menu Fields

FIELD	DESCRIPTION
IP Address Assignment	If your ISP did not assign you an explicit IP address, press [SPACE BAR] and then [ENTER] to select **Dynamic**; otherwise select **Static** and enter the IP address & subnet mask in the following fields.
(Rem) IP Address	If you have a static IP Assignment, enter the IP address assigned to you by your ISP.
(Rem) IP Subnet Mask	If you have a static IP Assignment, enter the subnet mask assigned to you.
Gateway IP Addr	This field is applicable to **Ethernet** encapsulation only. Enter the gateway IP address assigned to you if you are using a static IP address.
My WAN Addr	This field is applicable to **PPPoE** and **PPTP** encapsulations only. Some implementations, especially the UNIX derivatives, require the WAN link to have a separate IP network number from the LAN and each end must have a unique address within the WAN network number. If this is the case, enter the IP address assigned to the WAN port of your ZyWALL.
Note that this is the address assigned to your local ZyWALL, not the remote router.

Table 176 Remote Node Network Layer Options Menu Fields (continued)

FIELD	DESCRIPTION
Network Address Translation	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet).
	Choose **None** to disable NAT.
	Choose **SUA Only** if you have a single public IP address. SUA (Single User Account) is a subset of NAT that supports two types of mapping: **Many-to-One** and **Server**.
	Choose **Full Feature** if you have multiple public IP addresses. **Full Feature** mapping types include: **One-to-One**, **Many-to-One** (SUA/PAT), **Many-to-Many Overload**, **Many- One-to-One** and **Server**. When you select **Full Feature** you must configure at least one address mapping set.
	See Chapter 16 Network Address Translation (NAT) for a full discussion on this feature.
NAT Lookup Set	If you select **SUA Only** in the **Network Address Translation** field, it displays **255** and indicates the SMT will use the pre-configured **Set 255** (read only) in menu 15.1.
	If you select **Full Feature** or **None** in the **Network Address Translation** field, it displays **1**, **2** or **3** and indicates the SMT will use the pre-configured **Set 1** in menu 15.1 for the first WAN port, **Set 2** in menu 15.1 for the second WAN port and **Set 3** for the Backup port.
	Refer to the NAT Setup section in Chapter 34 Network Address Translation (NAT) for more information.
Metric	Enter a number from 1 to 15 to set this route's priority among the ZyWALL's routes (see the TCP/IP Priority (Metric) section in Chapter 7 WAN Screens) The smaller the number, the higher priority the route has.
Private	This field is valid only for PPTP/PPPoE encapsulation. This parameter determines if the ZyWALL will include the route to this remote node in its RIP broadcasts. If set to **Yes**, this route is kept private and not included in RIP broadcast. If **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts.
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP direction from **Both**/ **None**/**In Only**/**Out Only**. See Chapter 4 LAN Screensfor more information on RIP. The default for RIP on the WAN side is **None**. It is recommended that you do not change this setting.
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version from **RIP-1**/**RIP-2B**/ **RIP-2M** or **None**.
Multicast	IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group. The ZyWALL supports both IGMP version 1 (**IGMP-v1**) and version 2 (**IGMP-v2**). Press [SPACE BAR] to enable IP Multicasting or select **None** to disable it. See Chapter 4 LAN Screens for more information on this feature.
Once you have completed filling in **Menu 11.3 Remote Node Network Layer Options**, press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration and return to menu 11, or press [ESC] at any time to cancel.	

32.5 Remote Node Filter

Move the cursor to the field **Edit Filter Sets** in menu 11.1, and then press [SPACE BAR] to set the value to **Yes**. Press [ENTER] to open **Menu 11.1.4 - Remote Node Filter**.

Use menu 11.1.4 to specify the filter set(s) to apply to the incoming and outgoing traffic between this remote node and the ZyWALL to prevent certain packets from triggering calls. You can specify up to 4 filter sets separated by commas, for example, 1, 5, 9, 12, in each filter field. Note that spaces are accepted in this field. For more information on defining the filters, please refer to Chapter 36 Filter Configuration. For PPPoE or PPTP encapsulation, you have the additional option of specifying remote node call filter sets.

Figure 267 Menu 11.1.4: Remote Node Filter (Ethernet Encapsulation)

```
          Menu 11.1.4 - Remote Node Filter

          Input Filter Sets:
            protocol filters=
               device filters=
          Output Filter Sets:
            protocol filters=
               device filters=


          Enter here to CONFIRM or ESC to CANCEL:
```

Figure 268 Menu 11.1.4: Remote Node Filter (PPPoE or PPTP Encapsulation)

```
          Menu 11.1.4 - Remote Node Filter

          Input Filter Sets:
            protocol filters=
               device filters=
          Output Filter Sets:
            protocol filters=
               device filters=
          Call Filter Sets:
            protocol filters=
               device filters=



          Enter here to CONFIRM or ESC to CANCEL:
```

CHAPTER 33
IP Static Route Setup

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

33.1 IP Static Route Setup

Enter 12 from the main menu. Select one of the IP static routes as shown next to configure IP static routes in menu 12.1.

> **Note:** The first static route entries is for the 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 route name changes from "default" to "-default" after you change the static WAN IP address to a dynamic WAN IP address, indicating the static route is inactive.

Figure 269   Menu 12: IP Static Route Setup

```
                   Menu 12 - IP Static Route Setup


      1. _____     16. _____     31. _____     46. _____
      2. _____     17. _____     32. _____     47. _____
      3. _____     18. _____     33. _____     48. _____
      4. _____     19. _____     34. _____
      5. _____     20. _____     35. _____
      6. _____     21. _____     36. _____
      7. _____     22. _____     37. _____
      8. _____     23. _____     38. _____
      9. _____     24. _____     39. _____
     10. _____     25. _____     40. _____
     11. _____     26. _____     41. _____
     12. _____     27. _____     42. _____
     13. _____     28. _____     43. _____
     14. _____     29. _____     44. _____
     15. _____     30. _____     45. _____



      Enter selection number:
```

Now, enter the index number of the static route that you want to configure.

Figure 270 Menu 12. 1: Edit IP Static Route

```
          Menu 12.1 - Edit IP Static Route

          Route #: 2
          Route Name= ?
          Active= No
          Destination IP Address= ?
          IP Subnet Mask= ?
          Gateway IP Address= ?
          Metric= 2
          Private= No



          Press ENTER to CONFIRM or ESC to CANCEL:
```

`The following table describes the IP Static Route Menu fields.

Table 177 Menu 12. 1: Edit IP Static Route

FIELD	DESCRIPTION
Route #	This is the index number of the static route that you chose in menu 12.
Route Name	Enter a descriptive name for this route. This is for identification purposes only.
Active	This field allows you to activate/deactivate this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask for this destination.
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your ZyWALL that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your ZyWALL; over the WAN, the gateway must be the IP address of one of the remote nodes.
Metric	Enter a number from 1 to 15 to set this route's priority among the ZyWALL's routes (see the TCP/IP Priority (Metric) section in Chapter 7 WAN Screens). The smaller the number, the higher priority the route has.
Private	This parameter determines if the ZyWALL will include the route to this remote node in its RIP broadcasts. If set to **Yes**, this route is kept private and not included in RIP broadcast. If **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts.
Once you have completed filling in this menu, press [ENTER] at the message "Press ENTER to Confirm…" to save your configuration, or press [ESC] to cancel.	

C HAPTER 34
Network Address Translation (NAT)

This chapter discusses how to configure NAT on the ZyWALL.

34.1 Using NAT

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

34.1.1 SUA (Single User Account) Versus NAT

SUA (Single User Account) is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. See the Address Mapping Sets section for a detailed description of the NAT set for SUA. The ZyWALL also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types.

> **Note:** Choose **SUA Only** if you have just one public WAN IP address for your ZyWALL.
> **Note:** Choose **Full Feature** if you have multiple public WAN IP addresses for your ZyWALL.

34.1.2 Applying NAT

You apply NAT via menus 4 or 11.1.2 as displayed next. The next figure shows you how to apply NAT for Internet access in menu 4. Enter 4 from the main menu to go to **Menu 4 - Internet Access Setup**.

Figure 271   Menu 4: Applying NAT for Internet Access

```
           Menu 4 - Internet Access Setup

          ISP's Name= ChangeMe
          Encapsulation= Ethernet
            Service Type= Standard
            My Login= N/A
            My Password= N/A
            Retype to Confirm= N/A
            Login Server= N/A
            Relogin Every (min)=  N/A
          IP Address Assignment= Dynamic
            IP Address= N/A
            IP Subnet Mask= N/A
            Gateway IP Address= N/A
          Network Address Translation= SUA Only


          Press ENTER to Confirm or ESC to Cancel:
```

The following figure shows how you apply NAT to the remote node in menu 11.1.

1 Enter 11 from the main menu.

2 Enter 1 to open **Menu 11.1 - Remote Node Profile**.

3 Move the cursor to the **Edit IP** field, press [SPACE BAR] to select **Yes** and then press [ENTER] to bring up **Menu 11.1.2 - Remote Node Network Layer Options**.

Figure 272   Menu 11.1.2: Applying NAT to the Remote Node

```
           Menu 11.1.2 - Remote Node Network Layer Options

          IP Address Assignment= Dynamic
          IP Address= N/A
          IP Subnet Mask= N/A
          Gateway IP Addr= N/A

          Network Address Translation= Full Feature
          Metric= 1
          Private= N/A
          RIP Direction= None
            Version= N/A
          Multicast= None


          Enter here to CONFIRM or ESC to CANCEL:
```

The following table describes the fields in this menu.

Table 178 Applying NAT in Menus 4 & 11.1.2

FIELD	DESCRIPTION	OPTIONS
Network Address Translation	When you select this option the SMT will use Address Mapping Set 1 (menu 15.1 - see the Address Mapping Sets section for further discussion). You can configure any of the mapping types described in Chapter 16 Network Address Translation (NAT). Choose **Full Feature** if you have multiple public WAN IP addresses for your ZyWALL. When you select **Full Feature** you must configure at least one address mapping set.	Full Feature
	NAT is disabled when you select this option.	None
	When you select this option the SMT will use Address Mapping Set 255 (menu 15.1 - see the Address Mapping Sets section). Choose **SUA Only** if you have just one public WAN IP address for your ZyWALL.	SUA Only

34.2 NAT Setup

Use the address mapping sets menus and submenus to create the mapping table used to assign global addresses to computers on the LAN and the DMZ. **Set 255** is used for SUA. When you select **Full Feature** in menu 4, menu 11.1.2 or menu 11.2.2, the SMT will use **Set 1** for the first WAN port and **Set 2** for the second WAN port. When you select **SUA Only**, the SMT will use the pre-configured **Set 255** (read only).

The server set is a list of LAN and DMZ servers mapped to external ports. To use this set, a server rule must be set up inside the NAT address mapping set. Please see the section on port forwarding in Chapter 16 Network Address Translation (NAT) for further information on these menus. To configure NAT, enter 15 from the main menu to bring up the following screen.

Figure 273   Menu 15: NAT Setup

```
                    Menu 15 - NAT Setup

                  1. Address Mapping Sets
                  2. Port Forwarding Setup
                  3. Trigger Port Setup




            Enter Menu Selection Number:
```

> **Note:** Configure DMZ and LAN IP addresses in NAT menus 15.1 and 15.2. DMZ IP addresses must be on subnets separate from LAN IP addresses.

34.2.1 Address Mapping Sets

Enter 1 to bring up **Menu 15.1 - Address Mapping Sets.**

Figure 274   Menu 15.1: Address Mapping Sets

```
              Menu 15.1 - Address Mapping Sets

                    1. NAT_SET
                    2.
                  255. SUA (read only)




              Enter Menu Selection Number:
```

34.2.1.1 SUA Address Mapping Set

Enter 255 to display the next screen (see also the SUA (Single User Account) Versus NAT section). The fields in this menu cannot be changed.

Figure 275   Menu 15.1.255: SUA Address Mapping Rules

```
           Menu 15.1.1 - Address Mapping Rules

   Set Name= SUA

   Idx  Local Start IP   Local End IP    Global Start IP  Global End IP  Type
   ---  ---------------  ---------------  ---------------  -------------  --
   1.  0.0.0.0          255.255.255.255  0.0.0.0                          M-1
   2.                                    0.0.0.0                          Server
   3.
   4.
   5.
   6.
   7.
   8.
   9.
   10.

         Press ENTER to Confirm or ESC to Cancel:
```

The following table explains the fields in this menu.

> **Note:** Menu 15.1.255 is read-only.

Table 179   SUA Address Mapping Rules

FIELD	DESCRIPTION
Set Name	This is the name of the set you selected in menu 15.1 or enter the name of a new set you want to create.
Idx	This is the index or rule number.
Local Start IP	**Local Start IP** is the starting local IP address (ILA).
Local End IP	**Local End IP** is the ending local IP address (ILA). If the rule is for all local IPs, then the start IP is 0.0.0.0 and the end IP is 255.255.255.255.
Global Start IP	This is the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the **Global Start IP**.
Global End IP	This is the ending global IP address (IGA).
Type	These are the mapping types discussed above. **Server** allows us to specify multiple servers of different types behind NAT to this machine. See later for some examples.
Once you have finished configuring a rule in this menu, press [ENTER] at the message "Press ENTER to Confirm…" to save your configuration, or press [ESC] to cancel.

34.2.1.2 User-Defined Address Mapping Sets

Now look at option 1 in menu 15.1. Enter 1 to bring up this menu. Look at the differences from the previous menu. Note the extra **Action** and **Select Rule** fields mean you can configure rules in this screen. Note also that the [?] in the **Set Name** field means that this is a required field and you must enter a name for the set.

> **Note:** The entire set will be deleted if you leave the Set Name field blank and press [ENTER] at the bottom of the screen.

Figure 276 Menu 15.1.1: First Set

```
          Menu 15.1.1 - Address Mapping Rules

  Set Name= NAT_SET

  Idx  Local Start IP   Local End IP   Global Start IP  Global End IP  Type
  ---  ---------------  -------------  ---------------  -------------  ----
   1.
   2.
   3.
   4.
   5.
   6.
   7.
   8.
   9.
  10.

        Action= None           Select Rule= N/A
        Press ENTER to Confirm or ESC to Cancel:
```

> **Note:** The Type, Local and Global Start/End IPs are configured in menu 15.1.1.1 (described later) and the values are displayed here.

34.2.1.3 Ordering Your Rules

Ordering your rules is important because the ZyWALL applies the rules in the order that you specify. When a rule matches the current packet, the ZyWALL takes the corresponding action and the remaining rules are ignored. If there are any empty rules before your new configured rule, your configured rule will be pushed up by that number of empty rules. For example, if you have already configured rules 1 to 6 in your current set and now you configure rule number 9. In the set summary screen, the new rule will be rule 7, not 9.

Now if you delete rule 4, rules 5 to 7 will be pushed up by 1 rule, so as old rule 5 becomes rule 4, old rule 6 becomes rule 5 and old rule 7 becomes rule 6.

Table 180 Fields in Menu 15.1.1

FIELD	DESCRIPTION
Set Name	Enter a name for this set of rules. This is a required field. If this field is left blank, the entire set will be deleted.
Action	The default is **Edit**. **Edit** means you want to edit a selected rule (see following field). **Insert Before** means to insert a rule before the rule selected. The rules after the selected rule will then be moved down by one rule. **Delete** means to delete the selected rule and then all the rules after the selected one will be advanced one rule. **None** disables the **Select Rule** item.
Select Rule	When you choose **Edit**, **Insert Before** or **Delete** in the previous field the cursor jumps to this field to allow you to select the rule to apply the action in question.

![Note icon] **Note:** You must press [ENTER] at the bottom of the screen to save the whole set. You must do this again if you make any changes to the set – including deleting a rule. No changes to the set take place until this action is taken.

Selecting **Edit** in the **Action** field and then selecting a rule brings up the following menu, **Menu 15.1.1.1 - Address Mapping Rule** in which you can edit an individual rule and configure the **Type**, **Local** and **Global Start/End IPs**.

![Note icon] **Note:** An IP End address must be numerically greater than its corresponding IP Start address.

Figure 277 Menu 15.1.1.1: Editing/Configuring an Individual Rule in a Set

```
          Menu 15.1.1.1 Address Mapping Rule

               Type= One-to-One

               Local IP:
                 Start=
                 End  = N/A

               Global IP:
                 Start=
                 End  = N/A


          Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

Table 181 Menu 15.1.1.1: Editing/Configuring an Individual Rule in a Set

FIELD	DESCRIPTION
Type	Press [SPACE BAR] and then [ENTER] to select from a total of five types. These are the mapping types discussed in Chapter 16 Network Address Translation (NAT). **Server** allows you to specify multiple servers of different types behind NAT to this computer. See the Example 3: Multiple Public IP Addresses With Inside Servers section for an example.
Local IP	Only local IP fields are **N/A** for server; Global IP fields MUST be set for **Server**.
Start	Enter the starting local IP address (ILA).
End	Enter the ending local IP address (ILA). If the rule is for all local IPs, then put the Start IP as 0.0.0.0 and the End IP as 255.255.255.255. This field is **N/A** for One-to-One and Server types.
Global IP	
Start	Enter the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the **Global IP Start**. Note that **Global IP Start** can be set to 0.0.0.0 only if the types are **Many-to-One** or **Server**.

Table 181 Menu 15.1.1.1: Editing/Configuring an Individual Rule in a Set

FIELD	DESCRIPTION
End	Enter the ending global IP address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server types**.
Once you have finished configuring a rule in this menu, press [ENTER] at the message "Press ENTER to Confirm…" to save your configuration, or press [ESC] to cancel.	

34.3 Configuring a Server behind NAT

> If you do not assign a **Default Server** IP address, the ZyWALL discards all packets received for ports that are not specified here or in the remote management setup.

Follow these steps to configure a server behind NAT:

1 Enter 15 in the main menu to go to **Menu 15 - NAT Setup.**

2 Enter 2 to open **Menu 15.2 - NAT Server Sets**.

Figure 278   Menu 15.2: NAT Server Sets

```
          Menu 15.2 - NAT Server Sets

      1. Server Set 1
      2. Server Set 2



          Enter Set Number to Edit:
```

3 Enter 1 to go to **Menu 15.2.1 - NAT Server Setup** and configure the address mapping rules for the WAN 1 port.

4 Select **Edit Rule** in the **Select Command** field; type the index number of the NAT server you want to configure in the **Select Rule** field and press [ENTER] to open **Menu 15.2.1.2 - NAT Server Configuration** (see the next figure).

Figure 279 15.2.1.2: NAT Server Configuration

```
         15.2.1.1 - NAT Server Configuration

         Wan= 1                          Index= 1

    -------------------------------------------------

         Name= 1

         Active= Yes

         Start port= 21                  End port= 25

         IP Address= 192.168.1.33

    Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this screen.

Table 182 15.2.1.2: NAT Server Configuration

FIELD	DESCRIPTION
WAN	The ZyWALL has two WAN ports. You can configure port forwarding and trigger port rules for the first WAN port and separate sets of rules for the second WAN port.
	This is the WAN port (server set) you select in menu 15.2.
Index	This is the index number of an individual port forwarding server entry.
Name	Enter a name to identify this port-forwarding rule.
Active	Press [SPACE BAR] and then [ENTER] to select **Yes** to enable the NAT server entry.
Start Port	Enter a port number in the **Start Port** field. To forward only one port, enter it again in the **End Port** field. To specify a range of ports, enter the last port to be forwarded in the **End Port** field.
End Port	
IP Address	Enter the inside IP address of the server.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

5 Enter a port number in the **Start Port** field. To forward only one port, enter it again in the **End Port** field. To specify a range of ports, enter the last port to be forwarded in the **End Port** field.

6 Enter the inside IP address of the server in the **IP Address** field. In the following figure, you have a computer acting as an FTP, Telnet and SMTP server (ports 21, 23 and 25) at 192.168.1.33.

7 Press [ENTER] at the "Press ENTER to confirm …" prompt to save your configuration after you define all the servers or press [ESC] at any time to cancel.

Note: The last port forwarding rule is reserved for Roadrunner services. The rule is activated only when you set the **WAN Encapsulation** to **Ethernet** and the **Service Type** to something other than **Standard.**

Figure 280 Menu 15.2: NAT Server Setup

```
                Menu 15.2.1 - NAT Server Setup

           Default Server: 0.0.0.0
     Rule  Act.    Start Port   End Port    IP Address
     ---------------------------------------------------
     001   Yes     21           25          192.168.1.33
     002   No      0            0           0.0.0.0
     003   No      0            0           0.0.0.0
     004   No      0            0           0.0.0.0
     005   No      0            0           0.0.0.0
     006   No      0            0           0.0.0.0
     007   No      0            0           0.0.0.0
     008   No      0            0           0.0.0.0
     009   No      0            0           0.0.0.0
     010   No      0            0           0.0.0.0


     Select Command= None          Select Rule= N/A
          Press ENTER to Confirm or ESC to Cancel:
```

You assign the private network IP addresses. The NAT network appears as a single host on the Internet. A is the FTP/Telnet/SMTP server.

Figure 281 Server Behind NAT Example
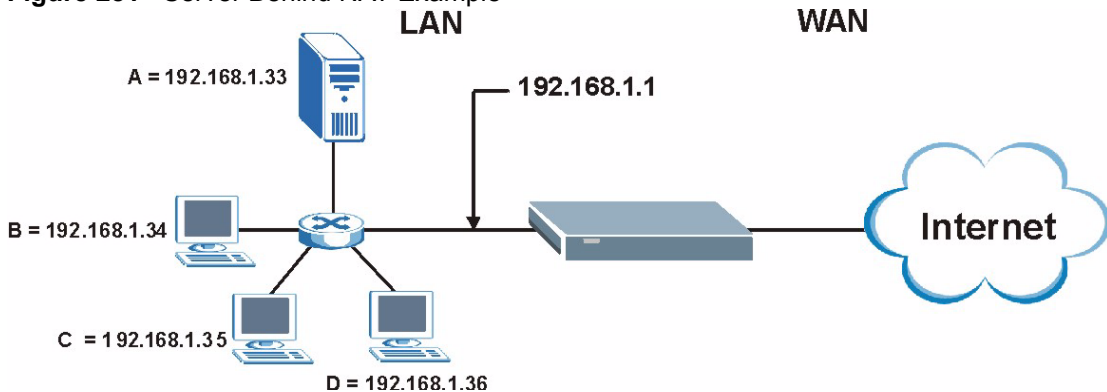
34.4 General NAT Examples

The following are some examples of NAT configuration.

34.4.1 Internet Access Only

In the following Internet access example, you only need one rule where all your ILAs (Inside Local addresses) map to one dynamic IGA (Inside Global Address) assigned by your ISP.

Figure 282   NAT Example 1
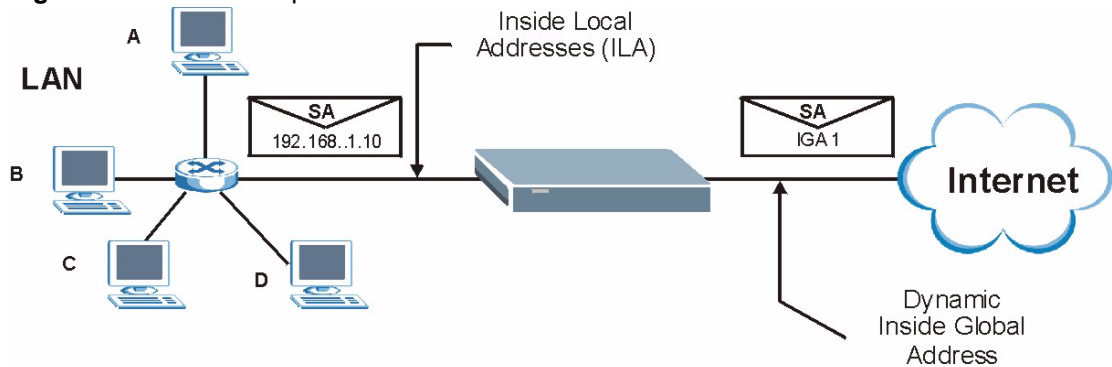
Figure 283   Menu 4: Internet Access & NAT Example

```
            Menu 4 - Internet Access Setup

            ISP's Name= ChangeMe
            Encapsulation= Ethernet
              Service Type= Standard
              My Login= N/A
              My Password= N/A
              Retype to Confirm= N/A
              Login Server= N/A
              Relogin Every (min)=  N/A
            IP Address Assignment= Dynamic
              IP Address= N/A
              IP Subnet Mask= N/A
              Gateway IP Address= N/A
            Network Address Translation= SUA Only


            Press ENTER to Confirm or ESC to Cancel:
```

From menu 4 shown above, simply choose the **SUA Only** option from the **Network Address Translation** field. This is the Many-to-One mapping discussed in the General NAT Examples section. The **SUA Only** read-only option from the **Network Address Translation** field in menus 4 and 11.3 is specifically pre-configured to handle this case.

34.4.2 Example 2: Internet Access with an Default Server

Figure 284 NAT Example 2
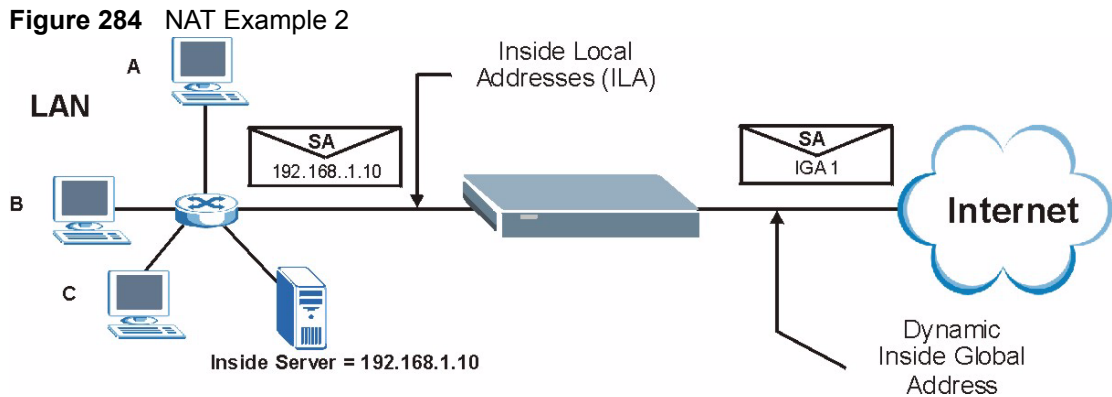
In this case, you do exactly as above (use the convenient pre-configured **SUA Only** set) and also go to menu 15.2.1 to specify the **Default Server** behind the NAT as shown in the next figure.

Figure 285 Menu 15.2.1: Specifying an Inside Server

```
              Menu 15.2.1 - NAT Server Setup

              Default Server: 192.168.1.10
        Rule  Act.   Start Port   End Port    IP Address
        ------------------------------------------------------
        001   Yes    21           25          192.168.1.33
        002   No     0            0           0.0.0.0
        003   No     0            0           0.0.0.0
        004   No     0            0           0.0.0.0
        005   No     0            0           0.0.0.0
        006   No     0            0           0.0.0.0
        007   No     0            0           0.0.0.0
        008   No     0            0           0.0.0.0
        009   No     0            0           0.0.0.0
        010   No     0            0           0.0.0.0



        Select Command= None          Select Rule= N/A
             Press ENTER to Confirm or ESC to Cancel:
```

34.4.3 Example 3: Multiple Public IP Addresses With Inside Servers

In this example, there are 3 IGAs from our ISP. There are many departments but two have their own FTP server. All departments share the same router. The example will reserve one IGA for each department with an FTP server and all departments use the other IGA. Map the FTP servers to the first two IGAs and the other LAN traffic to the remaining IGA. Map the third IGA to an inside web server and mail server. Four rules need to be configured, two bi-directional and two uni-directional as follows.

1 Map the first IGA to the first inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).

2 Map the second IGA to our second inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).

3 Map the other outgoing LAN traffic to IGA3 (**Many : 1** mapping).

4 You also map your third IGA to the web server and mail server on the LAN. Type **Server** allows you to specify multiple servers, of different types, to other computers behind NAT on the LAN.

The example situation looks somewhat like this:

Figure 286   NAT Example 3
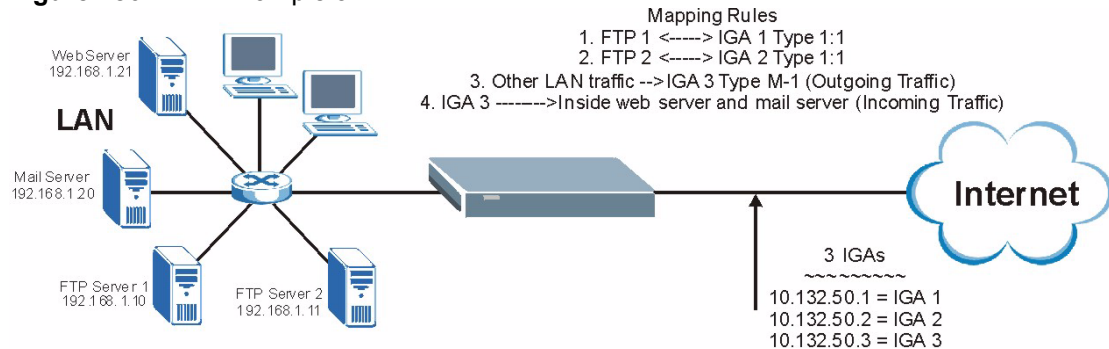
1 In this case you need to configure Address Mapping Set 1 from **Menu 15.1 - Address Mapping Sets**. Therefore you must choose the **Full Feature** option from the **Network Address Translation** field (in menu 4 or menu 11.3) in Figure 287.

2 Then enter 15 from the main menu.

3 Enter 1 to configure the Address Mapping Sets.

4 Enter 1 to begin configuring this new set. Enter a Set Name, choose the **Edit Action** and then enter 1 for the **Select Rule** field. Press **[ENTER]** to confirm.

5 Select **Type** as **One-to-One** (direct mapping for packets going both ways), and enter the local **Start IP** as 192.168.1.10 (the IP address of FTP Server 1), the global **Start IP** as 10.132.50.1 (our first IGA). (See Figure 288*).*

6 Repeat the previous step for rules 2 to 4 as outlined above.

7 When finished, menu 15.1.1 should look like as shown in Figure 289.

Figure 287 Example 3: Menu 11.1.2

```
              Menu 11.1.2 - Remote Node Network Layer Options

                     IP Address Assignment= Dynamic
                     IP Address= N/A
                     IP Subnet Mask= N/A
                     Gateway IP Addr= N/A

                     Network Address Translation= SUA Only
                     Metric= 2
                     Private=
                     RIP Direction= None
                       Version= N/A
                     Multicast= None


            Enter here to CONFIRM or ESC to CANCEL:
```

The following figure shows how to configure the first rule.

Figure 288 Example 3: Menu 15.1.1.1

```
            Menu 15.1.1.1 Address Mapping Rule

                 Type= One-to-One

                 Local IP:
                   Start= 192.168.1.10
                   End  = N/A

                 Global IP:
                   Start= 10.132.50.1
                   End  = N/A

                 Server Mapping Set= N/A

        Press ENTER to Confirm or ESC to Cancel:
```

Figure 289   Example 3: Final Menu 15.1.1

```
Menu 15.1.1 - Address Mapping Rules

Set Name= Example3

Idx  Local Start IP   Local End IP    Global Start IP  Global End IP    Type
---  ---------------  --------------  ---------------  ---------------  ---
 1. 192.168.1.10                      10.132.50.1                       1-1
 2  192.168.1.11                      10.132.50.2                       1-1
 3. 0.0.0.0           255.255.255.255 10.132.50.3                       M-1
 4.                                   10.132.50.3                       Server
 5.
 6.
 7.
 8.
 9.
10.

Action= Edit         Select Rule=

Press ENTER to Confirm or ESC to Cancel:
```

Now configure the IGA3 to map to our web server and mail server on the LAN.

1 Enter 15 from the main menu.

2 Enter 2 to go to **Menu 15.2 - NAT Server Sets**.

3 Now enter 1 from this menu and configure it as shown in Figure 290.

Figure 290   Example 3: Menu 15.2.1

```
              Menu 15.2.1 - NAT Server Setup

          Default Server: 0.0.0.0
    Rule   Act.   Start Port   End Port   IP Address
    ---------------------------------------------------
    001    Yes    80           80         192.168.1.21
    002    Yes    25           25         192.168.1.20
    003    No     0            0          0.0.0.0
    004    No     0            0          0.0.0.0
    005    No     0            0          0.0.0.0
    006    No     0            0          0.0.0.0
    007    No     0            0          0.0.0.0
    008    No     0            0          0.0.0.0
    009    No     0            0          0.0.0.0
    010    No     0            0          0.0.0.0



    Select Command= None          Select Rule= N/A
         Press ENTER to Confirm or ESC to Cancel:
```

34.4.4 Example 4: NAT Unfriendly Application Programs

Some applications do not support NAT Mapping using TCP or UDP port address translation. In this case it is better to use **Many-One-to-One** mapping as port numbers do *not* change for **Many-One-to-One** (and **One-to-One**) NAT mapping types. The following figure illustrates this.

Figure 291   NAT Example 4
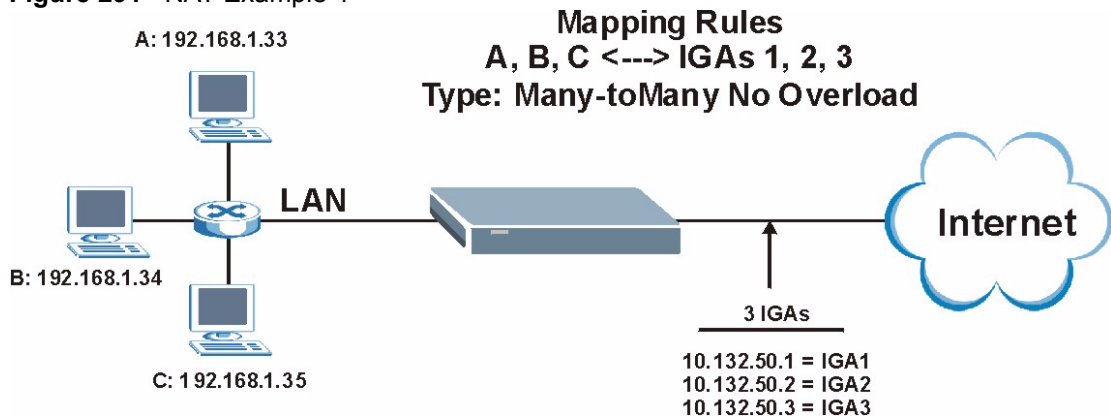
> **Note:** Other applications such as some gaming programs are NAT unfriendly because they embed addressing information in the data stream. These applications won't work through NAT even when using **One-to-One** and **Many-One-to-One** mapping types.

Follow the steps outlined in example 3 above to configure these two menus as follows.

Figure 292 Example 4: Menu 15.1.1.1: Address Mapping Rule

```
                 Menu 15.1.1.1 Address Mapping Rule

                   Type= Many-One-to-One

                   Local IP:
                     Start= 192.168.1.10
                     End  = 192.168.1.12

                   Global IP:
                     Start= 10.132.50.1
                     End  = 10.132.50.3

           Press ENTER to Confirm or ESC to Cancel:
```

After you've configured your rule, you should be able to check the settings in menu 15.1.1 as shown next.

Figure 293 Example 4: Menu 15.1.1: Address Mapping Rules

```
                     Menu 15.1.1 - Address Mapping Rules

     Set Name= Example4

  Idx  Local Start IP    Local End IP    Global Start IP   Global End IP   Type
  ---  ---------------   -------------   ---------------   -------------   -----
   1.  192.168.1.10      192.168.1.12    10.132.50.1       10.132.50.3     M-1-1
   2.
   3.
   4.
   5.
   6.
   7.
   8.
   9.
  10.

          Action= Edit         Select Rule=

          Press ENTER to Confirm or ESC to Cancel:
```

34.5 Trigger Port Forwarding

Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address.

Trigger port forwarding solves this problem by allowing computers on the LAN to dynamically take turns using the service. The ZyWALL records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a "trigger" port). When the ZyWALL's WAN port receives a response with a specific port number and protocol ("incoming" port), the ZyWALL forwards the traffic to the LAN IP address of the computer that sent the request. After that computer's connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

34.5.1 Two Points To Remember About Trigger Ports

1 Trigger events only happen on data that is going coming from inside the ZyWALL and going to the outside.

2 If an application needs a continuous data stream, that port (range) will be tied up so that another computer on the LAN can't trigger it.

> **Note:** Only one LAN computer can use a trigger port (range) at a time.

Enter 3 in menu 15 to display **Menu 15.3 - Trigger Ports**, and enter 1 or 2 to go to **Menu 15.3.x (where x is 1 or 2) - Trigger Port Setup** and configure trigger port rules for the first or second WAN port, shown next.

Figure 294 Menu 15.3.1: Trigger Port Setup

```
             Menu 15.3.1 - Trigger Port Setup

                        Incoming                 Trigger
    Rule     Name      Start Port  End Port   Start Port  End Port
    ---------------------------------------------------------------
     1.   Real Audio      6970       7170        7070        7070
     2.                      0          0           0           0
     3.                      0          0           0           0
     4.                      0          0           0           0
     5.                      0          0           0           0
     6.                      0          0           0           0
     7.                      0          0           0           0
     8.                      0          0           0           0
     9.                      0          0           0           0
    10.                      0          0           0           0
    11.                      0          0           0           0
    12.                      0          0           0           0


                 Press ENTER to Confirm or ESC to Cancel:

    HTTP:80  FTP:21  Telnet:23  SMTP:25  POP3:110  PPTP:1723
```

The following table describes the fields in this menu.

Table 183 Menu 15.3: Trigger Port Setup

FIELD	DESCRIPTION
Rule	This is the rule index number.
Name	Enter a unique name for identification purposes. You may enter up to 15 characters in this field. All characters are permitted - including spaces.
Incoming	Incoming is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The ZyWALL forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.
Start Port	Enter a port number or the starting port number in a range of port numbers.
End Port	Enter a port number or the ending port number in a range of port numbers.
Trigger	The trigger port is a port (or a range of ports) that causes (or triggers) the ZyWALL to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Start Port	Enter a port number or the starting port number in a range of port numbers.
End Port	Enter a port number or the ending port number in a range of port numbers.
Press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.	

Chapter 34 Network Address Translation (NAT)

CHAPTER 35
Introducing the ZyWALL Firewall

This chapter shows you how to get started with the ZyWALL firewall.

35.1 Using ZyWALL SMT Menus

From the main menu enter 21 to go to **Menu 21 - Filter Set and Firewall Configuration** to display the screen shown next.

Figure 295   Menu 21: Filter and Firewall Setup

```
              Menu 21 - Filter and Firewall Setup

                      1. Filter Setup
                      2. Firewall Setup


              Enter Menu Selection Number:
```

35.1.1 Activating the Firewall

Enter option 2 in this menu to bring up the following screen. Press [SPACE BAR] and then [ENTER] to select **Yes** in the **Active** field to activate the firewall. The firewall must be active to protect against Denial of Service (DoS) attacks. Use the web configurator to configure firewall rules.

Figure 296   Menu 21.2: Firewall Setup

```
              Menu 21.2 - Firewall Setup

  The firewall protects against Denial of Service (DoS) attacks when it is
  active.

  Your network is vulnerable to attacks when the firewall is turned off.

  Refer to the User's Guide for details about the firewall default
  policies.

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

  Active: Yes

  You can use the Web Configurator to configure the firewall.

          Press ENTER to Confirm or ESC to Cancel:
```

> **Note:** Configure the firewall rules using the web configurator or CLI commands.

Chapter 35 Introducing the ZyWALL Firewall

CHAPTER 36
Filter Configuration

This chapter shows you how to create and apply filters.

36.1 Introduction to Filters

Your ZyWALL uses filters to decide whether to allow passage of a data packet and/or to make a call. There are two types of filter applications: data filtering and call filtering. Filters are subdivided into device and protocol filters, which are discussed later.

Data filtering screens the data to determine if the packet should be allowed to pass. Data filters are divided into incoming and outgoing filters, depending on the direction of the packet relative to a port. Data filtering can be applied on either the WAN side or the LAN side. Call filtering is used to determine if a packet should be allowed to trigger a call. Remote node call filtering is only applicable when using PPPoE encapsulation. Outgoing packets must undergo data filtering before they encounter call filtering as shown in the following figure.

Figure 297   Outgoing Packet Filtering Process
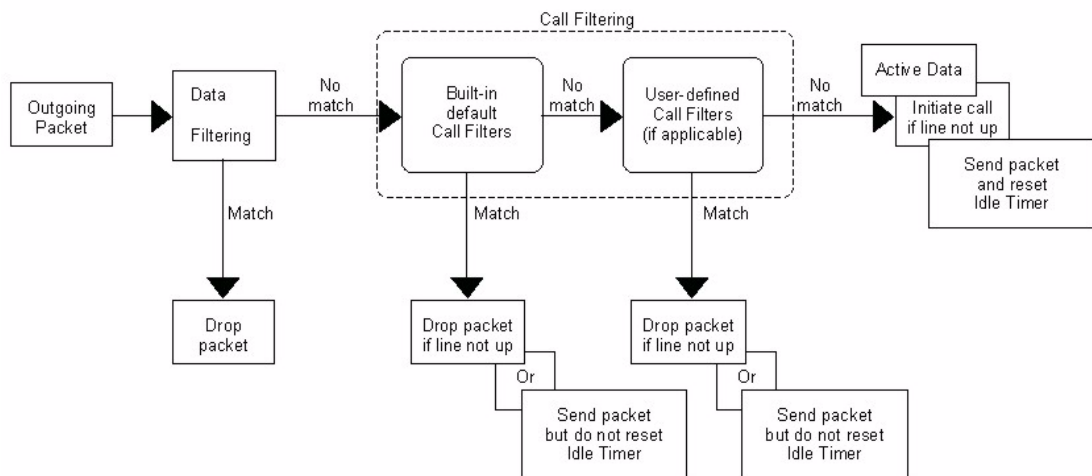
For incoming packets, your ZyWALL applies data filters only. Packets are processed depending upon whether a match is found. The following sections describe how to configure filter sets.

36.1.1 The Filter Structure of the ZyWALL

A filter set consists of one or more filter rules. Usually, you would group related rules, e.g., all the rules for NetBIOS, into a single set and give it a descriptive name. The ZyWALL allows you to configure up to twelve filter sets with six rules in each set, for a total of 72 filter rules in the system. You <u>cannot</u> mix device filter rules and protocol filter rules within the same set. You can apply up to four filter sets to a particular port to block multiple types of packets. With each filter set having up to six rules, you can have a maximum of 24 rules active for a single port.

Sets of factory default filter rules have been configured in menu 21 to prevent NetBIOS traffic from triggering calls and to prevent incoming telnet sessions. A summary of their filter rules is shown in the figures that follow.

The following figure illustrates the logic flow when executing a filter rule. See also Figure 302 for the logic flow when executing an IP filter.

Figure 298   Filter Rule Process
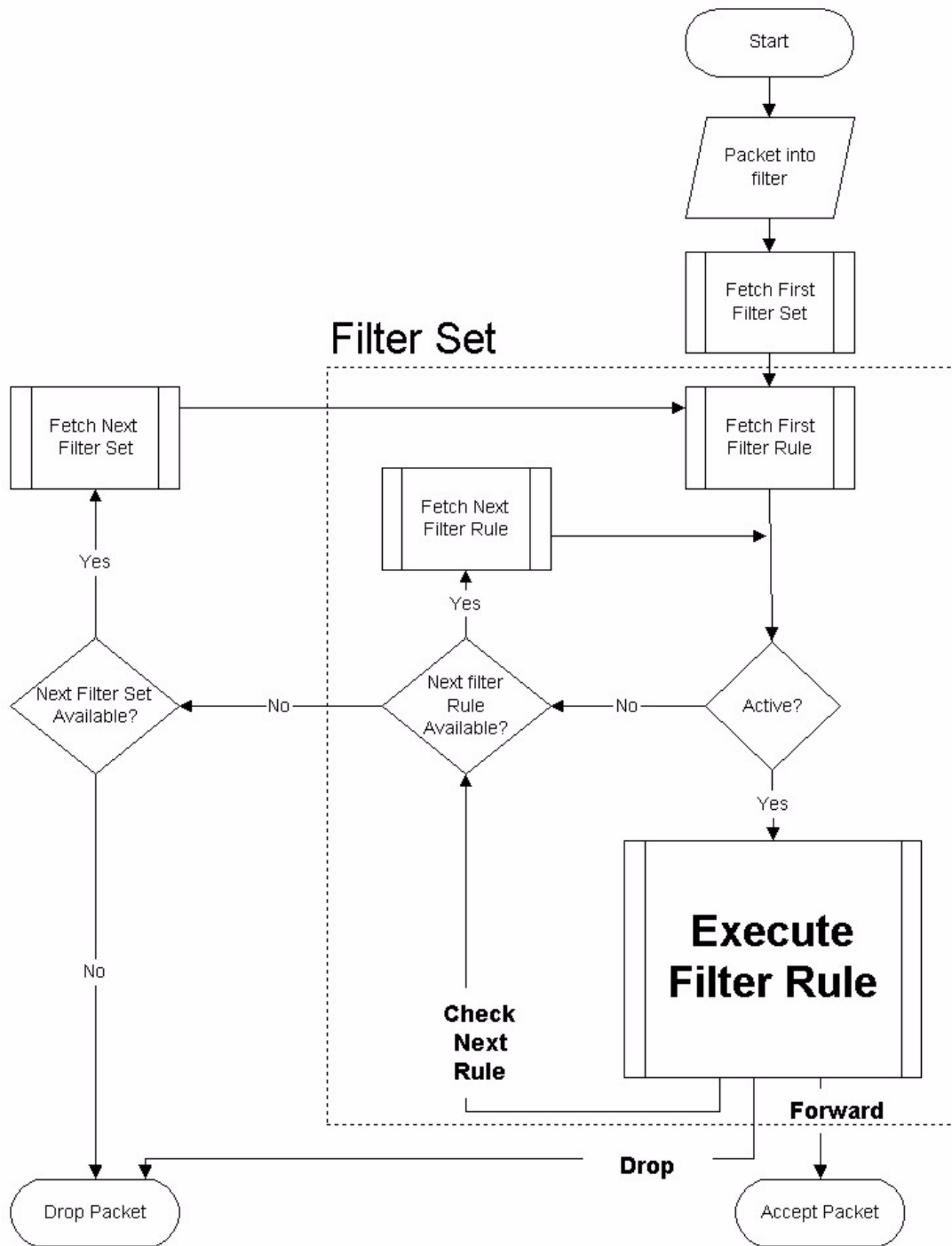
You can apply up to four filter sets to a particular port to block multiple types of packets. With each filter set having up to six rules, you can have a maximum of 24 rules active for a single port.

36.2 Configuring a Filter Set

The ZyWALL includes filtering for NetBIOS over TCP/IP packets by default. To configure another filter set, follow the procedure below.

1 Enter 21 in the main menu to open menu 21.

Figure 299 Menu 21: Filter and Firewall Setup

```
              Menu 21 - Filter and Firewall Setup

                       1. Filter Setup
                       2. Firewall Setup




              Enter Menu Selection Number:
```

2 Enter 1 to bring up the following menu.

Figure 300 Menu 21.1: Filter Set Configuration

```
              Menu 21.1 - Filter Set Configuration

     Filter                            Filter
     Set #        Comments             Set #        Comments
     ------    -----------------       ------    -----------------
      1        _____          7        _____
      2        _____          8        _____
      3        _____          9        _____
      4        _____         10        _____
      5        _____         11        _____
      6        _____         12        _____


          Enter Filter Set Number to Configure= 0

          Edit Comments= N/A

          Press ENTER to Confirm or ESC to Cancel:
```

3 Select the filter set you wish to configure (1-12) and press [ENTER].

4 Enter a descriptive name or comment in the **Edit Comments** field and press [ENTER].

5 Press [ENTER] at the message [Press ENTER to confirm] to open **Menu 21.1.1 - Filter Rules Summary**.

This screen shows the summary of the existing rules in the filter set. The following tables contain a brief description of the abbreviations used in the previous menus.

Table 184 Abbreviations Used in the Filter Rules Summary Menu

FIELD	DESCRIPTION
A	Active: "Y" means the rule is active. "N" means the rule is inactive.
Type	The type of filter rule: "GEN" for Generic, "IP" for TCP/IP.
Filter Rules	These parameters are displayed here.
M	More. "Y" means there are more rules to check which form a rule chain with the present rule. An action cannot be taken until the rule chain is complete. "N" means there are no more rules to check. You can specify an action to be taken i.e., forward the packet, drop the packet or check the next rule. For the latter, the next rule is independent of the rule just checked.
m	Action Matched. "F" means to forward the packet immediately and skip checking the remaining rules. "D" means to drop the packet. "N" means to check the next rule.
n	Action Not Matched. "F" means to forward the packet immediately and skip checking the remaining rules. "D" means to drop the packet. "N" means to check the next rule.

The protocol dependent filter rules abbreviation are listed as follows:

Table 185 Rule Abbreviations Used

ABBREVIATION		DESCRIPTION
IP		
	Pr	Protocol
	SA	Source Address
	SP	Source Port number
	DA	Destination Address
	DP	Destination Port number
GEN		
	Off	Offset
	Len	Length

Refer to the next section for information on configuring the filter rules.

36.2.1 Configuring a Filter Rule

To configure a filter rule, type its number in **Menu 21.1.1 - Filter Rules Summary** and press [ENTER] to open menu 21.1.1.1 for the rule.

To speed up filtering, all rules in a filter set must be of the same class, i.e., protocol filters or generic filters. The class of a filter set is determined by the first rule that you create. When applying the filter sets to a port, separate menu fields are provided for protocol and device filter sets. If you include a protocol filter set in a device filter field or vice versa, the ZyWALL will warn you and will not allow you to save.

36.2.2 Configuring a TCP/IP Filter Rule

This section shows you how to configure a TCP/IP filter rule. TCP/IP rules allow you to base the rule on the fields in the IP and the upper layer protocol, for example, UDP and TCP headers.

To configure TCP/IP rules, select **TCP/IP Filter Rule** from the **Filter Type** field and press [ENTER] to open **Menu 21.1.1.1 - TCP/IP Filter Rule**, as shown next.

Figure 301 Menu 21.1.1.1: TCP/IP Filter Rule

```
                 Menu 21.1.1.1 - TCP/IP Filter Rule

          Filter #: 1,1
          Filter Type= TCP/IP Filter Rule
          Active= Yes
          IP Protocol= 0      IP Source Route= No
          Destination: IP Addr=
                       IP Mask=
                       Port #=
                       Port # Comp= None
               Source: IP Addr=
                       IP Mask=
                       Port #=
                       Port # Comp= None
          TCP Estab= N/A
          More= No            Log= None
          Action Matched= Check Next Rule
          Action Not Matched= Check Next Rule


          Press ENTER to Confirm or ESC to Cancel:
```

The following table describes how to configure your TCP/IP filter rule.

Table 186 Menu 21.1.1.1: TCP/IP Filter Rule

FIELD	DESCRIPTION
Active	Press [SPACE BAR] and then [ENTER] to select **Yes** to activate the filter rule or **No** to deactivate it.
IP Protocol	Protocol refers to the upper layer protocol, e.g., TCP is 6, UDP is 17 and ICMP is 1. Type a value between 0 and 255. A value of 0 matches ANY protocol.
IP Source Route	Press [SPACE BAR] and then [ENTER] to select **Yes** to apply the rule to packets with an IP source route option. Otherwise the packets must not have a source route option. The majority of IP packets do not have source route.

Table 186 Menu 21.1.1.1: TCP/IP Filter Rule

FIELD	DESCRIPTION
Destination	
IP Addr	Enter the destination IP Address of the packet you wish to filter. This field is ignored if it is 0.0.0.0.
IP Mask	Enter the IP mask to apply to the **Destination: IP Addr**.
Port #	Enter the destination port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0.
Port # Comp	Press [SPACE BAR] and then [ENTER] to select the comparison to apply to the destination port in the packet against the value given **in Destination: Port #**. Options are **None**, **Equal**, **Not Equal**, **Less** and **Greater**.
Source	
IP Addr	Enter the source IP Address of the packet you wish to filter. This field is ignored if it is 0.0.0.0.
IP Mask	Enter the IP mask to apply to the **Source: IP Addr**.
Port #	Enter the source port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0.
Port # Comp	Press [SPACE BAR] and then [ENTER] to select the comparison to apply to the source port in the packet against the value given in **Source: Port #**. Options are **None**, **Equal**, **Not Equal**, **Less** and **Greater**.
TCP Estab	This field is applicable only when the IP Protocol field is 6, TCP. Press [SPACE BAR] and then [ENTER] to select **Yes**, to have the rule match packets that want to establish a TCP connection (SYN=1 and ACK=0); if **No**, it is ignored.
More	Press [SPACE BAR] and then [ENTER] to select **Yes** or **No**. If **Yes**, a matching packet is passed to the next filter rule before an action is taken; if **No**, the packet is disposed of according to the action fields. If **More** is **Yes**, then **Action Matched** and **Action Not Matched** will be **N/A**.
Log	Press [SPACE BAR] and then [ENTER] to select a logging option from the following: **None** – No packets will be logged. **Action Matched** - Only packets that match the rule parameters will be logged. **Action Not Matched** - Only packets that do not match the rule parameters will be logged. **Both** – All packets will be logged.
Action Matched	Press [SPACE BAR] and then [ENTER] to select the action for a matching packet. Options are **Check Next Rule**, **Forward** and **Drop**.
Action Not Matched	Press [SPACE BAR] and then [ENTER] to select the action for a packet not matching the rule. Options are **Check Next Rule**, **Forward** and **Drop**.
When you have **Menu 21.1.1.1 - TCP/IP Filter Rule** configured, press [ENTER] at the message "Press ENTER to Confirm" to save your configuration, or press [ESC] to cancel. This data will now be displayed on **Menu 21.1.1 - Filter Rules Summary**.	

The following figure illustrates the logic flow of an IP filter.

Figure 302 Executing an IP Filter
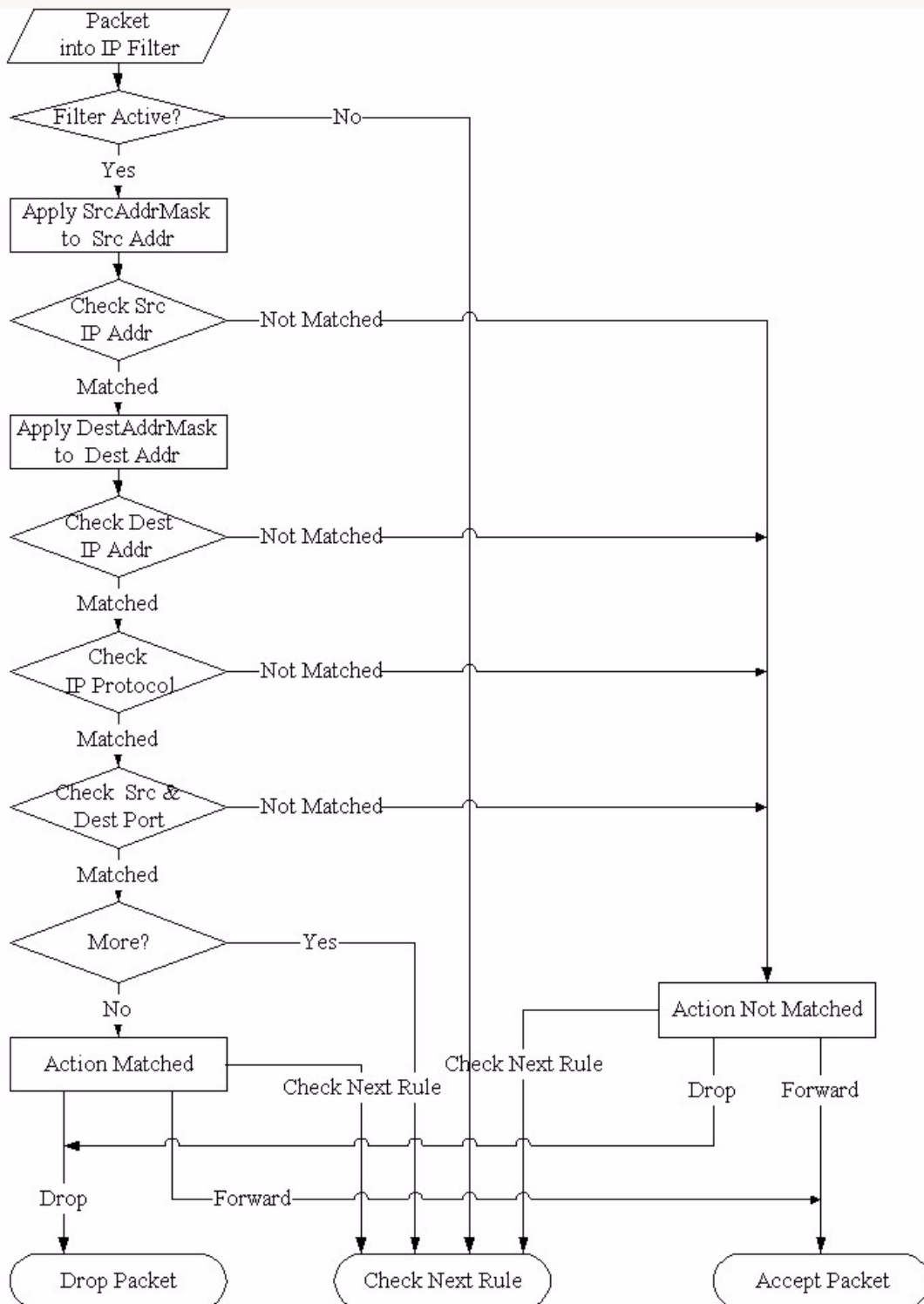
36.2.3 Configuring a Generic Filter Rule

This section shows you how to configure a generic filter rule. The purpose of generic rules is

to allow you to filter non-IP packets. For IP, it is generally easier to use the IP rules directly.

For generic rules, the ZyWALL treats a packet as a byte stream as opposed to an IP or IPX packet. You specify the portion of the packet to check with the **Offset** (from 0) and the **Length** fields, both in bytes. The ZyWALL applies the Mask (bit-wise ANDing) to the data portion before comparing the result against the Value to determine a match. The **Mask** and **Value** are specified in hexadecimal numbers. Note that it takes two hexadecimal digits to represent a byte, so if the length is 4, the value in either field will take 8 digits, for example, FFFFFFFF.

To configure a generic rule, select **Generic Filter Rule** in the **Filter Type** field in menu 21.1.1.1 and press [ENTER] to open Generic Filter Rule, as shown below.

Figure 303 Menu 21.1.1.1: Generic Filter Rule

```
            Menu 21.1.1.1 - Generic Filter Rule

            Filter #: 1,1
            Filter Type= Generic Filter Rule
            Active= No
            Offset= 0
            Length= 0
            Mask= N/A
            Value= N/A
            More= No            Log= None
            Action Matched= Check Next Rule
            Action Not Matched= Check Next Rule

            Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in the **Generic Filter Rule** menu.

Table 187   Generic Filter Rule Menu Fields

FIELD	DESCRIPTION
Filter #	This is the filter set, filter rule co-ordinates, i.e., 2,3 refers to the second filter set and the third rule of that set.
Filter Type	Use [SPACE BAR] and then [ENTER] to select a rule type. Parameters displayed below each type will be different. TCP/IP filter rules are used to filter IP packets while generic filter rules allow filtering of non-IP packets. Options are **Generic Filter Rule** and **TCP/IP Filter Rule**.
Active	Select **Yes** to turn on the filter rule or **No** to turn it off.
Offset	Enter the starting byte of the data portion in the packet that you wish to compare. The range for this field is from 0 to 255.
Length	Enter the byte count of the data portion in the packet that you wish to compare. The range for this field is 0 to 8.
Mask	Enter the mask (in Hexadecimal notation) to apply to the data portion before comparison.
Value	Enter the value (in Hexadecimal notation) to compare with the data portion.

Table 187 Generic Filter Rule Menu Fields

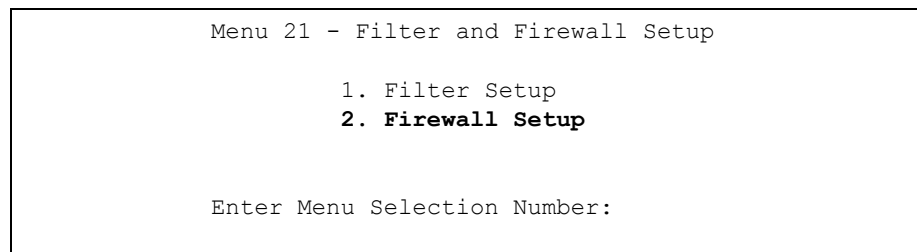| FIELD	DESCRIPTION
More	If **Yes**, a matching packet is passed to the next filter rule before an action is taken; else the packet is disposed of according to the action fields. If **More** is **Yes**, then Action Matched and Action Not Matched will be **No**.
Log	Select the logging option from the following: **None** - No packets will be logged. **Action Matched** - Only packets that match the rule parameters will be logged. **Action Not Matched** - Only packets that do not match the rule parameters will be logged. **Both** – All packets will be logged.
Action Matched	Select the action for a packet matching the rule. Options are **Check Next Rule**, **Forward** and **Drop**.
Action Not Matched	Select the action for a packet not matching the rule. Options are **Check Next Rule**, **Forward** and **Drop**.
Once you have completed filling in **Menu 21.1.1.1 - Generic Filter Rule**, press [ENTER] at the message "Press ENTER to Confirm" to save your configuration, or press [ESC] to cancel. This data will now be displayed on **Menu 21.1.1 - Filter Rules Summary**.	

36.3 Example Filter

Let's look at an example to block outside users from accessing the ZyWALL via telnet. Please see our included disk for more example filters.

Figure 304   Telnet Filter Example
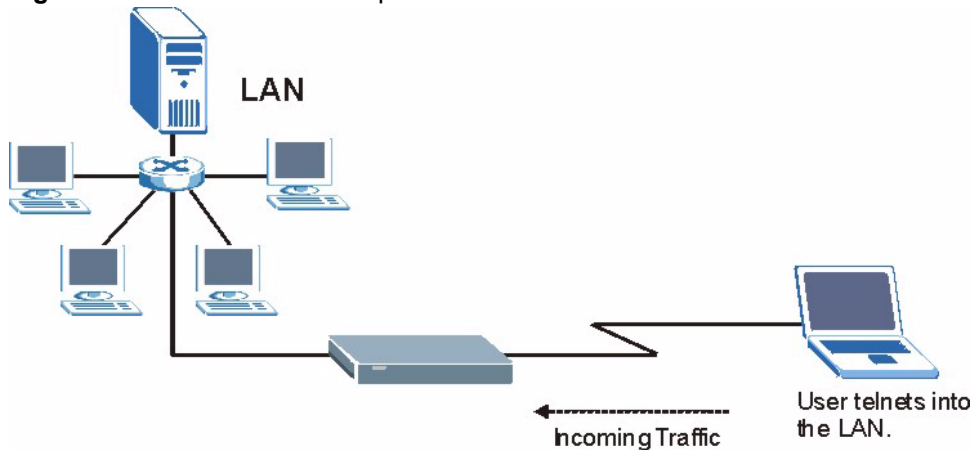
1 Enter 21 from the main menu to open **Menu 21 - Filter and Firewall Setup**.

2 Enter 1 to open Menu 21.1 - Filter Set Configuration.

3 Enter the index of the filter set you wish to configure (say 3) and press [ENTER].

4 Enter a descriptive name or comment in the **Edit Comments** field and press [ENTER].

5 Press [ENTER] at the message [Press ENTER to confirm] to open **Menu 21.1.3 - Filter Rules Summary**.

6 Enter 1 to configure the first filter rule (the only filter rule of this set). Make the entries in this menu as shown in the following figure.

Figure 305 Example Filter: Menu 21.1.3.1

```
                  Menu 21.1.3.1 - TCP/IP Filter Rule

          Filter #: 3,1
          Filter Type= TCP/IP Filter Rule
          Active= Yes
          IP Protocol= 6      IP Source Route= No
          Destination: IP Addr= 0.0.0.0
                       IP Mask= 0.0.0.0
                       Port #= 23
                       Port # Comp= Equal
                Source: IP Addr= 0.0.0.0
                       IP Mask= 0.0.0.0
                       Port #= 0
                       Port # Comp= None
          TCP Estab= No
          More= No                Log= None
          Action Matched= Drop
          Action Not Matched= Forward


                   Press ENTER to Confirm or ESC to Cancel:
          Press Space Bar to Toggle.
```

The port number for the telnet service (TCP protocol) is **23**. See *RFC 1060* for port numbers of well-known services.

When you press [ENTER] to confirm, you will see the following screen. Note that there is only one filter rule in this set.

Figure 306 Example Filter Rules Summary: Menu 21.1.3

```
          Menu 21.1.3 - Filter Rules Summary

   # A Type                      Filter Rules           M m n
   - - ---- ------------------------------------------------- - - -
   1 Y IP    Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=23           N D F
   2 N
   3 N
   4 N
   5 N
   6 N



   Enter Filter Rule Number (1-6) to Configure: 1
```

This shows you that you have configured and activated (**A = Y**) a TCP/IP filter rule (**Type = IP**, **Pr = 6**) for destination telnet ports (**DP = 23**).

M = N means an action can be taken immediately. The action is to drop the packet (**m = D**) if the action is matched and to forward the packet immediately (**n = F**) if the action is not matched no matter whether there are more rules to be checked (there aren't in this example).

After you've created the filter set, you must apply it.

1 Enter 11 from the main menu to go to menu 11.

2 Go to the **Edit Filter Sets** field, press [SPACE BAR] to select **Yes** and press [ENTER].

3 This brings you to menu 11.5. Apply a filter set (our example filter set 3) as shown in Figure 310.

4 Press [ENTER] to confirm after you enter the set numbers and to leave menu 11.5.

36.4 Filter Types and NAT

There are two classes of filter rules, **Generic Filter** (Device) rules and protocol filter (**TCP/IP**) rules. Generic filter rules act on the raw data from/to LAN and WAN. Protocol filter rules act on the IP packets. Generic and TCP/IP filter rules are discussed in more detail in the next section. When NAT (Network Address Translation) is enabled, the inside IP address and port number are replaced on a connection-by-connection basis, which makes it impossible to know the exact address and port on the wire. Therefore, the ZyWALL applies the protocol filters to the "native" IP address and port number before NAT for outgoing packets and after NAT for incoming packets. On the other hand, the generic, or device filters are applied to the raw packets that appear on the wire. They are applied at the point when the ZyWALL is receiving and sending the packets; i.e. the interface. The interface can be an Ethernet port or any other hardware port. The following diagram illustrates this.

Figure 307   Protocol and Device Filter Sets
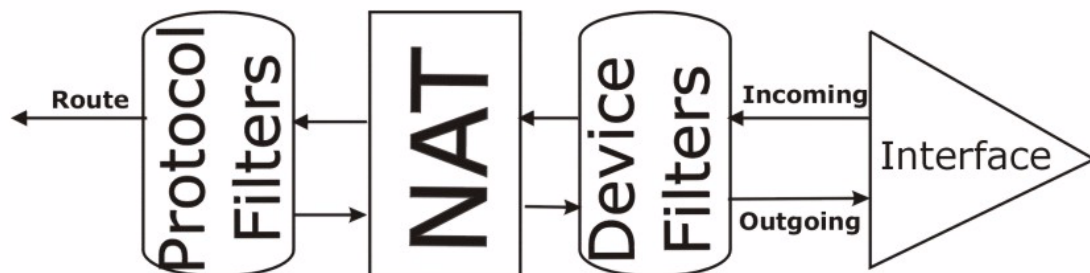
36.5 Firewall Versus Filters

Firewall configuration is discussed in Chapter 10 Firewall Screens. Further comparisons are also made between filtering, NAT and the firewall.

36.6 Applying a Filter

This section shows you where to apply the filter(s) after you design it (them). The ZyWALL already has filters to prevent NetBIOS traffic from triggering calls, and block incoming telnet, FTP and HTTP connections.

> **Note:** If you do not activate the firewall, it is advisable to apply filters.

36.6.1 Applying LAN Filters

LAN traffic filter sets may be useful to block certain packets, reduce traffic and prevent security breaches. Go to menu 3.1 (shown next) and enter the number(s) of the filter set(s) that you want to apply as appropriate. You can choose up to four filter sets (from twelve) by entering their numbers separated by commas, e.g., 3, 4, 6, 11. Input filter sets filter incoming traffic to the ZyWALL and output filter sets filter outgoing traffic from the ZyWALL. For PPPoE or PPTP encapsulation, you have the additional option of specifying remote node call filter sets.

Figure 308   Filtering LAN Traffic

```
                Menu 3.1 - LAN Port Filter Setup

        Input Filter Sets:
          protocol filters=
            device filters=
        Output Filter Sets:
          protocol filters=
            device filters=


        Press ENTER to Confirm or ESC to Cancel:
```

36.6.2 Applying DMZ Filters

DMZ traffic filter sets may be useful to block certain packets, reduce traffic and prevent security breaches. Go to menu 5.1 (shown next) and enter the number(s) of the filter set(s) that you want to apply as appropriate. You can choose up to four filter sets (from twelve) by entering their numbers separated by commas, e.g., 3, 4, 6, 11. Input filter sets filter incoming traffic to the ZyWALL and output filter sets filter outgoing traffic from the ZyWALL. The ZyWALL already has filters to prevent NetBIOS traffic from triggering calls, and block incoming telnet, FTP and HTTP connections.

Figure 309   Filtering DMZ Traffic

```
          Menu 5.1 - DMZ Port Filter Setup

   Input Filter Sets:
     protocol filters=
        device filters=
   Output Filter Sets:
     protocol filters=
        device filters=


   Press ENTER to Confirm or ESC to Cancel:
```

36.6.3 Applying Remote Node Filters

Go to menu 11.1.4 (shown below – note that call filter sets are only present for PPPoE encapsulation) and enter the number(s) of the filter set(s) as appropriate. You can cascade up to four filter sets by entering their numbers separated by commas. The ZyWALL already has filters to prevent NetBIOS traffic from triggering calls, and block incoming telnet, FTP and HTTP connections.

Figure 310   Filtering Remote Node Traffic

```
          Menu 11.1.4 - Remote Node Filter Setup

   Input Filter Sets:
     protocol filters=
        device filters=
   Output Filter Sets:
     protocol filters=
        device filters=


   Press ENTER to Confirm or ESC to Cancel:
```

CHAPTER 37
SNMP Configuration

This chapter explains SNMP configuration menu 22.

37.1 SNMP Configuration

To configure SNMP, enter 22 from the main menu to display **Menu 22 - SNMP Configuration** as shown next. The "community" for **Get**, **Set** and **Trap** fields is SNMP terminology for password.

Figure 311 Menu 22: SNMP Configuration

```
              Menu 22 - SNMP Configuration

                    SNMP:
                      Get Community= public
                      Set Community= public
                      Trusted Host= 0.0.0.0
                      Trap:
                        Community= public
                        Destination= 0.0.0.0



              Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the SNMP configuration parameters.

Table 188 SNMP Configuration Menu Fields

FIELD	DESCRIPTION
Get Community	Type the Get community, which is the password for the incoming Get- and GetNext requests from the management station.
Set Community	Type the Set community, which is the password for incoming Set requests from the management station.
Trusted Host	If you enter a trusted host, your ZyWALL will only respond to SNMP messages from this address. A blank (default) field means your ZyWALL will respond to all SNMP messages it receives, regardless of source.
Trap	
Community	Type the Trap community, which is the password sent with each trap to the SNMP manager.

Table 188   SNMP Configuration Menu Fields (continued)

FIELD	DESCRIPTION
Destination	Type the IP address of the station to send your SNMP traps to.
When you have completed this menu, press [ENTER] at the prompt "Press [ENTER] to confirm or [ESC] to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

37.2 SNMP Traps

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

Table 189   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.

CHAPTER 38
System Information & Diagnosis

This chapter covers SMT menus 24.1 to 24.4.

38.1 Introduction to System Status

This chapter covers the diagnostic tools that help you to maintain your ZyWALL. These tools include updates on system status, port status and log and trace capabilities.

Select menu 24 in the main menu to open **Menu 24 - System Maintenance, as shown below.**

Figure 312   Menu 24: System Maintenance

```
                   Menu 24 - System Maintenance

            1.   System Status
            2.   System Information and Console Port Speed
            3.   Log and Trace
            4.   Diagnostic
            5.   Backup Configuration
            6.   Restore Configuration
            7.   Upload Firmware
            8.   Command Interpreter Mode
            9.   Call Control
            10.  Time and Date Setting
            11.  Remote Management Setup



         Enter Menu Selection Number:
```
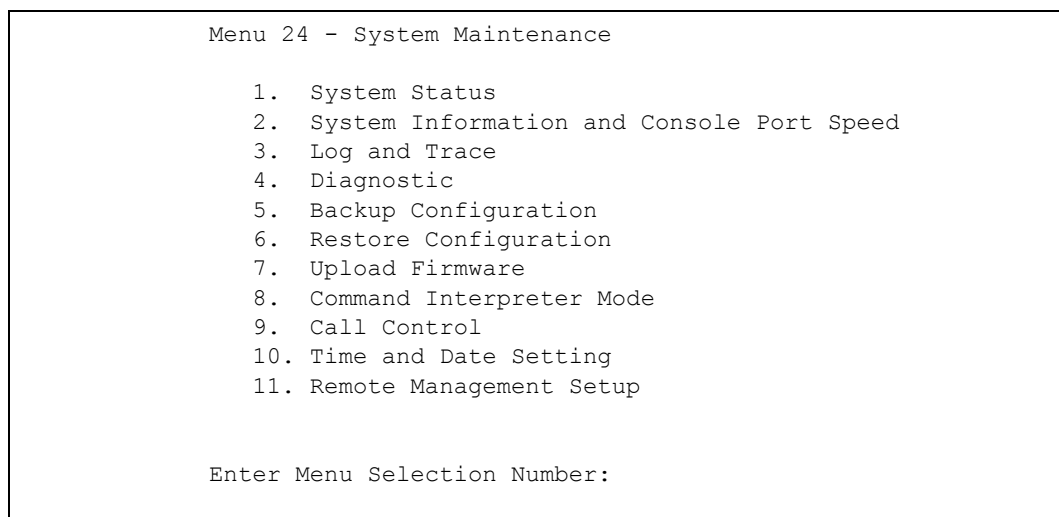
38.2 System Status

The first selection, System Status, gives you information on the version of your system firmware and the status and statistics of the ports, as shown in the next figure. System Status is a tool that can be used to monitor your ZyWALL. Specifically, it gives you information on your system firmware version, number of packets sent and number of packets received.

To get to the System Status:

1 Enter number 24 to go to Menu 24 - System Maintenance.

2 In this menu, enter 1 to open System Maintenance - Status.

3 There are three commands in **Menu 24.1 - System Maintenance - Status**. Entering 1 drops the WAN connection, 9 resets the counters and [ESC] takes you back to the previous screen.

Figure 313 Menu 24.1: System Maintenance: Status

```
           Menu 24.1 - System Maintenance - Status          08:17:55
                                              Wed. Jul. 07, 2004

Port    Status       TxPkts      RxPkts     Cols    Tx B/s   Rx B/s    Up Time
WAN1    100M/Full      9439      332111        0         0     1062    2:35:42
WAN2    Down              0           0        0         0        0    0:00:00
 LAN    100M/Full      7802       11353        0       354      192    2:35:42
WLAN    Down              0           0        0         0        0    0:00:00
 DMZ    100M/Full         0           0        0         0        0    2:35:42

Port    Ethernet Address        IP Address           IP Mask        DHCP
WAN1    00:A0:C5:01:23:46     172.22.1.162       255.255.0.0      Client
WAN2    00:A0:C5:01:23:48          0.0.0.0           0.0.0.0      Client
 LAN    00:A0:C5:01:23:45     192.168.1.1       255.255.255.0      Server
WLAN    00:00:00:00:00:00
 DMZ    00:A0:C5:01:23:47          0.0.0.0           0.0.0.0        None

     System up Time:     2:35:47

                              Press Command:

COMMANDS: 1, 2-Drop WAN1,2 9-Reset Counters    ESC-Exit
```

The following table describes the fields present in **Menu 24.1 - System Maintenance - Status**. These fields are READ-ONLY and meant for diagnostic purposes. The upper right corner of the screen shows the time and date according to the format you set in menu 24.10.

Table 190   System Maintenance: Status Menu Fields

FIELD	DESCRIPTION
Port	This field identifies a port (WAN, LAN, WLAN or DMZ) on the ZyWALL.
Status	This field shows 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.
Cols	This is the number of collisions on this port.
Tx B/s	This field shows the transmission speed in Bytes per second on this port.
Rx B/s	This field shows the reception speed in Bytes per second on this port.
Up Time	This is the total amount of time the line has been up.
Ethernet Address	This is the Ethernet address of the port listed on the left.
IP Address	This is the IP address of the port listed on the left.

Table 190 System Maintenance: Status Menu Fields (continued)

FIELD	DESCRIPTION
IP Mask	This is the IP mask of the port listed on the left.
DHCP	This is the DHCP setting of the port listed on the left.
System up Time	This is the total time the ZyWALL has been on.
You may enter 1 to drop the WAN connection, 9 to reset the counters or [ESC] to return to menu 24.	

38.3 System Information and Console Port Speed

This section describes your system and allows you to choose different console port speeds. To get to the System Information and Console Port Speed:

1 Enter 24 to go to **Menu 24 - System Maintenance**.

2 Enter 2 to open **Menu 24.2 - System Information and Console Port Speed**.

3 From this menu you have two choices as shown in the next figure:

Figure 314 Menu 24.2: System Information and Console Port Speed

```
        Menu 24.2 - System Information and Console Port Speed

              1. System Information
              2. Console Port Speed

        Please enter selection:
```

38.3.1 System Information

System Information gives you information about your system as shown below. More specifically, it gives you information on your routing protocol, Ethernet address, IP address, etc.

Figure 315   Menu 24.2.1: System Maintenance: Information

```
          Menu 24.2.1 - System Maintenance - Information

          Name:
          Routing: IP
          ZyNOS F/W Version: V3.63(WZ.0)b1 | 09/23/2004
          Country Code: 255

          LAN
            Ethernet Address: 00:A0:C5:70:F7:EB
            IP Address: 192.168.1.1
            IP Mask: 255.255.255.0
            DHCP: Server


                Press ESC or RETURN to Exit:
```

The following table describes the fields in this screen.

Table 191   Fields in System Maintenance: Information

FIELD	DESCRIPTION
Name	This is the ZyWALL's system name + domain name assigned in menu 1. For example, System Name= xxx; Domain Name= baboo.mickey.com Name= xxx.baboo.mickey.com
Routing	Refers to the routing protocol used.
ZyNOS F/W Version	Refers to the version of ZyXEL's Network Operating System software.
Country Code	Refers to the country code of the firmware.
LAN	
Ethernet Address	Refers to the Ethernet MAC (Media Access Control) address of your ZyWALL.
IP Address	This is the IP address of the ZyWALL in dotted decimal notation.
IP Mask	This shows the IP mask of the ZyWALL.
DHCP	This field shows the DHCP setting of the ZyWALL.
When finished viewing, press [ESC] or [ENTER] to exit.	

38.3.2 Console Port Speed

You can change the speed of the console port through **Menu 24.2.2 – Console Port Speed**. Your ZyWALL supports 9600 (default), 19200, 38400, 57600, and 115200 bps for the console port. Press [SPACE BAR] and then [ENTER] to select the desired speed in menu 24.2.2, as shown next.

Figure 316 Menu 24.2.2: System Maintenance: Change Console Port Speed

```
          Menu 24.2.2 - System Maintenance - Change Console Port Speed

                         Console Port Speed: 9600


                         Press ENTER to Confirm or ESC to Cancel:Press
          Space Bar to Toggle.
```

38.4 Log and Trace

There are two logging facilities in the ZyWALL. The first is the error logs and trace records that are stored locally. The second is the UNIX syslog facility for message logging.

38.4.1 Viewing Error Log

The first place you should look for clues when something goes wrong is the error/trace log. Follow the procedure below to view the local error/trace log:

1 Select option 24 from the main menu to open **Menu 24 - System Maintenance**.

2 From menu 24, select option 3 to open **Menu 24.3 - System Maintenance - Log and Trace**.

3 Select the first option from **Menu 24.3 - System Maintenance - Log and Trace** to display the error log in the system.

After the ZyWALL finishes displaying, you will have the option to clear the error log.

Figure 317 Menu 24.3: System Maintenance: Log and Trace

```
          Menu 24.3 - System Maintenance - Log and Trace

          1. View Error Log
          2. UNIX Syslog

          4. Call-Triggering Packet


                  Please enter selection
```

Examples of typical error and information messages are presented in the following figure.

Figure 318   Examples of Error and Information Messages

```
52 Thu Jul  1 05:54:53 2004 PP05  ERROR Wireless LAN init fail, code=15
53 Thu Jul  1 05:54:53 2004 PINI  INFO  Channel 0 ok
54 Thu Jul  1 05:54:56 2004 PP05 -WARN  SNMP TRAP 3: interface 3: link up
55 Thu Jul  1 05:54:56 2004 PP0d  INFO  LAN promiscuous mode <0>
57 Thu Jul  1 05:54:56 2004 PP0d  INFO  LAN promiscuous mode <1>
58 Thu Jul  1 05:54:56 2004 PINI  INFO  Last errorlog repeat 1 Times
59 Thu Jul  1 05:54:56 2004 PINI  INFO  main: init completed
60 Thu Jul  1 05:55:26 2004 PSSV -WARN  SNMP TRAP 0: cold start
61 Thu Jul  1 05:56:56 2004 PINI  INFO  SMT Session Begin
62 Thu Jul  1 07:50:58 2004 PINI  INFO  SMT Session End
63 Thu Jul  1 07:53:28 2004 PINI  INFO  SMT Session Begin
Clear Error Log (y/n):
```

38.4.2 UNIX Syslog

 The ZyWALL uses the UNIX syslog facility to log the CDR (Call Detail Record) and system messages to a syslog server. Syslog and accounting can be configured in **Menu 24.3.2 - System Maintenance - Unix Syslog**, as shown next.

Figure 319   Menu 24.3.2: System Maintenance: UNIX Syslog

```
            Menu 24.3.2 - System Maintenance - Syslog Logging

                 Syslog:
                 Active= No
                 Syslog Server IP Address= 0.0.0.0
                 Log Facility= Local 1


             Press ENTER to Confirm or ESC to Cancel:
```

You need to configure the UNIX syslog parameters described in the following table to activate syslog then choose what you want to log.

Table 192   System Maintenance Menu Syslog Parameters

FIELD	DESCRIPTION
Syslog:	
Active	Press [SPACE BAR] and then [ENTER] to turn syslog on or off.
Syslog Server IP Address	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
Log Facility	Press [SPACE BAR] and then [ENTER] to select a location. The log facility allows you to log the messages to different files in the syslog server. Refer to the documentation of your syslog program for more details.
When finished configuring this screen, press [ENTER] to confirm or [ESC] to cancel.	

Your ZyWALL sends five types of syslog messages. Some examples (not all ZyWALL specific) of these syslog messages with their message formats are shown next:

1 CDR

```
CDR Message Format

   SdcmdSyslogSend( SYSLOG_CDR, SYSLOG_INFO, String );
   String = board xx line xx channel xx, call xx, str
   board = the hardware board ID
   line = the WAN ID in a board
   Channel = channel ID within the WAN
   call = the call reference number which starts from 1 and increments by 1 for
each new call
   str = C01 Outgoing Call dev xx ch xx (dev:device No. ch:channel No.)
        L02 Tunnel Connected(L2TP)
        C02 OutCall Connected xxxx (means connected speed) xxxxx (means Remote
Call Number)
        L02 Call Terminated
        C02 Call Terminated
Jul 19 11:19:27 192.168.102.2 ZyXEL: board 0 line 0 channel 0, call 1, C01
Outgoing Call dev=2 ch=0 40002
Jul 19 11:19:32 192.168.102.2 ZyXEL: board 0 line 0 channel 0, call 1, C02 OutCall
Connected 64000 40002
Jul 19 11:20:06 192.168.102.2 ZyXEL: board 0 line 0 channel 0, call 1, C02 Call
Terminated
```

2 Packet triggered

```
Packet triggered Message Format

SdcmdSyslogSend( SYSLOG_PKTTRI, SYSLOG_NOTICE, String );
        String = Packet trigger: Protocol=xx Data=xxxxxxxxxx…..x
        Protocol: (1:IP 2:IPX 3:IPXHC 4:BPDU 5:ATALK 6:IPNG)
        Data: We will send forty-eight Hex characters to the server
Jul 19 11:28:39 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1,
Data=4500003c100100001f010004c0a86614ca849a7b08004a5c0200010061626364656667686969a
6b6c6d6e6f7071727374
Jul 19 11:28:56 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1,
Data=4500002c1b0140001f06b50ec0a86614ca849a7b0427001700195b3e0000000006002200008cd4
0000020405b4
Jul 19 11:29:06 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1,
Data=45000028240140001f06ac12c0a86614ca849a7b0427001700195b451d1430135004000077600
0000
```

3 Filter log

```
Filter log Message Format
```

```
SdcmdSyslogSend(SYSLOG_FILLOG, SYSLOG_NOTICE, String );
String = IP[Src=xx.xx.xx.xx Dst=xx.xx.xx.xx prot spo=xxxx dpo=xxxx] S04>R01mD
IP[…] is the packet header and S04>R01mD means filter set 4 (S) and rule 1 (R),
match (m) drop (D).
     Src: Source Address
     Dst: Destination Address
     prot: Protocol ("TCP","UDP","ICMP")
spo: Source port
dpo: Destination portMar 03 10:39:43 202.132.155.97 ZyXEL:
GEN[fffffffffffnordff0080] }S05>R01mF
Mar 03 10:41:29 202.132.155.97 ZyXEL:
GEN[00a0c5f502fnord010080] }S05>R01mF
Mar 03 10:41:34 202.132.155.97 ZyXEL:
IP[Src=192.168.2.33 Dst=202.132.155.93 ICMP]}S04>R01mF
Mar 03 11:59:20 202.132.155.97 ZyXEL:
GEN[00a0c5f502fnord010080] }S05>R01mF
Mar 03 12:00:52 202.132.155.97 ZyXEL:
GEN[fffffffffffff0080] }S05>R01mF
Mar 03 12:00:57 202.132.155.97 ZyXEL:
GEN[00a0c5f502010080] }S05>R01mF
Mar 03 12:01:06 202.132.155.97 ZyXEL:
IP[Src=192.168.2.33 Dst=202.132.155.93 TCP spo=01170  dpo=00021]}S04>R01mF
```

4 PPP log

```
PPP Log Message Format
```

```
SdcmdSyslogSend( SYSLOG_PPPLOG, SYSLOG_NOTICE, String );
String = ppp:Proto Starting / ppp:Proto Opening / ppp:Proto Closing / ppp:Proto
Shutdown
Proto = LCP / ATCP / BACP / BCP / CBCP / CCP / CHAP/ PAP / IPCP /
IPXCP
Jul 19 11:42:44 192.168.102.2 ZyXEL: ppp:LCP Closing
Jul 19 11:42:49 192.168.102.2 ZyXEL: ppp:IPCP Closing
Jul 19 11:42:54 192.168.102.2 ZyXEL: ppp:CCP Closing
```

5 Firewall log

```
Firewall Log Message Format
```

```
SdcmdSyslogSend(SYSLOG_FIREWALL, SYSLOG_NOTICE, buf);
buf = IP[Src=xx.xx.xx.xx : spo=xxxx Dst=xx.xx.xx.xx : dpo=xxxx | prot | rule |
action]
Src: Source Address
spo: Source port (empty means no source port information)
Dst: Destination Address
dpo: Destination port (empty means no destination port information)
prot: Protocol ("TCP","UDP","ICMP", "IGMP", "GRE", "ESP")
rule: <a,b> where a means "set" number; b means "rule" number.
Action: nothing(N) block (B) forward (F)
08-01-200011:48:41Local1.Notice192.168.10.10RAS: FW 172.21.1.80     :137  -
>172.21.1.80      :137  |UDP|default permit:<2,0>|B
08-01-200011:48:41Local1.Notice192.168.10.10RAS: FW 192.168.77.88   :520  -
>192.168.77.88   :520  |UDP|default permit:<2,0>|B
08-01-200011:48:39Local1.Notice192.168.10.10RAS: FW 172.21.1.50   ->172.21.1.50
|IGMP<2>|default permit:<2,0>|B
08-01-200011:48:39Local1.Notice192.168.10.10RAS: FW 172.21.1.25   ->172.21.1.25
|IGMP<2>|default permit:<2,0>|B
```

38.4.3 Call-Triggering Packet

Call-Triggering Packet displays information about the packet that triggered a dial-out call in an easy readable format. Equivalent information is available in menu 24.1 in hex format. An example is shown next.

Figure 320   Call-Triggering Packet Example

```
  IP Frame: ENET0-RECV Size:  44/  44   Time: 17:02:44.262
   Frame Type:

     IP Header:
       IP Version             = 4
       Header Length          = 20
       Type of Service        = 0x00 (0)
       Total Length           = 0x002C (44)
       Identification         = 0x0002 (2)
       Flags                  = 0x00
       Fragment Offset        = 0x00
       Time to Live           = 0xFE (254)
       Protocol               = 0x06 (TCP)
       Header Checksum        = 0xFB20 (64288)
       Source IP              = 0xC0A80101 (192.168.1.1)
       Destination IP         = 0x00000000 (0.0.0.0)

     TCP Header:
       Source Port            = 0x0401 (1025)
       Destination Port       = 0x000D (13)
       Sequence Number        = 0x05B8D000 (95997952)
       Ack Number             = 0x00000000 (0)
       Header Length          = 24
       Flags                  = 0x02 (....S.)
       Window Size            = 0x2000 (8192)
       Checksum               = 0xE06A (57450)
       Urgent Ptr             = 0x0000 (0)
       Options                =
           0000: 02 04 02 00

     RAW DATA:
       0000: 45 00 00 2C 00 02 00 00-FE 06 FB 20 C0 A8 01 01  E......... ....
       0010: 00 00 00 00 04 01 00 0D-05 B8 D0 00 00 00 00 00
................
       0020: 60 02 20 00 E0 6A 00 00-02 04 02 00
  Press any key to continue...
```

38.5 Diagnostic

The diagnostic facility allows you to test the different aspects of your ZyWALL to determine if it is working properly. Menu 24.4 allows you to choose among various types of diagnostic tests to evaluate your system, as shown next.

Follow the procedure below to get to **Menu 24.4 - System Maintenance - Diagnostic**.

1 From the main menu, select option 24 to open **Menu 24 - System Maintenance**.

2 From this menu, select option 4. Diagnostic. This will open **Menu 24.4 - System Maintenance - Diagnostic**.

Figure 321 Menu 24.4: System Maintenance: Diagnostic

```
              Menu 24.4 - System Maintenance - Diagnostic


                     TCP/IP
                       1. Ping Host
                       2. WAN DHCP Release
                       3. WAN DHCP Renewal
                       4. Internet Setup Test

                     System
                       11. Reboot System


              Enter Menu Selection Number:

              WAN=
              Host IP Address= N/A
```

38.5.1 WAN DHCP

DHCP functionality can be enabled on the LAN or WAN as shown in Figure 322. LAN DHCP has already been discussed. The ZyWALL can act either as a WAN DHCP client (**IP Address Assignment** field in menu 4 or menu 11.3 is **Dynamic** and the **Encapsulation** field in menu 4 or menu 11 is **Ethernet**) or **None**, (when you have a static IP). The **WAN Release** and **Renewal** fields in menu 24.4 conveniently allow you to release and/or renew the assigned WAN IP address, subnet mask and default gateway in a fashion similar to winipcfg.

Figure 322 WAN & LAN DHCP
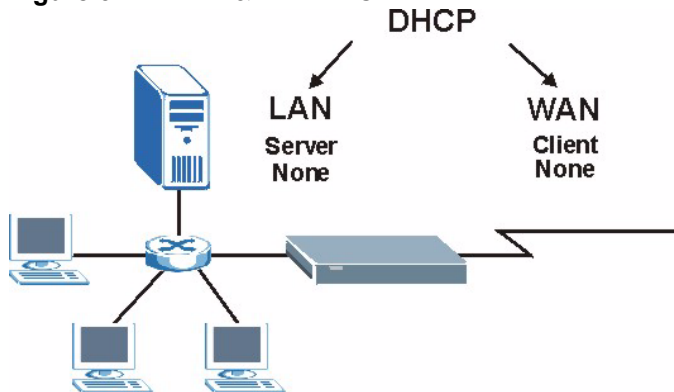
The following table describes the diagnostic tests available in menu 24.4 for your ZyWALL and associated connections.

Table 193 System Maintenance Menu Diagnostic

FIELD	DESCRIPTION
Ping Host	Enter 1 to ping any machine (with an IP address) on your LAN or WAN. Enter its IP address in the **Host IP Address** field below.
WAN DHCP Release	Enter 2 to release your WAN DHCP settings.
WAN DHCP Renewal	Enter 3 to renew your WAN DHCP settings.
Internet Setup Test	Enter 4 to test the Internet setup. You can also test the Internet setup in **Menu 4 - Internet Access**. Please refer to Chapter 29 Internet Access for more details. This feature is only available for dial-up connections using PPPoE or PPTP encapsulation.
Reboot System	Enter 11 to reboot the ZyWALL.
WAN	If you entered 2 or 3 in the **Enter Menu Selection Number** field, enter the number of the WAN port in this field.
Host IP Address	If you entered 1in the **Enter Menu Selection Number** field, then enter the IP address of the computer you want to ping in this field.
Enter the number of the selection you would like to perform or press [ESC] to cancel.	

C H A P T E R 39
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.

39.1 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.

39.2 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 <u>not</u> on the ZyWALL, that is, on your computer, local network or FTP site and so the name (but not the extension) may vary. After uploading new firmware, see the **ZyNOS F/W Version** field in **Menu 24.2.1 - System Maintenance - Information** to confirm that you have uploaded the correct firmware version. The AT command is the command you enter after you press "y" when prompted in the SMT menu to go into debug mode.

Table 194   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

39.3 Backup Configuration

> **Note:** The ZyWALL displays different messages explaining different ways to backup, restore and upload files in menus 24.5, 24.6, 24. 7.1 and 24.7.2 depending on whether you use the console port or Telnet.

Option 5 from **Menu 24 - System Maintenance** allows you to backup the current ZyWALL configuration to your computer. Backup is highly recommended once your ZyWALL is functioning properly. FTP is the preferred method for backing up your current configuration to your computer since it is faster. You can also perform backup and restore using menu 24 through the console port. Any serial communications program should work fine; however, you must use Xmodem protocol to perform the download/upload and you don't have to rename the files.

Please note that terms "download" and "upload" are relative to the computer. Download means to transfer from the ZyWALL to the computer, while upload means from your computer to the ZyWALL.

39.3.1 Backup Configuration

Follow the instructions as shown in the next screen.

Figure 323 Telnet into Menu 24.5

```
                      Menu 24.5 - Backup Configuration

 To transfer the configuration file to your workstation, follow the
 procedure below:

     1. Launch the FTP client on your workstation.
     2. Type "open" and the IP address of your router. Then type
        "root" and SMT password as requested.
     3. Locate the 'rom-0' file.
     4. Type 'get rom-0' to back up the current router
        configuration to your workstation.

 For details on FTP commands, please consult the documentation of your FTP
 client program.  For details on backup using TFTP (note that you must
 remain in this menu to back up using TFTP), please see your router manual.


     Press ENTER to Exit:
```

39.3.2 Using the FTP Command from the Command Line

1 Launch the FTP client on your computer.

2 Enter "open", followed by a space and the IP address of your ZyWALL.

3 Press [ENTER] when prompted for a username.

4 Enter your password as requested (the default is "1234").

5 Enter "bin" to set transfer mode to binary.

6 Use "get" to transfer files from the ZyWALL to the computer, for example, "get rom-0 config.rom" transfers the configuration file on the ZyWALL to your computer and renames it "config.rom". See earlier in this chapter for more information on filename conventions.

7 Enter "quit" to exit the ftp prompt.

39.3.3 Example of FTP Commands from the Command Line

Figure 324 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
```

39.3.4 GUI-based FTP Clients

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

Table 195 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).

39.3.5 File Maintenance Over WAN

TFTP, FTP and Telnet over the WAN will not work when:

1 The firewall is active (turn the firewall off in menu 21.2 or create a firewall rule to allow access from the WAN).

2 You have disabled Telnet service in menu 24.11.

3 You have applied a filter in menu 3.1 (LAN) or in menu 11.5 (WAN) to block Telnet service.

4 The IP you entered in the **Secured Client IP** field in menu 24.11 does not match the client IP. If it does not match, the ZyWALL will disconnect the Telnet session immediately.

5 You have an SMT console session running.

39.3.6 Backup Configuration Using TFTP

The ZyWALL supports the up/downloading of the firmware and the configuration file using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To backup the configuration file, follow the procedure shown next.

1 Use telnet from your computer to connect to the ZyWALL and log in. Because TFTP does not have any security checks, the ZyWALL records the IP address of the telnet client and accepts TFTP requests only from this address.

2 Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.

3 Enter command "sys stdio 0" to disable the SMT timeout, so the TFTP transfer will not be interrupted. Enter command "sys stdio 5" to restore the five-minute SMT timeout (default) when the file transfer is complete.

4 Launch the TFTP client on your computer and connect to the ZyWALL. Set the transfer mode to binary before starting data transfer.

5 Use the TFTP client (see the example below) to transfer files between the ZyWALL and the computer. The file name for the configuration file is "rom-0" (rom-zero, not capital o).

Note that the telnet connection must be active and the SMT in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use "get" to transfer from the ZyWALL to the computer and "binary" to set binary transfer mode.

39.3.7 TFTP Command Example

The following is an example TFTP command:

```
tftp [-i] host get rom-0 config.rom
```

Where "i" specifies binary image transfer mode (use this mode when transferring binary files), "host" is the ZyWALL IP address, "get" transfers the file source on the ZyWALL (rom-0, name of the configuration file on the ZyWALL) to the file destination on the computer and renames it config.rom.

39.3.8 GUI-based TFTP Clients

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

Table 196   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 the File Maintenance Over WAN section to read about configurations that disallow TFTP and FTP over WAN.

39.3.9 Backup Via Console Port

Back up configuration via console port by following the HyperTerminal procedure shown next. Procedures using other serial communications programs should be similar.

1 Display menu 24.5 and enter "y" at the following screen.

Figure 325   System Maintenance: Backup Configuration

```
          Ready to backup Configuration via Xmodem.
          Do you want to continue (y/n):
```

2 The following screen indicates that the Xmodem download has started.

Figure 326   System Maintenance: Starting Xmodem Download Screen

```
          You can enter ctrl-x to terminate operation any
          time.
          Starting XMODEM download...
```

3 Run the HyperTerminal program by clicking **Transfer**, then **Receive File** as shown in the following screen.

Figure 327 Backup Configuration Example

Type a location for storing the configuration file or click **Browse** to look for one.

Choose the **Xmodem** protocol.

Then click **Receive**.

4 After a successful backup you will see the following screen. Press any key to return to the SMT menu.

Figure 328 Successful Backup Confirmation Screen

```
              ** Backup Configuration completed. OK.
              ### Hit any key to continue.###
```

39.4 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.

39.4.1 Restore Using FTP

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

Figure 329 Telnet into Menu 24.6

```
        Menu 24.6 -- System Maintenance - Restore Configuration

 To transfer the firmware and configuration file to your workstation,
 follow the procedure below:

 1. Launch the FTP client on your workstation.
 2. Type "open" and the IP address of your router. Then type "root" and
 SMT password as requested.
 3. Type "put backupfilename rom-0" where backupfilename is the name of
 your backup configuration file on your workstation and rom-0 is the
 remote file name on the router. This restores the configuration to  your
 router.
 4. The system reboots automatically after a successful file transferFor
 details on FTP commands, please consult the documentation of your
 FTPclient program.

 For details on backup using TFTP (note that you must remain in this menu
 to back up using TFTP), please see your router manual.

                        Press ENTER to Exit:
```

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.

39.4.2 Restore Using FTP Session Example

Figure 330 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 the File Maintenance Over WAN section to read about configurations that disallow TFTP and FTP over WAN.

39.4.3 Restore Via Console Port

Restore configuration via console port by following the HyperTerminal procedure shown next. Procedures using other serial communications programs should be similar.

1 Display menu 24.6 and enter "y" at the following screen.

Figure 331 System Maintenance: Restore Configuration

```
Ready to restore Configuration via Xmodem.
Do you want to continue (y/n):
```

2 The following screen indicates that the Xmodem download has started.

Figure 332 System Maintenance: Starting Xmodem Download Screen

```
Starting XMODEM download (CRC mode) ...CCCCCCCCC
```

3 Run the HyperTerminal program by clicking **Transfer**, then **Send File** as shown in the following screen.

Figure 333 Restore Configuration Example
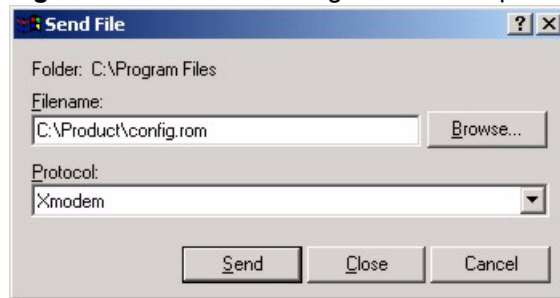
Type the configuration file's location, or click **Browse** to search for it.

Choose the **Xmodem** protocol.

Then click **Send**.

4 After a successful restoration you will see the following screen. Press any key to restart the ZyWALL and return to the SMT menu.

Figure 334 Successful Restoration Confirmation Screen

```
                        Save to ROM
                        Hit any key to start system reboot.
```
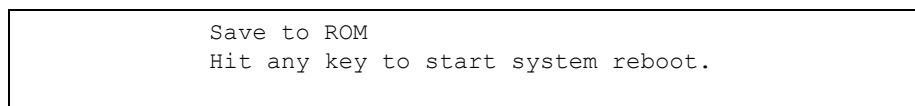
39.5 Uploading Firmware and Configuration Files

This section shows you how to upload firmware and configuration files. You can upload configuration files by following the procedure in the Restore Configuration section or by following the instructions in **Menu 24.7.2 - System Maintenance - Upload System Configuration File** (for console port).

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

39.5.1 Firmware File Upload

FTP is the preferred method for uploading the firmware and configuration. To use this feature, your computer must have an FTP client.

When you telnet into the ZyWALL, you will see the following screens for uploading firmware and the configuration file using FTP.

Figure 335   Telnet Into Menu 24.7.1: Upload System Firmware

```
          Menu 24.7.1 - System Maintenance - Upload System Firmware

To upload the system firmware, follow the procedure below:

  1. Launch the FTP client on your workstation.
  2. Type "open" and the IP address of your system. Then type "root" and
SMT password as requested.
  3. Type "put firmwarefilename ras" where "firmwarefilename" is the name
of your firmware upgrade file on your workstation and "ras" is the remote
file name on the system.
  4. The system reboots automatically after a successful firmware upload.

For details on FTP commands, please consult the documentation of your FTP
client program. For details on uploading system firmware using TFTP (note
that you must remain on this menu to upload system firmware using TFTP),
please see your manual.

Press ENTER to Exit:
```

39.5.2 Configuration File Upload

You see the following screen when you telnet into menu 24.7.2.

Figure 336   Telnet Into Menu 24.7.2: System Maintenance

```
   Menu 24.7.2 - System Maintenance - Upload System Configuration File

To upload the system configuration file, follow the procedure below:

  1. Launch the FTP client on your workstation.
  2. Type "open" and the IP address of your system. Then type "root" and
SMT password as requested.
  3. Type "put configurationfilename rom-0" where "configurationfilename"
is the name of your system configuration file on your workstation, which
will be transferred to the "rom-0" file on the system.
  4. The system reboots automatically after the upload system
configuration file process is complete.

For details on FTP commands, please consult the documentation of your FTP
client program. For details on uploading configuration file using TFTP
(note that you must remain on this menu to upload configuration file using
TFTP), please see your manual.

Press ENTER to Exit:
```

To upload the firmware and the configuration file, follow these examples

39.5.3 FTP File Upload Command from the DOS Prompt Example

1 Launch the FTP client on your computer.

2 Enter "open", followed by a space and the IP address of your ZyWALL.

3 Press [ENTER] when prompted for a username.

4 Enter your password as requested (the default is "1234").

5 Enter "bin" to set transfer mode to binary.

6 Use "put" to transfer files from the computer to the ZyWALL, for example, "put firmware.bin ras" transfers the firmware on your computer (firmware.bin) to the ZyWALL and renames it "ras". Similarly, "put config.rom rom-0" transfers the configuration file on your computer (config.rom) to the ZyWALL and renames it "rom-0". Likewise "get rom-0 config.rom" transfers the configuration file on the ZyWALL to your computer and renames it "config.rom." See earlier in this chapter for more information on filename conventions.

7 Enter "quit" to exit the ftp prompt.

39.5.4 FTP Session Example of Firmware File Upload

Figure 337   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 the File Maintenance Over WAN section to read about configurations that disallow TFTP and FTP over WAN.

39.5.5 TFTP File Upload

The ZyWALL also supports the uploading of firmware files using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To transfer the firmware and the configuration file, follow the procedure shown next.

1 Use telnet from your computer to connect to the ZyWALL and log in. Because TFTP does not have any security checks, the ZyWALL records the IP address of the telnet client and accepts TFTP requests only from this address.

2 Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.

3 Enter the command "sys stdio 0" to disable the console timeout, so the TFTP transfer will not be interrupted. Enter "command sys stdio 5" to restore the five-minute console timeout (default) when the file transfer is complete.

4 Launch the TFTP client on your computer and connect to the ZyWALL. Set the transfer mode to binary before starting data transfer.

5 Use the TFTP client (see the example below) to transfer files between the ZyWALL and the computer. The file name for the firmware is "ras".

Note that the telnet connection must be active and the ZyWALL in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use "get" to transfer from the ZyWALL to the computer, "put" the other way around, and "binary" to set binary transfer mode.

39.5.6 TFTP Upload Command Example

The following is an example TFTP command:

```
tftp [-i] host put firmware.bin ras
```

Where "i" specifies binary image transfer mode (use this mode when transferring binary files), "host" is the ZyWALL's IP address, "put" transfers the file source on the computer (firmware.bin – name of the firmware on the computer) to the file destination on the remote host (ras - name of the firmware on the ZyWALL).

Commands that you may see in GUI-based TFTP clients are listed earlier in this chapter.

39.5.7 Uploading Via Console Port

FTP or TFTP are the preferred methods for uploading firmware to your ZyWALL. However, in the event of your network being down, uploading files is only possible with a direct connection to your ZyWALL via the console port. Uploading files via the console port under normal conditions is not recommended since FTP or TFTP is faster. Any serial communications program should work fine; however, you must use the Xmodem protocol to perform the download/upload.

39.5.8 Uploading Firmware File Via Console Port

1 Select 1 from Menu 24.7 – System Maintenance – Upload Firmware to display Menu 24.7.1 - System Maintenance - Upload System Firmware, and then follow the instructions as shown in the following screen.

Figure 338   Menu 24.7.1 As Seen Using the Console Port
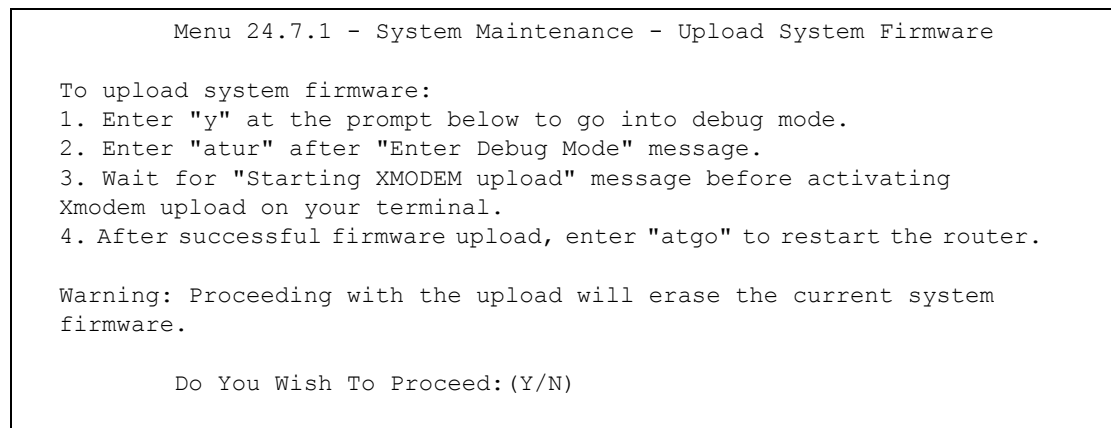
```
         Menu 24.7.1 - System Maintenance - Upload System Firmware

 To upload system firmware:
 1. Enter "y" at the prompt below to go into debug mode.
 2. Enter "atur" after "Enter Debug Mode" message.
 3. Wait for "Starting XMODEM upload" message before activating
 Xmodem upload on your terminal.
 4. After successful firmware upload, enter "atgo" to restart the router.

 Warning: Proceeding with the upload will erase the current system
 firmware.

         Do You Wish To Proceed:(Y/N)
```

2 After the "Starting Xmodem upload" message appears, activate the Xmodem protocol on your computer. Follow the procedure as shown previously for the HyperTerminal program. The procedure for other serial communications programs should be similar.

39.5.9 Example Xmodem Firmware Upload Using HyperTerminal

Click **Transfer**, then **Send File** to display the following screen.

Figure 339   Example Xmodem Upload
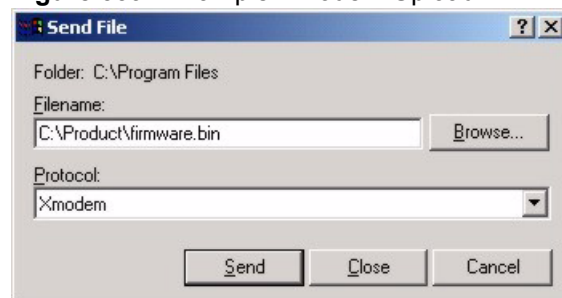
After the firmware upload process has completed, the ZyWALL will automatically restart.

39.5.10 Uploading Configuration File Via Console Port

1 Select 2 from Menu 24.7 – System Maintenance – Upload Firmware to display Menu 24.7.2 - System Maintenance - Upload System Configuration File. Follow the instructions as shown in the next screen.

Figure 340   Menu 24.7.2 As Seen Using the Console Port

```
    Menu 24.7.2 - System Maintenance - Upload System Configuration File

To upload system configuration file:
1. Enter "y" at the prompt below to go into debug mode.
2. Enter "atlc" after "Enter Debug Mode" message.
3. Wait for "Starting XMODEM upload" message before activating
   Xmodem upload on your terminal.
4. After successful firmware upload, enter "atgo" to restart
   the system.

Warning:
1. Proceeding with the upload will erase the current configuration file.
2. The system's console port speed (Menu 24.2.2) may change when it is
restarted; please adjust your terminal's speed accordingly. The password
may change (menu 23), also.
3. When uploading the DEFAULT configuration file, the console port speed
will be reset to 9600 bps and the password to "1234".

          Do You Wish To Proceed:(Y/N)
```

2 After the "Starting Xmodem upload" message appears, activate the Xmodem protocol on your computer. Follow the procedure as shown previously for the HyperTerminal program. The procedure for other serial communications programs should be similar.

3 Enter "atgo" to restart the ZyWALL.

39.5.11 Example Xmodem Configuration Upload Using HyperTerminal

Click **Transfer**, then **Send File** to display the following screen.

Figure 341   Example Xmodem Upload
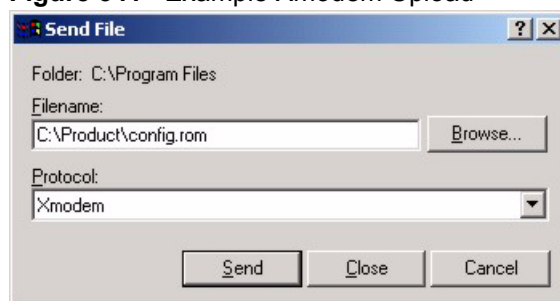
After the configuration upload process has completed, restart the ZyWALL by entering "atgo".

Chapter 39 Firmware and Configuration File Maintenance

CHAPTER 40
System Maintenance Menus 8 to 10

This chapter leads you through SMT menus 24.8 to 24.10.

40.1 Command Interpreter Mode

The Command Interpreter (CI) is a part of the main router firmware. The CI provides much of the same functionality as the SMT, while adding some low-level setup and diagnostic functions. Enter the CI from the SMT by selecting menu 24.8. Access can be by Telnet or by a serial connection to the console port, although some commands are only available with a serial connection. See the included disk or zyxel.com for more detailed information on CI commands. Enter 8 from **Menu 24 - System Maintenance**.

> **Note:** Use of undocumented commands or misconfiguration can damage the unit and possibly render it unusable.

Figure 342   Command Mode in Menu 24

```
             Menu 24 - System Maintenance

        1.  System Status
        2.  System Information and Console Port Speed
        3.  Log and Trace
        4.  Diagnostic
        5.  Backup Configuration
        6.  Restore Configuration
        7.  Upload Firmware
        8.  Command Interpreter Mode
        9.  Call Control
        10. Time and Date Setting
        11. Remote Management Setup


        Enter Menu Selection Number:
```

40.1.1 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.

40.1.2 Command Usage

A list of 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.

Figure 343 Valid Commands

```
Copyright (c) 1994 - 2004 ZyXEL Communications Corp.
ras> ?
Valid commands are:
sys             ls              exit            ether
aux             ip              ipsec           bridge
bm              certificates    8021x           radius
ras>
```

The following table describes some commands in this screen.

Table 197 Valid Commands

COMMAND	DESCRIPTION
sys	The system commands display device information and configure device settings.
exit	This command returns you to the SMT main menu.
ether	These commands display Ethernet information and configure Ethernet settings.
aux	These commands display dial backup information and control dial backup connections.
ip	These commands display IP information and configure IP settings.
ipsec	These commands display IPSec information and configure IPSec settings.
bridge	These commands display bridge information.
bm	These commands configure bandwidth management settings and display bandwidth management information.
certificates	These commands display certificate information and configure certificate settings.
8021x	These commands configure 802.1x settings and display 802.1x information.
radius	These commands display RADIUS information and configure RADIUS settings.

40.2 Call Control Support

The ZyWALL provides two call control functions: budget management and call history. Please note that this menu is only applicable when **Encapsulation** is set to **PPPoE** or **PPTP** in menu 4 or menu 11.1.

The budget management function allows you to set a limit on the total outgoing call time of the ZyWALL within certain times. When the total outgoing call time exceeds the limit, the current call will be dropped and any future outgoing calls will be blocked.

Call history chronicles preceding incoming and outgoing calls.

To access the call control menu, select option 9 in menu 24 to go to **Menu 24.9 - System Maintenance - Call Control**, as shown in the next table.

Figure 344 Call Control

```
          Menu 24.9 - System Maintenance - Call Control

              1.Budget Management
              2.Call History

          Enter Menu Selection Number:
```

40.2.1 Budget Management

Menu 24.9.1 shows the budget management statistics for outgoing calls. Enter 1 from **Menu 24.9 - System Maintenance - Call Control** to bring up the following menu.

Figure 345 Budget Management

```
            Menu 24.9.1 - Budget Management

  Remote Node   Connection Time/Total Budget   Elapsed Time/Total
  Period

  1.WAN_1                  No Budget                  No Budget

  2.WAN_2                  No Budget                  No Budget

  3.Dial                   No Budget                  No Budget


            Reset Node (0 to update screen):
```

The total budget is the time limit on the accumulated time for outgoing calls to a remote node. When this limit is reached, the call will be dropped and further outgoing calls to that remote node will be blocked. After each period, the total budget is reset. The default for the total budget is 0 minutes and the period is 0 hours, meaning no budget control. You can reset the accumulated connection time in this menu by entering the index of a remote node. Enter 0 to update the screen. The budget and the reset period can be configured in menu 11.1 for the remote node.

Table 198 Budget Management

FIELD	DESCRIPTION	EXAMPLE
Remote Node	Enter the index number of the remote node you want to reset (just one in this case)	1
Connection Time/ Total Budget	This is the total connection time that has gone by (within the allocated budget that you set in menu 11.1).	5/10 means that 5 minutes out of a total allocation of 10 minutes have lapsed.
Elapsed Time/Total Period	The period is the time cycle in hours that the allocation budget is reset (see menu 11.1.) The elapsed time is the time used up within this period.	0.5/1 means that 30 minutes out of the 1-hour time period has lapsed.
Enter "0" to update the screen or press [ESC] to return to the previous screen.		

40.2.2 Call History

This is the second option in **Menu 24.9 - System Maintenance - Call Control**. It displays information about past incoming and outgoing calls. Enter 2 from **Menu 24.9 - System Maintenance - Call Control** to bring up the following menu.

Figure 346 Call History

```
               Menu 24.9.2 - Call History

    Phone Number   Dir  Rate #call  Max   Min   Total
   1.
   2.
   3.
   4.
   5.
   6.
   7.
   8.
   9.
  10.

  Enter Entry to Delete(0 to exit):
```

The following table describes the fields in this screen.

Table 199 Call History

FIELD	DESCRIPTION
Phone Number	The PPPoE service names are shown here.
Dir	This shows whether the call was incoming or outgoing.
Rate	This is the transfer rate of the call.
#call	This is the number of calls made to or received from that telephone number.
Max	This is the length of time of the longest telephone call.
Min	This is the length of time of the shortest telephone call.
Total	This is the total length of time of all the telephone calls to/from that telephone number.
You may enter an entry number to delete it or '"0" to exit.	

40.3 Time and Date Setting

The Real Time Chip (RTC) keeps track of the time and date. There is also a software mechanism to set the time manually or get the current time and date from an external server when you turn on your ZyWALL. Menu 24.10 allows you to update the time and date settings of your ZyWALL. The real time is then displayed in the ZyWALL error logs and firewall logs.

Select menu 24 in the main menu to open **Menu 24 - System Maintenance**, as shown next.

Figure 347   Menu 24: System Maintenance

```
             Menu 24 - System Maintenance

        1.   System Status
        2.   System Information and Console Port Speed
        3.   Log and Trace
        4.   Diagnostic
        5.   Backup Configuration
        6.   Restore Configuration
        7.   Upload Firmware
        8.   Command Interpreter Mode
        9.   Call Control
        10.  Time and Date Setting
        11.  Remote Management Setup


             Enter Menu Selection Number:
```

Enter 10 to go to **Menu 24.10 - System Maintenance - Time and Date Setting** to update the
time and date settings of your ZyWALL as shown in the following screen.

Figure 348   Menu 24.10 System Maintenance: Time and Date Setting

```
      Menu 24.10 - System Maintenance - Time and Date Setting

    Time Protocol= NTP (RFC-1305)
    Time Server Address= a.ntp.alphazed.net

    Current Time:                        08 : 24 : 26
    New Time (hh:mm:ss):                 N/A  N/A  N/A

    Current Date:                        2004 - 07 - 01
    New Date (yyyy-mm-dd):               N/A    N/A  N/A

    Time Zone= GMT

    Daylight Saving= No
    Start Date (mm-nth-week-hr):         Jan. - 1st  - Wed. -  00
    End Date (mm-nth-week-hr):           Jan. - 1st  - Wed. -  00


      Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this screen.

Table 200 Menu 24.10 System Maintenance: Time and Date Setting

FIELD	DESCRIPTION
Time Protocol	Enter the time service protocol that your timeserver 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 differences between them are 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)**. Select **Manual** to enter the new time and new date manually.
Time Server Address	Enter the IP address or domain name of your timeserver. Check with your ISP/network administrator if you are unsure of this information. The default is tick.stdtime.gov.tw
Current Time	This field displays an updated time only when you reenter this menu.
New Time	Enter the new time in hour, minute and second format. This field is available when you select **Manual** in the **Time Protocol** field.
Current Date	This field displays an updated date only when you reenter this menu.
New Date	Enter the new date in year, month and day format. This field is available when you select **Manual** in the **Time Protocol** field.
Time Zone	Press [SPACE BAR] and then [ENTER] to set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Saving	Daylight Saving Time is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daylight time in the evenings. If you use daylight savings time, then choose **Yes**.
Start Date (mm-nth-week-hr)	Configure the day and time when Daylight Saving Time starts if you selected **Yes** in the **Daylight Saving** field. The **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).

Table 200 Menu 24.10 System Maintenance: Time and Date Setting

FIELD	DESCRIPTION
End Date (mm-nth-week-hr)	Configure the day and time when Daylight Saving Time ends if you selected **Yes** in the **Daylight Saving** field. The **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).
Once you have filled in this menu, press [ENTER] at the message "Press ENTER to Confirm or ESC to Cancel" to save your configuration, or press [ESC] to cancel.	

40.3.1 Resetting the Time

The ZyWALL resets the time in three instances:

- On leaving menu 24.10 after making changes.
- When the ZyWALL starts up, if there is a timeserver configured in menu 24.10.
- 24-hour intervals after starting.

C HAPTER 41
Remote Management

This chapter covers remote management found in SMT menu 24.11.

41.1 Remote Management

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

You may manage your ZyWALL from a remote location via:

- Internet (WAN only)
- ALL (LAN, WAN and DMZ)
- LAN only
- Neither (Disable)
- DMZ only

> **Note:** When you Choose **WAN only** or **ALL** (LAN & WAN&DMZ), 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.

Enter 11 from menu 24 to bring up **Menu 24.11 - Remote Management Control**.

Figure 349 Menu 24.11 – Remote Management Control

```
           Menu 24.11 - Remote Management Control

   TELNET Server:      Port = 23          Access = ALL
                       Secure Client IP = 0.0.0.0
   FTP Server:         Port = 21          Access = ALL
                       Secure Client IP = 0.0.0.0
   SSH  Server:        Certificate = auto_generated_self_signed_cert
                       Port = 22          Access = ALL
                       Secure Client IP = 0.0.0.0
   HTTPS Server:       Certificate = auto_generated_self_signed_cert
                       Authenticate Client Certificates = No
                       Port = 443         Access = ALL
                       Secure Client IP = 0.0.0.0
   HTTP Server:        Port = 80          Access = ALL
                       Secure Client IP = 0.0.0.0
   SNMP Service:       Port = 161         Access = ALL
                       Secure Client IP = 0.0.0.0
   DNS Service:        Port = 53          Access = ALL
                       Secure Client IP = 0.0.0.0


                    Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this screen.

Table 201 Menu 24.11 – Remote Management Control

FIELD	DESCRIPTION
Telnet Server FTP Server SSH Server HTTPS Server HTTP Server SNMP Service DNS Service	Each of these read-only labels denotes a service that you may use to remotely manage the ZyWALL.
Port	This field shows the port number for the service or protocol. You may change the port number if needed, but you must use the same port number to access the ZyWALL.
Access	Select the access interface (if any) by pressing [SPACE BAR], then [ENTER] to choose from: **LAN only**, **WAN only**, **DMZ only**, **ALL** or **Disable**.
Secure Client IP	The default 0.0.0.0 allows any client to use this service to remotely manage the ZyWALL. Enter an IP address to restrict access to a client with a matching IP address.
Certificate	Press [SPACE BAR] and then [ENTER] to select the certificate that the ZyWALL will use to identify itself. The ZyWALL is the SSL server and must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the ZyWALL).
Authenticate Client Certificates	Select **Yes** by pressing [SPACE BAR], then [ENTER] to require the SSL client to authenticate itself to the ZyWALL by sending the ZyWALL a certificate. To do that the SSL client must have a CA-signed certificate from a CA that has been imported as a trusted CA on the ZyWALL (see Appendix L Importing Certificates for details).
Once you have filled in this menu, press [ENTER] at the message "Press ENTER to Confirm or ESC to Cancel" to save your configuration, or press [ESC] to cancel.	

41.1.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

1 A filter in menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a Telnet, FTP or Web service.

2 You have disabled that service in menu 24.11.

3 The IP address in the **Secured Client IP** field (menu 24.11) does not match the client IP address. If it does not match, the ZyWALL will disconnect the session immediately.

4 There is an SMT console session running.

5 There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.

6 There is a firewall rule that blocks it.

CHAPTER 42
IP Policy Routing

This chapter covers setting and applying policies used for IP routing.

42.1 IP Routing Policy Summary

Menu 25 shows the summary of a policy rule, including the criteria and the action of a single policy, and whether a policy is active or not. Each policy contains two lines. The former part is the criteria of the incoming packet and the latter is the action. Between these two parts, separator "|" means the action is taken on criteria matched and separator "=" means the action is taken on criteria not matched.

Figure 350   Menu 25: Sample IP Routing Policy Summary

```
                    Menu 25 - IP Routing Policy Summary

  #   A                        Criteria/Action
 --- - ------------------------------------------------------
 001 N SA=1.1.1.1-1.1.1.1 DA=2.2.2.2-2.2.2.5
       SP=20-25 DP=20-25 P=6 T=NM PR=0             |GW=192.168.1.1 T=MT PR=0
 002 N _____
       _____
 003 N _____
       _____
 004 N _____
       _____
 005 N _____
       _____
 006 N _____
       _____


             Select Command= None           Select Rule= N/A
                 Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

The following table describes the fields in this screen.

Table 202   Menu 25: Sample IP Routing Policy Summary

FIELD	DESCRIPTION
#	This is the policy index number.
A	This displays whether a policy is active (**Y**) or not (**N**).

Table 202   Menu 25: Sample IP Routing Policy Summary (continued)

FIELD	DESCRIPTION
Criteria/Action	This displays the details about to which packets the policy applies and how the policy has the ZyWALL handle those packets. Refer to Table 203 for detailed information.
Select Command	Press [SPACE BAR] to choose from **None**, **Edit**, **Delete**, **Go To Rule**, **Next Page** or **Previous Page** and then press [ENTER]. You must select a rule in the next field when you choose the **Edit**, **Delete** or **Go To** commands. Select **None** and then press [ENTER] to go to the "Press ENTER to Confirm…" prompt. Use **Edit** to create or edit a rule. Use **Delete** to remove a rule. To edit or delete a rule, first make sure you are on the correct page. When a rule is deleted, subsequent rules do not move up in the page list. Use **Go To Rule** to view the page where your desired rule is listed. Select **Next Page** or **Previous Page** to view the next or previous page of rules (respectively).
Select Rule	Type the policy index number you wish to edit or delete and then press [ENTER].
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

Table 203   IP Routing Policy Setup

ABBREVIATION		MEANING
Criterion	SA	Source IP Address
	SP	Source Port
	DA	Destination IP Address
	DP	Destination Port
	P	IP layer 4 protocol number (TCP=6, UDP=17…)
	T	Type of service of incoming packet
	PR	Precedence of incoming packet
Action	GW	Gateway IP address
	T	Outgoing Type of service
	P	Outgoing Precedence
Service	NM	Normal
	MD	Minimum Delay
	MT	Maximum Throughput
	MR	Maximum Reliability
	MC	Minimum Cost

42.2 IP Routing Policy Setup

To setup a routing policy, perform the following procedures:

1 Type 25 in the main menu to open **Menu 25 - IP Routing Policy Summary**.

2 Select **Edit** in the **Select Command** field; type the index number of the rule you want to configure in the **Select Rule** field and press [ENTER] to open **Menu 25.1 - IP Routing Policy Setup** (see the next figure).

Figure 351 Menu 25.1: IP Routing Policy Setup

```
             Menu 25.1 - IP Routing Policy Setup

  Rule Index= 1                           Active= Yes
  Criteria:
    IP Protocol    = 6
    Type of Service= Normal              Packet length= 40
    Precedence     = 0                     Len Comp= Equal
    Source:
      addr start= 1.1.1.1                end= 1.1.1.1
      port start= 20                     end= 25
    Destination:
      addr start= 2.2.2.2                end= 2.2.2.5
      port start= 20                     end= 25
  Action= Matched
    Gateway addr= 192.168.1.1            Log= No
    Type of Service= Max Thruput
    Precedence     = 0
  Edit policy to packets received from= No

                    Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this screen.

Table 204   Menu 25.1: IP Routing Policy Setup

FIELD	DESCRIPTION
Rule Index	This is the index number of the routing policy selected in **Menu 25 - IP Routing Policy Summary**.
Active	Press [SPACE BAR] and then [ENTER] to select **Yes** to activate the policy.
Criteria	
IP Protocol	Enter a number that represents an IP layer 4 protocol, for example, UDP=17, TCP=6, ICMP=1 and Don't care=0.
Type of Service	Prioritize incoming network traffic by choosing from **Don't Care**, **Normal**, **Min Delay**, **Max Thruput** or **Max Reliable**.
Precedence	Precedence value of the incoming packet. Press [SPACE BAR] and then [ENTER] to select a value from **0** to **7** or **Don't Care**.
Packet Length	Type the length of incoming packets (in bytes). The operators in the **Len Comp** (next field) apply to packets of this length.
Len Comp	Press [SPACE BAR] and then [ENTER] to choose from **Equal**, **Not Equal**, **Less**, **Greater**, **Less or Equal** or **Greater or Equal**.
Source	
addr start / end	Source IP address range from start to end.

Table 204   Menu 25.1: IP Routing Policy Setup

FIELD	DESCRIPTION
port start / end	Source port number range from start to end; applicable only for TCP/UDP.
Destination	
addr start / end	Destination IP address range from start to end.
port start / end	Destination port number range from start to end; applicable only for TCP/UDP.
Action	Specifies whether action should be taken on criteria Matched or Not Matched.
Gateway addr	Defines the outgoing gateway address. The gateway must be on the same subnet as the ZYWALL if it is on the LAN, otherwise, the gateway must be the IP address of a remote node. The default gateway is specified as 0.0.0.0.
Type of Service	Set the new TOS value of the outgoing packet. Prioritize incoming network traffic by choosing **Don't Care**, **Normal**, **Min Delay**, **Max Thruput**, **Max Reliable** or **Min Cost**.
Precedence	Set the new outgoing packet precedence value. Values are **0** to **7** or **Don't Care**.
Log	Press [SPACE BAR] and then [ENTER] to select Yes to make an entry in the system log when a policy is executed.
Edit policy to packets received from	Press [SPACE BAR] and then [ENTER] to select Yes or No (default). Select Yes to configure Menu 25.1.1: IP Routing Policy Setup discussed next.
When you have completed this menu, press [ENTER] at the prompt "Press [ENTER] to confirm or [ESC] to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

42.2.1 Applying Policy to Packets

To apply the policy to packets received on the selected interface(s), go to **Menu 25.1: IP Routing Policy Setup** and press [SPACE BAR] to select **Yes** in the **Edit policy to packets received from** field. Press [ENTER] to display **Menu 25.1.1 - IP Routing Policy Setup** (shown next).

Figure 352   Menu 25.1.1: IP Routing Policy Setup

```
        Menu 25.1.1 - IP Routing Policy Setup

                  Apply policy to packets received from:
                    LAN= No
                    DMZ= No
                    ALL WAN= Yes
                        Selected Remote Node index= N/A


        Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this screen.

Table 205   Menu 25.1.1: IP Routing Policy Setup

FIELD	DESCRIPTION
LAN/DMZ/ALL WAN	Press [SPACE BAR] to select **Yes** or **No**. Choose **Yes** and press [ENTER] to apply the policy to packets received on the specific interface(s).
Selected Remote Node index	If you select **No** in the **ALL WAN** field, enter the number of the WAN port.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

42.3 IP Policy Routing Example

If a network has both Internet and remote node connections, you can route Web packets to the Internet using one policy and route FTP packets to a remote network using another policy. See the next figure.

Route 1 represents the default IP route and route 2 represents the configured IP route.

Figure 353   Example of IP Policy Routing
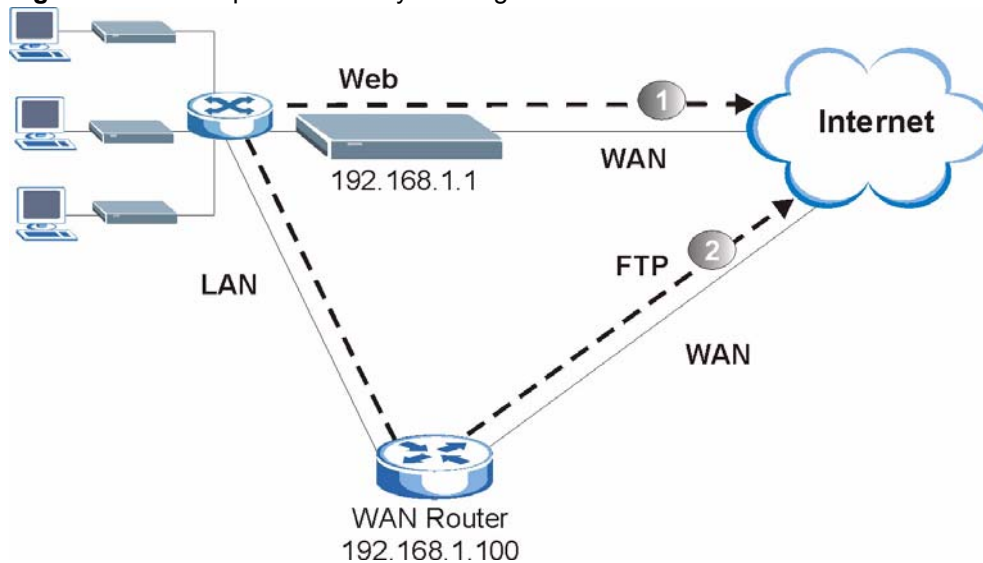
To force Web packets coming from clients with IP addresses of 192.168.1.33 to 192.168.1.64 to be routed to the Internet via the WAN port of the ZyWALL, follow the steps as shown next.

1 Create a rule in **Menu 25.1 - IP Routing Policy Setup** as shown next.

Figure 354 IP Routing Policy Example 1

```
          Menu 25.1 - IP Routing Policy Setup

  Rule Index= 1                          Active= Yes
  Criteria:
   IP Protocol    = 6
   Type of Service= Don't Care        Packet length= 10
   Precedence     = Don't Care          Len Comp= Equal
   Source:
     addr start= 192.168.1.33       end= 192.168.1.64
     port start= 0                  end= N/A
   Destination:
     addr start= 0.0.0.0                end= N/A
     port start= 80                     end= 80
  Action= Matched
   Gateway addr= 192.168.1.1          Log= No
   Type of Service= Normal
   Precedence     = 0
  Edit policy to packets received from= No

                    Press ENTER to Confirm or ESC to Cancel:
```

2 Select **Yes** in the **LAN** field in menu 25.1.1 to apply the policy to packets received on the LAN port.

3 Check **Menu 25 - IP Routing Policy Summary** to see if the rule is added correctly.

4 Create another rule in menu 25.1 for this rule to route packets from any host (IP=0.0.0.0 means any host) with protocol TCP and port FTP access through another gateway (192.168.1.100).

Figure 355 IP Routing Policy Example 2

```
        Menu 25.1 - IP Routing Policy Setup

  Rule Index= 2                            Active= No
  Criteria:
    IP Protocol    = 6
    Type of Service= Don't Care        Packet length= 10
    Precedence    = Don't Care          Len Comp= Equal
    Source:
      addr start= 0.0.0.0              end= N/A
      port start= 0                    end= N/A
    Destination:
      addr start= 0.0.0.0              end= N/A
      port start= 20                   end= 21
  Action= Matched
    Gateway addr= 192.168.1.100        Log= No
    Type of Service= Don't Care
    Precedence     = Don't Care
  Edit policy to packets received from= No

                  Press ENTER to Confirm or ESC to Cancel:
```

5 Select **Yes** in the **LAN** field in menu 25.1.1 to apply the policy to packets received on the LAN port.

6 Check **Menu 25 - IP Routing Policy Summary** to see if the rule is added correctly.

Chapter 42 IP Policy Routing

C HAPTER 43
Call Scheduling

Call scheduling allows you to dictate when a remote node should be called and for how long.

43.1 Introduction to Call Scheduling

The call scheduling feature allows the ZyWALL to manage a remote node and dictate when a remote node should be called and for how long. This feature is similar to the scheduler in a videocassette recorder (you can specify a time period for the VCR to record). You can apply up to 4 schedule sets in **Menu 11.1 - Remote Node Profile. From the main menu, enter 26 to access Menu 26 - Schedule Setup as shown next.**

Figure 356   Schedule Setup

```
                    Menu 26 - Schedule Setup

       Schedule                        Schedule
       Set #      Name                 Set #      Name
       ------     ------------------   ------     ------------------
       1          _____   7          _____
       2          _____   8          _____
       3          _____   9          _____
       4          _____   10         _____
       5          _____   11         _____
       6          _____   12         _____


       Enter Schedule Set Number to Configure= 0
       Edit Name= N/A
       Press ENTER to Confirm or ESC to Cancel:
```

Lower numbered sets take precedence over higher numbered sets thereby avoiding scheduling conflicts. For example, if sets 1, 2, 3 and 4 are applied in the remote node, then set 1 will take precedence over set 2, 3 and 4 as the ZyWALL, by default, applies the lowest numbered set first. Set 2 will take precedence over set 3 and 4, and so on.

You can design up to 12 schedule sets but you can only apply up to four schedule sets for a remote node.

> **Note:** To delete a schedule set, enter the set number and press [SPACE BAR] and then [ENTER] or [DEL] in the Edit Name field.

To set up a schedule set, select the schedule set you want to setup from menu 26 (1-12) and press [ENTER] to see **Menu 26.1 - Schedule Set Setup** as shown next.

Figure 357 Schedule Set Setup

```
            Menu 26.1 - Schedule Set Setup

            Active= Yes
            How Often= Once
            Start Date(yyyy-mm-dd)= N/A
            Once:
              Date(yyyy-mm-dd)= 2000 - 01 - 01
            Weekdays:
              Sunday= N/A
              Monday= N/A
              Tuesday= N/A
              Wednesday= N/A
              Thursday= N/A
              Friday= N/A
              Saturday= N/A
            Start Time(hh:mm)= 00 : 00
            Duration(hh:mm)= 00 : 00
            Action= Forced On

            Press ENTER to Confirm or ESC to Cancel:
            Press Space Bar to Toggle
```

If a connection has been already established, your ZyWALL will not drop it. Once the connection is dropped manually or it times out, then that remote node can't be triggered up until the end of the **Duration**.

Table 206 Schedule Set Setup

FIELD	DESCRIPTION
Active	Press [SPACE BAR] to select **Yes** or **No**. Choose **Yes** and press [ENTER] to activate the schedule set.
Start Date	Enter the start date when you wish the set to take effect in year -month-date format. Valid dates are from the present to 2036-12-31.
How Often	Should this schedule set recur weekly or be used just once only? Press [SPACE BAR] and then [ENTER] to select **Once** or **Weekly**. Both these options are mutually exclusive. If **Once** is selected, then all weekday settings are **N/A**. When **Once** is selected, the schedule rule deletes automatically after the scheduled time elapses.
Once:	
Date	If you selected **Once** in the **How Often** field above, then enter the date the set should activate here in year-month-date format.
Weekdays:	
Day	If you selected **Weekly** in the **How Often** field above, then select the day(s) when the set should activate (and recur) by going to that day(s) and pressing [SPACE BAR] to select **Yes**, then press [ENTER].
Start Time	Enter the start time when you wish the schedule set to take effect in hour-minute format.
Duration	The duration determines how long the ZyWALL is to apply the action configured in the **Action** field. Enter the maximum length of time in hour-minute format.

Table 206 Schedule Set Setup (continued)

FIELD	DESCRIPTION
Action	**Forced On** means that the connection is maintained whether or not there is a demand call on the line and will persist for the time period specified in the **Duration** field.
	Forced Down means that the connection is blocked whether or not there is a demand call on the line.
	Enable Dial-On-Demand means that this schedule permits a demand call on the line.
	Disable Dial-On-Demand means that this schedule prevents a demand call on the line.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

Once your schedule sets are configured, you must then apply them to the desired remote node(s). Enter 11 from the Main Menu and then enter the target remote node index. Press [SPACE BAR] and then [ENTER] to select **PPPoE** in the **Encapsulation** field to make the schedule sets field available as shown next.

Figure 358 Applying Schedule Set(s) to a Remote Node (PPPoE)

```
                   Menu 11.1 - Remote Node Profile

     Rem Node Name= ChangeMe          Route= IP
     Active= Yes

     Encapsulation= PPPoE             Edit IP= No
     Service Type= Standard           Telco Option:
     Service Name=                      Allocated Budget(min)= 0
     Outgoing=                          Period(hr)= 0
       My Login=                        Schedules= 1,2,3,4
       My Password= ********            Nailed-Up Connection= No
       Authen= CHAP/PAP
                                      Session Options:
                                        Edit Filter Sets= No
                                        Idle Timeout(sec)= 100



          Press ENTER to Confirm or ESC to Cancel:
```

You can apply up to four schedule sets, separated by commas, for one remote node. Change the schedule set numbers to your preference(s).

Figure 359 Applying Schedule Set(s) to a Remote Node (PPTP)

```
                    Menu 11.1 - Remote Node Profile

     Rem Node Name= ChangeMe              Route= IP
     Active= Yes

     Encapsulation= PPTP             Edit IP= No
     Service Type= Standard           Telco Option:
                                        Allocated Budget(min)= 0
     Outgoing=                          Period(hr)= 0
       My Login=                        Schedules= 1,2,3,4
       My Password= ********            Nailed-up Connections= No
       Retype to Confirm= ********
       Authen= CHAP/PAP
     PPTP:                              Session Options:
       My IP Addr=                        Edit Filter Sets= No
       My IP Mask=                        Idle Timeout(sec)= 100
       Server IP Addr=
       Connection ID/Name=


      Press ENTER to Confirm or ESC to Cancel:
```

C HAPTER 44
VPN/IPSec Setup

This chapter introduces the VPN SMT menus.

44.1 Introduction

The VPN/IPSec main SMT menu has these main submenus:

1 Define VPN policies in menu 27.1 submenus, including security policies, endpoint IP addresses, peer IPSec router IP address and key management.

2 **Menu 27.2 - SA Monitor** allows you to manage (refresh or disconnect) your SA connections.

This is an overview of the VPN menu tree.

Figure 360 VPN SMT Menu Tree
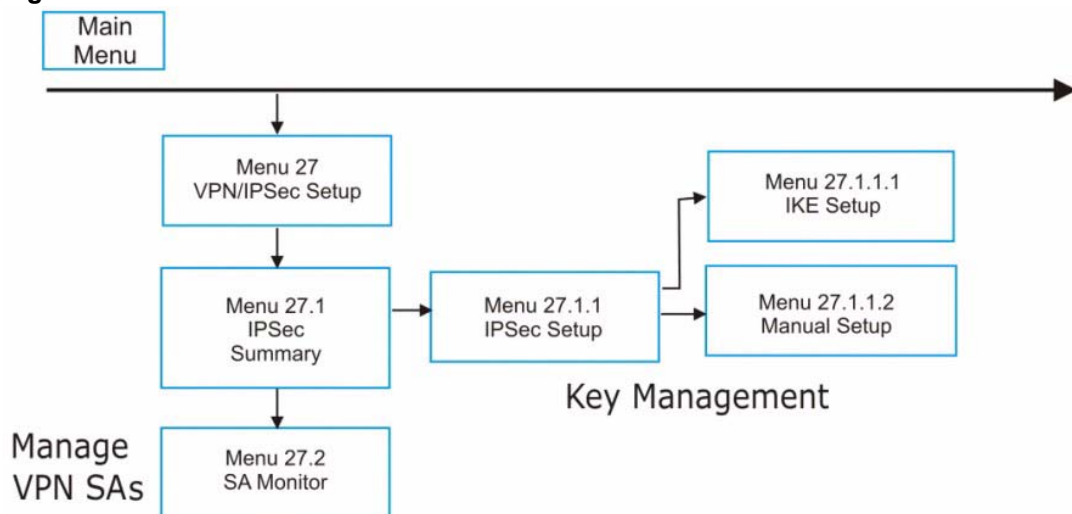
From the main menu, enter 27 to display the first VPN menu (shown next).

Figure 361   Menu 27: VPN/IPSec Setup

```
                    Menu 27 - VPN/IPSec Setup

                         1. IPSec Summary
                         2. SA Monitor




            Enter Menu Selection Number:
```

44.2 IPSec Summary Screen

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). Edit or create an IPSec rule by selecting an index number and then configuring the associated submenus.

Figure 362   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    Taiwan   Y  192.168.1.35       192.168.1.38    Tunnel   ESP AES MD5
       IKE         172.16.2.40        172.16.2.46           193.81.13.2
002    zw50     N  1.1.1.1             1.1.1.1        Tunnel   AH SHA1
       IKE         4.4.4.4            255.255.0.0          zw50test.zyxel.
003    China    N  192.168.1.40       192.168.1.42   Tunnel  ESP DES MD5
       IKE         N/A                   N/A                   0.0.0.0
004

005

              Select Command= None       Select Rule= N/A

Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this screen.

Table 207 Menu 27.1: IPSec Summary

FIELD	DESCRIPTION
#	This is the VPN policy index number.
Name	This field displays the unique identification name for this VPN rule. The name may be up to 32 characters long but only 10 characters will be displayed here.
A	**Y** signifies that this VPN rule is active.
Local Addr Start	When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Single**, this is a static IP address on the LAN behind your ZyWALL.
	When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Range**, this is the beginning (static) IP address, in a range of computers on the LAN behind your ZyWALL.
	When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **SUBNET**, this is a static IP address on the LAN behind your ZyWALL.
Addr End / Mask	When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Single**, this is the same (static) IP address as in the **Local Addr Start** field.
	When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Range**, this is the end (static) IP address, in a range of computers on the LAN behind your ZyWALL.
	When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **SUBNET**, this is a subnet mask on the LAN behind your ZyWALL.
Encap	This field displays **Tunnel** mode or **Transport** mode. See earlier for a discussion of these. You need to finish configuring the VPN policy in menu 27.1.1.1 or 27.1.1.2 if **???** is displayed.
IPSec Algorithm	This field displays the security protocols used for an SA. **ESP** provides confidentiality and integrity of data by encrypting the data and encapsulating it into IP packets. Encryption methods include 56-bit **DES**, 168-bit **3DES** and 128-bit **AES**. **NULL** denotes a tunnel without encryption.
	AH (Authentication Header) provides strong integrity and authentication by adding authentication information to IP packets. This authentication information is calculated using header and payload data in the IP packet. This provides an additional level of security. **AH** choices are **MD5** (default - 128 bits) and **SHA -1**(160 bits)**.**
	Both **AH** and **ESP** increase the ZyWALL's processing requirements and communications latency (delay).
	You need to finish configuring the VPN policy in menu 27.1.1.1 or 27.1.1.2 if **???** is displayed.
Key Mgt	This field displays the SA's type of key management, (**IKE** or **Manual**).
Remote Addr Start	When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Single**, this is a static IP address on the network behind the remote IPSec router.
	When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Range**, this is the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router.
	When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **SUBNET**, this is a static IP address on the network behind the remote IPSec router.
	This field displays **N/A** when you configure the **Secure Gw Addr** field in SMT 27.1.1 to 0.0.0.0.

Table 207 Menu 27.1: IPSec Summary (continued)

FIELD	DESCRIPTION
Addr End / Mask	When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Single**, this is the same (static) IP address as in the **Remote Addr Start** field.
	When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Range**, this is the end (static) IP address, in a range of computers on the network behind the remote IPSec router.
	When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **SUBNET**, this is a subnet mask on the network behind the remote IPSec router.
	This field displays **N/A** when you configure the **Secure Gw Addr** field in SMT 27.1.1 to 0.0.0.0.
Secure GW Addr	This is the WAN IP address or the domain name (up to the first 15 characters are displayed) of the IPSec router with which you are making the VPN connection. This field displays **0.0.0.0** when you configure the **Secure Gw Addr** field in SMT 27.1.1 to 0.0.0.0.
Select Command	Press [SPACE BAR] to choose from **None**, **Edit**, **Delete**, **Go To Rule**, **Next Page** or **Previous Page** and then press [ENTER]. You must select a rule in the next field when you choose the **Edit**, Delete or **Go To** commands.
	Select **None** and then press [ENTER] to go to the "Press ENTER to Confirm…" prompt.
	Use **Edit** to create or edit a rule. Use **Delete** to remove a rule. To edit or delete a rule, first make sure you are on the correct page. When a VPN rule is deleted, subsequent rules do not move up in the page list.
	Use **Go To Rule** to view the page where your desired rule is listed.
	Select **Next Page** or **Previous Page** to view the next or previous page of rules (respectively).
Select Rule	Type the VPN rule index number you wish to edit or delete and then press [ENTER].
	When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.

44.3 IPSec Setup

Select **Edit** in the **Select Command** field; type the index number of a rule in the **Select Rule** field and press [ENTER] to edit the VPN using the menu shown next.

Figure 363 Menu 27.1.1: IPSec Setup

```
                 Menu 27.1.1 - IPSec Setup

    Index= 1         Name= Taiwan
    Active= Yes      Keep Alive= No    NAT Traversal= No
    Local ID type = IP       Content:
    My Addr Type= IP          Address= 0.0.0.0
    Peer ID type= IP          Content:
    Secure Gateway Address= zwtest.zyxel.com.tw
    Protocol= 0      DNS Server= 0.0.0.0
    Local:      Addr Type= RANGE
                    IP Addr Start= 192.168.1.35   End/Subnet Mask=
                                            192.168.1.38
                    Port Start= 0                 End= N/A
    Remote:     Addr Type= SUBNET
                    IP Addr Start= 4.4.4.4        End/Subnet Mask=
                                            255.255.0.0
                    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:
```

> **Note:** You must also configure menu 27.1.1.1 or menu 27.1.1.2 to fully configure and use a VPN.

The following table describes the fields in this screen.

Table 208 Menu 27.1.1: IPSec Setup

FIELD	DESCRIPTION
Index	This is the VPN rule index number you selected in the previous menu.
Name	Enter a unique identification name for this VPN rule. The name may be up to 32 characters long but only 10 characters will be displayed in **Menu 27.1 - IPSec Summary**.
Active	Press [SPACE BAR] to choose either **Yes** or **No**. Choose **Yes** and press [ENTER] to activate the VPN tunnel. This field determines whether a VPN rule is applied before a packet leaves the firewall.
Keep Alive	Press [SPACE BAR] to choose either **Yes** or **No**. Choose **Yes** and press [ENTER] to have the ZyWALL automatically re-initiate the SA after the SA lifetime times out, even if there is no traffic. The remote IPSec router must also have keep alive enabled in order for this feature to work.
NAT Traversal	Choose **Yes** and press [ENTER] 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.

Table 208 Menu 27.1.1: IPSec Setup (continued)

FIELD	DESCRIPTION
Local ID type	Press [SPACE BAR] to choose **IP**, **DNS**, or **E-mail** and press [ENTER]. 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.
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 **Address** field (refer to the **My Addr Type** and **Address** fields 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.
My Addr Type	**My Address** identifies the WAN IP address of the ZyWALL. You can select **IP** and enter the ZyWALL's static WAN IP address (if it has one) or leave the **Address** field set to 0.0.0.0. The VPN tunnel has to be rebuilt if the **My Address** changes after setup. The following applies if the **Address** field is configured as 0.0.0.0: • When the WAN port operation mode is set to Active/Passive, the ZyWALL uses the IP address (static or dynamic) of the WAN port that is in use. • When the WAN port operation mode is set to Active/Active, the ZyWALL uses the IP address (static or dynamic) of the primary (highest priority) WAN port to set up the VPN tunnel as long as the corresponding WAN1 or WAN2 connection is up. If the corresponding WAN1 or WAN2 connection goes down, the ZyWALL uses the IP address of the other WAN port. • If both WAN connections go down, the ZyWALL uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect. See Chapter 7 WAN Screens or Chapter 27 WAN and Dial Backup Setup and Chapter 31 Route Setup for details on dial backup and traffic redirect. Select **DDNS** and enter one of the dynamic domain names that you have configured (in the **DDNS** screen) to have the ZyWALL use that dynamic domain name's IP address.
Address	When you select **IP** in the **My Addr Type** field, enter the IP address of your ZyWALL. When you select **DNS** in the **My Addr Type** field, type a domain name.
Peer ID type	Press [SPACE BAR] to choose **IP**, **DNS**, or **E-mail** and press [ENTER]. 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.

Table 208 Menu 27.1.1: IPSec Setup (continued)

FIELD	DESCRIPTION
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 **Secure Gateway Address** field (refer to the **Secure 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 Peer ID Type** with the following situations: • There is a NAT router between the two IPSec routers. • You want the ZyWALL to distinguish between VPN connection requests coming in from remote IPSec routers with dynamic WAN IP addresses. With either **Authentication Method** (**Pre-Shared Key** or **Certificate**) in menu 27.1.1.1, if you use **IP** as the peer ID type and configure the content as **0.0.0.0** (or blank) and the **Secure Gateway Address** is also configured as **0.0.0.0**, the ZyWALL does not check the peer's ID content. Regardless of how you configure the **ID Type** and **Content** fields, active rules cannot have overlapping local and remote IP address ranges.
Secure Gateway Address	Type the IP address or the domain name (up to 31 characters) of the IPSec router with which you're making the VPN connection. Set this field to 0.0.0.0 if the remote IPSec router has a dynamic WAN IP address (the **Key Management** field must be set to **IKE**, see later).
Protocol	Enter 1 for ICMP, 6 for TCP, 17 for UDP, etc. 0 is the default and signifies any protocol.
DNS Server	If there is a private DNS server that services the VPN, type its IP address here. The ZyWALL assigns this additional DNS server to the ZyWALL's DHCP clients that have IP addresses in this IPSec rule's range of local addresses. A DNS server allows clients on the VPN to find other computers and servers on the VPN by their (private) domain names.
Local	Local IP addresses must be static and correspond to the remote IPSec router's configured remote IP addresses. Two active SAs can have the same configured 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. In order to have more than one active rule with the **Secure Gateway Address** field set to **0.0.0.0**, the ranges of the local IP addresses cannot overlap between rules. If you configure an active rule with **0.0.0.0** in the **Secure Gateway Address** field and the LAN's full IP address range as the local IP address, then you cannot configure any other active rules with the **Secure Gateway Address** field set to **0.0.0.0**.
Addr Type	Press [SPACE BAR] to choose **SINGLE**, **RANGE**, or **SUBNET** and press [ENTER]. Select **SINGLE** with a single IP address. Select **RANGE** for a specific range of IP addresses. Select **SUBNET** to specify IP addresses on a network by their subnet mask.
IP Addr Start	When the **Addr Type** field is configured to **Single**, enter a static IP address on the LAN behind your ZyWALL. When the **Addr Type** field is configured to **Range**, enter the beginning (static) IP address, in a range of computers on your LAN behind your ZyWALL. When the **Addr Type** is configured to **SUBNET**, this is a (static) IP address on the LAN behind your ZyWALL.

Table 208   Menu 27.1.1: IPSec Setup (continued)

FIELD	DESCRIPTION
End	When the **Addr Type** field is configured to **Single**, this field is **N/A**.
	When the **Addr Type** field is configured to **Range**, enter the end (static) IP address, in a range of computers on the LAN behind your ZyWALL.
	When the **Addr Type** field is configured to **SUBNET**, this is a subnet mask on the LAN behind your ZyWALL.
Port Start	0 is the default and signifies any port. Type a port number from 0 to 65535. You cannot create a VPN tunnel if you try to connect using a port number that does not match this port number or range of port numbers.
	Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3
End	Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field. This field is **N/A** when 0 is configured in the **Port Start** field.
Remote	Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses. The remote fields are **N/A** when the **Secure Gateway Address** field is configured to 0.0.0.0.
	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.
Addr Type	Press [SPACE BAR] to choose **SINGLE**, **RANGE**, or **SUBNET** and press [ENTER]. Select **SINGLE** with a single IP address. Use **RANGE** for a specific range of IP addresses. Use **SUBNET** to specify IP addresses on a network by their subnet mask.
IP Addr Start	When the **Addr Type** field is configured to **Single**, enter a static IP address on the network behind the remote IPSec router.
	When the **Addr Type** field is configured to **Range**, enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router.
	When the **Addr Type** field is configured to **SUBNET**, enter a static IP address on the network behind the remote IPSec router.
	This field displays **N/A** when you configure the **Secure Gateway Address** field to 0.0.0.0.
End	When the **Addr Type** field is configured to **Single**, this field is **N/A**.
	When the **Addr Type** field is configured to **Range**, enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router.
	When the **Addr Type** field is configured to **SUBNET**, enter a subnet mask on the network behind the remote IPSec router.
	This field displays **N/A** when you configure the **Secure Gateway Address** field to 0.0.0.0.
Port Start	0 is the default and signifies any port. Type a port number from 0 to 65535. Someone behind the remote IPSec router cannot create a VPN tunnel when attempting to connect using a port number that does not match this port number or range of port numbers.
	Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.
End	Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field. This field is **N/A** when 0 is configured in the **Port Start** field.
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**.
	Press [SPACE BAR] to select **Yes** or **No**. Choose **Yes** and press [ENTER] to enable replay detection.

Table 208 Menu 27.1.1: IPSec Setup (continued)

FIELD	DESCRIPTION
Key Management	Press [SPACE BAR] to choose either **IKE** or **Manual** and then press [ENTER]. **Manual** is useful for troubleshooting if you have problems using **IKE** key management.
Edit Key Management Setup	Press [SPACE BAR] to change the default **No** to **Yes** and then press [ENTER] to go to a key management menu for configuring your key management setup (described later). If you set the **Key Management** field to **IKE**, this will take you to **Menu 27.1.1.1 – IKE Setup**. If you set the **Key Management** field to **Manual**, this will take you to **Menu 27.1.1.2 – Manual Setup**.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

44.4 IKE Setup

To edit this menu, the **Key Management** field **Menu 27.1.1 - IPSec Setup** must be set to **IKE**. 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**.

Figure 364   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= qwer1234
                Certificate= N/A
                Encryption Algorithm= AES
                Authentication Algorithm= SHA1
                SA Life Time (Seconds)= 300
                Key Group= DH1
              Phase 2
                Active Protocol= ESP
                Encryption Algorithm= AES
                Authentication Algorithm= MD5
                SA Life Time (Seconds)= 2880
                Encapsulation= Tunnel
                Perfect Forward Secrecy (PFS)= None


            Press ENTER to Confirm or ESC to Cancel:
          Press Space Bar to Toggle.
```

The following table describes the fields in this screen.

Table 209 Menu 27.1.1.1: IKE Setup

FIELD	DESCRIPTION
Phase 1	
Negotiation Mode	Press [SPACE BAR] to choose from **Main** or **Aggressive** and then press [ENTER]. See earlier for a discussion of these modes. Multiple SAs connecting through a secure gateway must have the same negotiation mode.
Authentication Method	Select **Pre-Shared Key** to use a pre-shared key to identify the ZyWALL and the remote IPSec router. 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.
	Select **Certificate** to identify the ZyWALL and the remote IPSec router by certificates.
PSK	ZyWALL gateways authenticate an IKE VPN session by matching pre-shared keys. Pre-shared keys are best for small networks with fewer than ten nodes. Enter your pre-shared key here. Enter up to 31 characters. Any character may be used, including spaces, but trailing spaces are truncated.
	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	Press [SPACE BAR] to choose the certificate to use for this VPN tunnel. You must have certificates already configured in the **My Certificates** web configurator screen
Encryption Algorithm	The ZyWALL and the remote IPSec router generate an encryption key from the Diffie-Hellman key exchange. ZyWALL **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 slightly increased latency and decreased throughput.
	This implementation of **AES** uses a 128-bit key. **AES** is faster than **3DES**.
	Press [SPACE BAR] to choose from **DES**, **3DES** or **AES** and then press [ENTER].
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 slightly slower.
	Press [SPACE BAR] to choose from **SHA1** or **MD5** and then press [ENTER].
SA Life Time (Seconds)	Define the length of time before an IKE Security Association 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.
Phase 2	
Active Protocol	Press [SPACE BAR] to choose from **ESP** or **AH** and then press [ENTER]. See earlier for a discussion of these protocols.
Encryption Algorithm	Press [SPACE BAR] to choose from **NULL**, **DES**, **3DES** or **AES** and then press [ENTER]. Select **NULL** to set up a tunnel without encryption.
Authentication Algorithm	Press [SPACE BAR] to choose from **SHA1** or **MD5** and then press [ENTER].
SA Life Time (Seconds)	Define the length of time before an IPSec Security Association automatically renegotiates in this field. It may range from 180 to 3,000,000 seconds (almost 35 days).

Table 209 Menu 27.1.1.1: IKE Setup (continued)

FIELD	DESCRIPTION
Encapsulation	Press [SPACE BAR] to choose from **Tunnel** mode or **Transport** mode and then press [ENTER]. See earlier for a discussion of these.
Perfect Forward Secrecy (PFS)	Perfect Forward Secrecy (PFS) is disabled (**None**) by default in phase 2 IPSec SA setup. This allows faster IPSec setup, but is not so secure. Press [SPACE BAR] and choose from **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).
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

44.5 Manual Setup

You only configure **Menu 27.1.1.2 – Manual Setup** when you select **Manual** in the **Key Management** field in **Menu 27.1.1 – IPSec Setup**. Manual key management is useful if you have problems with **IKE** key management.

44.5.1 Active Protocol

This field is a combination of mode and security protocols used for the VPN. See Chapter 13 Introduction to IPSec for more information on these parameters.

Table 210 Active Protocol: Encapsulation and Security Protocol

MODE	SECURITY PROTOCOL
Tunnel	ESP
Transport	AH

44.5.2 Security Parameter Index (SPI)

To edit this menu, move the cursor to the **Edit Manual Setup** field in **Menu 27.1.1 – IPSec Setup**, press [SPACE BAR] to select **Yes** and then press [ENTER] to go to **Menu 27.1.1.2 – Manual Setup**.

Figure 365 Menu 27.1.1.2: Manual Setup

```
            Menu 27.1.1.2 - Manual Setup

       Active Protocol= ESP Tunnel

       ESP Setup
         SPI (Decimal)= 1234
         Encryption Algorithm= DES
           Key1= 89abcde
           Key2= N/A
           Key3= N/A
         Authentication Algorithm= MD5
           Key= 123456789abcde

       AH Setup
         SPI (Decimal)= N/A
         Authentication Algorithm= N/A
           Key= N/A

       Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this screen.

Table 211 Menu 27.1.1.2: Manual Setup

FIELD	DESCRIPTION
Active Protocol	Press [SPACE BAR] to choose from **ESP Tunnel**, **ESP Transport**, **AH Tunnel** or **AH Transport** and then press [ENTER]. Choosing an **ESP** combination causes the **AH Setup** fields to be non-applicable (**N/A**)
ESP Setup	The **ESP Setup** fields are **N/A** if you chose an **AH Active Protocol**.
SPI (Decimal)	The **SPI** must be unique and from one to four integers ("0" to "9").
Encryption Algorithm	Press [SPACE BAR] to choose from **NULL**, **DES**, **3DES** or **AES** and then press [ENTER]. Fill in the **Key1** field below when you choose **DES** and fill in fields **Key1** to **Key3** when you choose **3DES**. Select **NULL** to set up a tunnel without encryption. When you select **NULL**, you do not enter any encryption keys.
Key1	Enter a unique eight-character key. Any character may be used, including spaces, but trailing spaces are truncated. Fill in the **Key1** field when you choose **DES** and fill in fields **Key1** to **Key3** when you choose **3DES**.
Key2	Enter a unique eight-character key. It can be comprised of any character including spaces (but trailing spaces are truncated).
Key3	Enter a unique eight-character key. It can be comprised of any character including spaces (but trailing spaces are truncated).
Authentication Algorithm	Press [SPACE BAR] to choose from **MD5** or **SHA1** and then press [ENTER].
Key	Enter the authentication key to be used by IPSec if applicable. The key must be unique. Enter 16 characters for **MD5** authentication and 20 characters for **SHA-1** authentication. Any character may be used, including spaces, but trailing spaces are truncated.
AH Setup	The **AH Setup** fields are **N/A** if you chose an **ESP Active Protocol**.

Table 211 Menu 27.1.1.2: Manual Setup (continued)

FIELD	DESCRIPTION
SPI (Decimal)	The **SPI** must be from one to four unique decimal characters ("0" to "9") long.
Authentication Algorithm	Press [SPACE BAR] to choose from **MD5** or **SHA1** and then press [ENTER].
Key	Enter the authentication key to be used by IPSec if applicable. The key must be unique. Enter 16 characters for **MD5** authentication and 20 characters for **SHA-1** authentication. Any character may be used, including spaces, but trailing spaces are truncated.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

C H A P T E R 45
SA Monitor

This chapter teaches you how to manage your SAs by using the SA Monitor in SMT menu 27.2.

45.1 Introduction

A Security Association (SA) is the group of security settings related to a specific VPN tunnel. This menu (shown next) displays active VPN connections.

> **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 the Keep Alive section in Chapter 14 VPN Screens to have the ZyWALL renegotiate an IPSec SA when the SA lifetime expires, even if there is no traffic.

45.2 Using SA Monitor

1 Use the **Refresh** function to display active VPN connections.

2 Use the **Disconnect** function to cut off active connections.

Type 2 in **Menu 27 - VPN/IPSec Setup**, and then press [ENTER] to go to **Menu 27.2 - SA Monitor**.

Figure 366 Menu 27.2: SA Monitor

```
           Menu 27.2 - SA Monitor

   #                 Name                    Encap.  IPSec ALgorithm
   ---         ---------------------------------------  -----------------
   001         Taiwan : 3.3.3.1 - 3.3.3.3.100 Tunnel   ESP DES MD5
   002
   003
   004
   005
   006
   007
   008
   009
   010
                          Select Command= Refresh
                          Select Connection= 1

   Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this screen.

Table 212 Menu 27.2: SA Monitor

FIELD	DESCRIPTION
#	This is the security association index number.
Name	This field displays the identification name for this VPN policy. This name is unique for each connection where the secure gateway IP address is a public static IP address.
	When the secure gateway IP address is 0.0.0.0 (as discussed in the last chapter), there may be different connections using this same VPN rule. In this case, the name is followed by the remote IP address as configured in **Menu 27.1.1. – IPSec Setup**. Individual connections using the same VPN rule may be terminated without affecting other connections using the same rule.
Encap.	This field displays **Tunnel** mode or **Transport** mode. See previous for discussion.
IPSec ALgorithm	This field displays the security protocols used for an SA. **ESP** provides confidentiality and integrity of data by encrypting the data and encapsulating it into IP packets. Encryption methods include 56-bit **DES**, 168-bit **3DES** and 128-bit **AES**. **NULL** denotes a tunnel without encryption.
	An incoming SA may have an **AH** in addition to **ESP**. The Authentication Header provides strong integrity and authentication by adding authentication information to IP packets. This authentication information is calculated using header and payload data in the IP packet. This provides an additional level of security. **AH** choices are **MD5** (default - 128 bits) and **SHA -1**(160 bits).
	Both **AH** and **ESP** increase ZyWALL processing requirements and communications latency (delay).
Select Command	Press [SPACE BAR] to choose from **Refresh**, **Disconnect**, **None**, **Next Page**, or **Previous Page** and then press [ENTER]. You must select a connection in the next field when you choose the **Disconnect** command. **Refresh** displays current active VPN connections. **None** allows you to jump to the "Press ENTER to Confirm…" prompt.
	Select **Next Page** or **Previous Page** to view the next or previous page of rules (respectively).

Table 212   Menu 27.2: SA Monitor (continued)

FIELD	DESCRIPTION
Select Connection	Type the VPN connection index number that you want to disconnect and then press [ENTER].
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.	

CHAPTER 46
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.

46.1 Problems Starting Up the ZyWALL

Table 213   Troubleshooting the Start-Up of Your ZyWALL

PROBLEM	CORRECTIVE ACTION	
None of the LEDs turn on when you turn on the ZyWALL.	Make sure that you have the included power adaptor or cord connected to the ZyWALL and to an appropriate power source.	
	If the error persists, you may have a hardware problem. In this case, you should contact your vendor.	
Cannot access the ZyWALL via the console port.	1. Check to see if the ZyWALL is connected to your computer's console port.	
	2. Check to see if the communications program is configured correctly. The communications software should be configured as follows:	VT100 terminal emulation
		9600 bps is the default speed on leaving the factory. Try other speeds in case the speed has been changed.
		No parity, 8 data bits, 1 stop bit, data flow set to none.

46.2 Problems with the LAN Interface

Table 214   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.

46.3 Problems with the DMZ Interface

Table 215   Troubleshooting the DMZ Interface

PROBLEM	CORRECTIVE ACTION
Cannot access servers on the DMZ from the LAN.	Check your Ethernet cable type and connections. Refer to the Quick Start Guide for DMZ connection instructions.
	Make sure the Ethernet adapters on the LAN computer and the DMZ server are installed and functioning properly.
	Verify that the IP address of the DMZ port and the LAN port are on separate subnets.
	Make sure that NAT is configured for your DMZ servers.
Cannot ping any computer on the DMZ.	Check the 10M/100M DMZ 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 servers are on the same subnet.

46.4 Problems with the WAN Interface

Table 216   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 7 WAN Screens or Chapter 29 Internet Access.
	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 7 WAN Screens or Chapter 27 WAN and Dial Backup Setup. 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 Chapter 3 Wizard Setup or Chapter 26 SMT Menu 1 - General Setup.

46.5 Problems with Internet Access

Table 217   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 7 WAN Screens or Chapter 29 Internet Access and verify your settings.

46.6 Problems with the Password

Table 218   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 the Resetting the ZyWALL section in Chapter 2 Introducing the Web Configurator for details.

46.7 Problems with Remote Management

Table 219   Troubleshooting Telnet

PROBLEM	CORRECTIVE ACTION
Cannot access the ZyWALL from the LAN or WAN.	Refer to the Remote Management Limitations section in Chapter 21 Remote Management 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 the Problems with the LAN Interface section for instructions on checking your LAN connection.
	Refer to the Problems with the WAN Interface section for instructions on checking your WAN connection.

Appendix A
Hardware Specifications

Table 220   General Specifications

Power Adaptor Specification	Input AC 120V / 60Hz; Output
MTBF	100000 hrs (Mean Time Between Failures)
Operation Temperature	0º C ~ 40º C
Ethernet Specification for WAN	10/100Mbps Half / Full Auto-negotiation
Ethernet Specification for LAN/ VPN Ports	10/100Mbps Half / Full Auto-negotiation, Auto-sensing

Cable Pin Assignments

In a serial communications connection, generally a computer is DTE (Data Terminal Equipment) and a modem is DCE (Data Circuit-terminating Equipment). The ZyWALL is DCE when you connect a computer to the console port. The ZyWALL is DTE when you connect a modem to the dial backup port.[1]

---

1. Pins 2,3 and 5 are used.

Figure 367 Console/Dial Backup Port Pin Layout
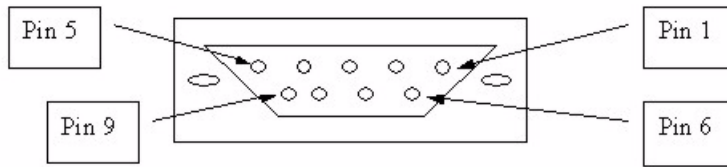
Table 221 Console/Dial Backup Port Pin Assignments

CONSOLE Port RS – 232 (Female) DB-9F	DIAL BACKUP RS – 232 (Male) DB-9M (Not on all models)
Pin 1 = NON Pin 2 = DCE-TXD Pin 3 = DCE –RXD Pin 4 = DCE –DSR Pin 5 = GND Pin 6 = DCE –DTR Pin 7 = DCE –CTS Pin 8 = DCE –RTS PIN 9 = NON	Pin 1 = NON Pin 2 = DTE-RXD Pin 3 = DTE-TXD Pin 4 = DTE-DTR Pin 5 = GND Pin 6 = DTE-DSR Pin 7 = DTE-RTS Pin 8 = DTE-CTS PIN 9 = NON.
The CON/AUX port also has these pin assignments. The CON/AUX switch changes the setting in the firmware only and does not change the CON/AUX port's pin assignments.	ZyWALLs with a CON/AUX port also have a 9-pin adaptor for the console cable with these pin assignments on the male end.

Figure 368 Ethernet Cable Pin Assignments
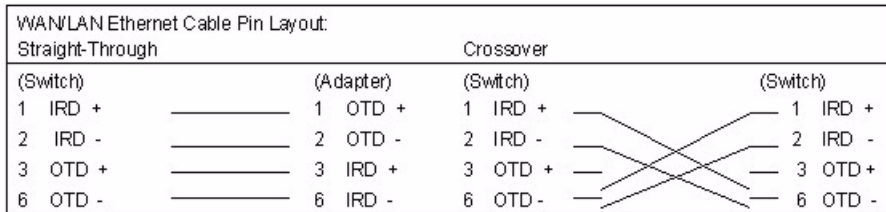
Power Adaptor Specifications

Table 222 North American AC Power Adaptor Specifications

AC Power Adapter model AD48-1201200DUY

Input power: AC120Volts/60Hz/0.25A

Output power: DC12Volts/1.2A

Table 222 North American AC Power Adaptor Specifications (continued)

Power consumption: 10 W
Plug: North American standards
Safety standards: UL, CUL (UL 1950, CSA C22.2 No.234-M90)
AC Power Adapter model AD48-1201200DUY
Input power: AC120Volts/60Hz
Output power: DC12Volts/1.2A
Power consumption: 9 W
Plug: North American standards
Safety standards: UL, CUL (UL1950, CSA C22.2 NO. 234-M90)

Table 223 European Union AC Power Adaptor Specifications

AC Power Adapter model AD-1201200DV
Input power: AC230Volts/50Hz/0.2A
Output power: DC12Volts/1.2A
Power consumption: 10 W
Plug: European Union standards
Safety standards: TUV, CE (EN 60950)
AC Power Adapter model JAD-121200E
Input power: AC230Volts/50Hz,
Output power: DC12Volts/1.2A
Power consumption: 9 W
Plug: European Union standards
Safety standards: TUV, CE (EN 60950)

Table 224 UK AC Power Adaptor Specifications

AC Power Adapter model AD-1201200DK
Input power: AC230Volts/50Hz/0.2A
Output power: DC12Volts/1.2A
Power consumption: 10 W
Plug: United Kingdom standards
Safety standards: TUV, CE (EN 60950, BS7002)

Table 225   Japan AC Power Adaptor Specifications

AC Power Adapter model JOD-48-1124
Input power: AC100Volts/ 50/60Hz/ 27VA
Output power: DC12Volts/1.2A
Power consumption: 10 W
Plug: Japan standards
Safety standards: T-Mark

Table 226   Australia and New Zealand AC Power Adaptor Specification

AC Power Adapter model AD-1201200Ds or AD-121200DS
Input power: AC240Volts/50Hz/0.2A
Output power: DC12Volts/1.2A
Power consumption: 10 W
Plug: Australia and New Zealand standards
Safety standards: NATA (AS 3260)

Appendix B
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 369 WIndows 95/98/Me: Network: Configuration
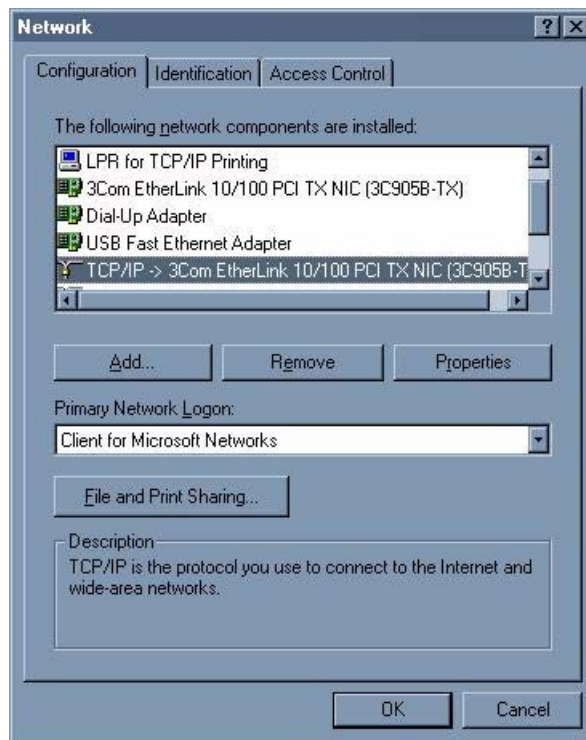
Installing Components

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 370 Windows 95/98/Me: TCP/IP Properties: IP Address
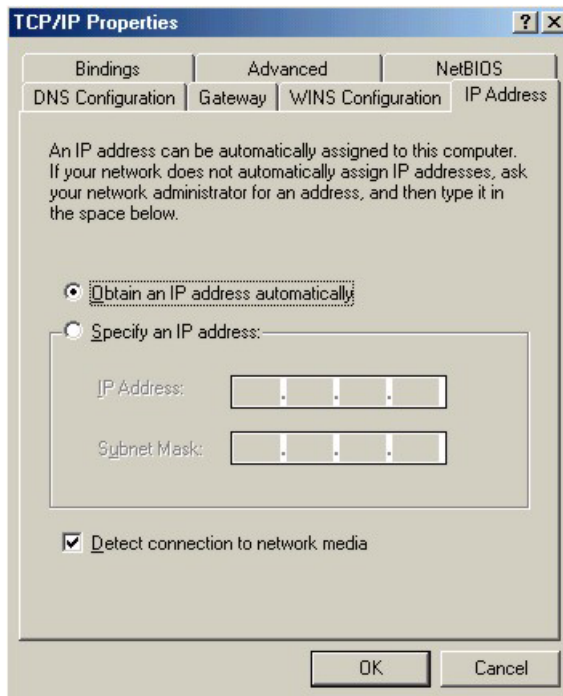
3 Click the **DNS** Configuration tab.

- 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 371 Windows 95/98/Me: TCP/IP Properties: DNS Configuration
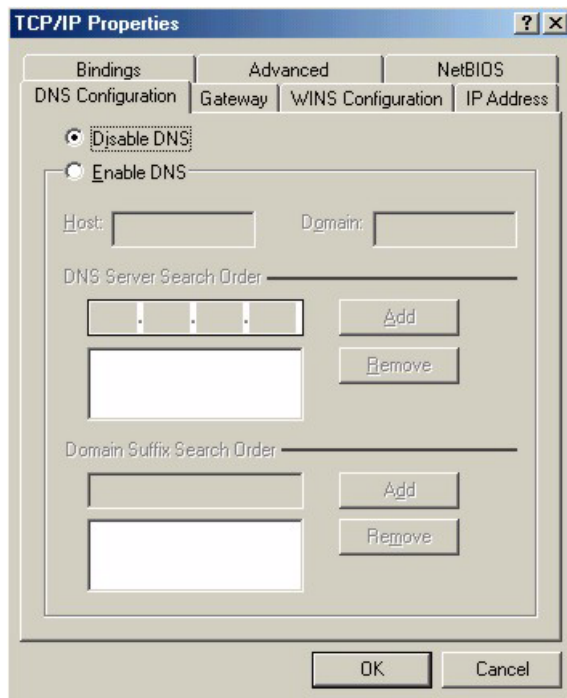
4 Click the **Gateway** tab.

- 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

1 For Windows XP, click **start**, **Control Panel**. In Windows 2000/NT, click **Start**, **Settings**, **Control Panel**.

Figure 372 Windows XP: Start Menu
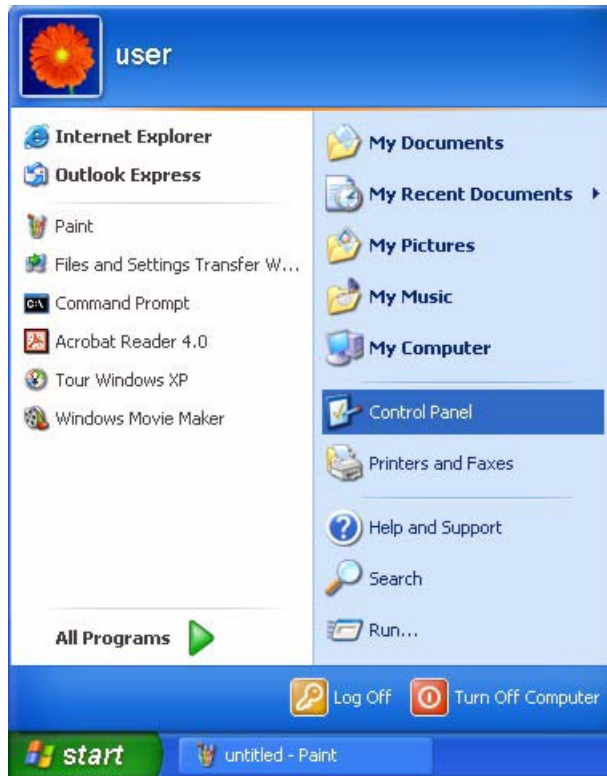
2 For Windows XP, click **Network Connections**. For Windows 2000/NT, click **Network and Dial-up Connections**.

Figure 373 Windows XP: Control Panel

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

Figure 374   Windows XP: Control Panel: Network Connections: Properties
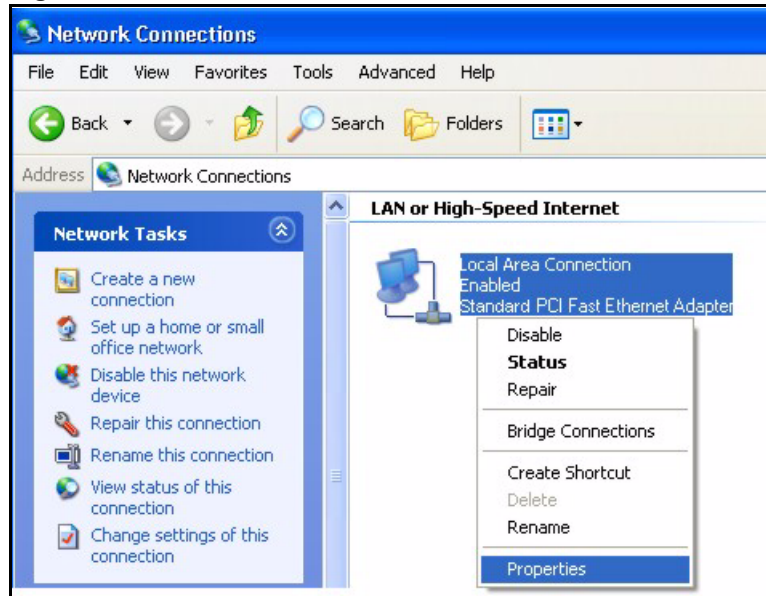
4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and click **Properties**.

Figure 375   Windows XP: Local Area Connection Properties
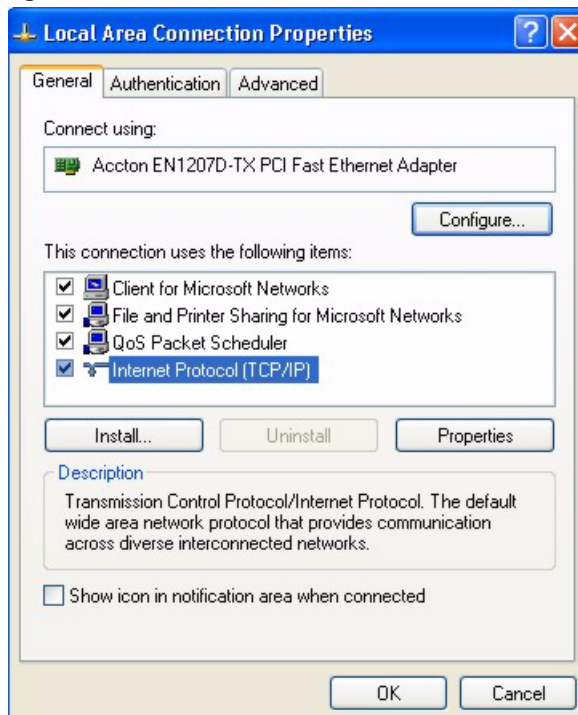
5 The **Internet Protocol TCP/IP Properties** window opens (the **General tab** in Windows XP).

- 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 376 Windows XP: Advanced TCP/IP Settings
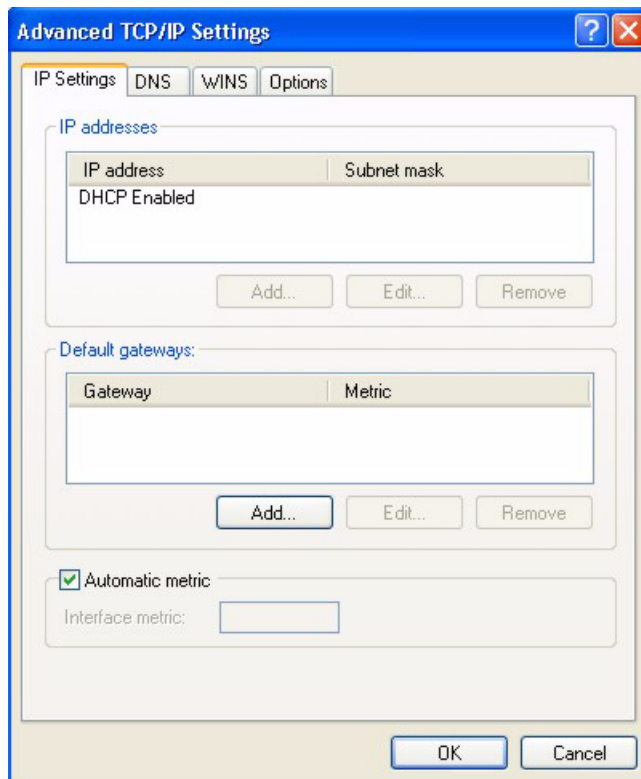
6 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settin**gs tab and click **OK**.

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.

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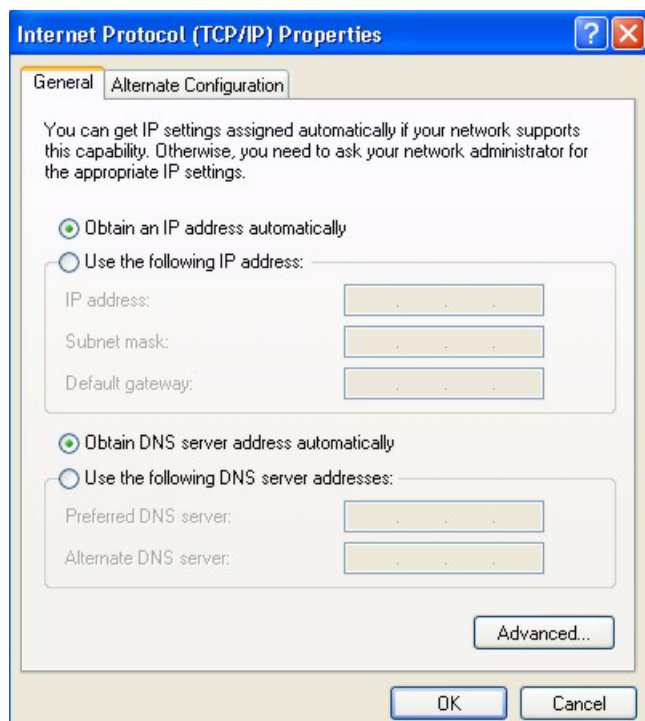
8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

9 Click **OK** to close the **Local Area Connection Properties** window.

10Turn 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 378 Macintosh OS 8/9: Apple Menu
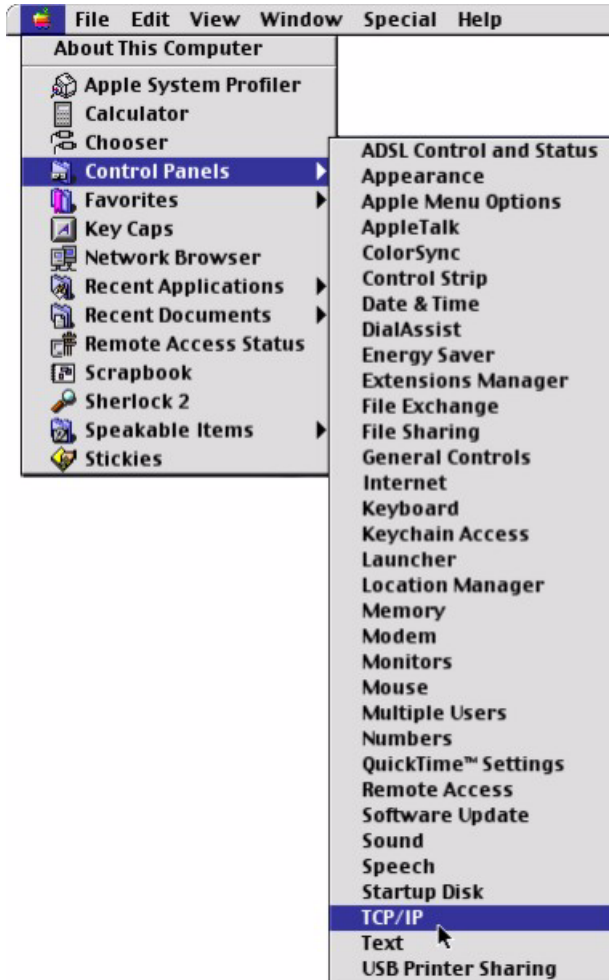
2 Select **Ethernet built-in** from the **Connect via** list.

Figure 379 Macintosh OS 8/9: TCP/IP
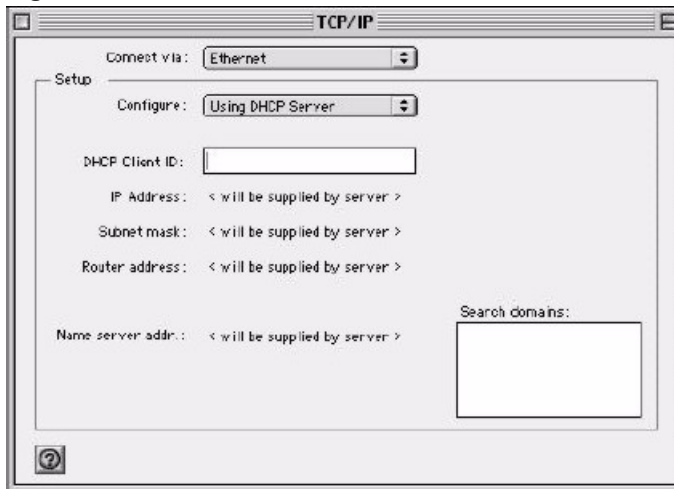
3 For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.

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 380 Macintosh OS X: Apple Menu
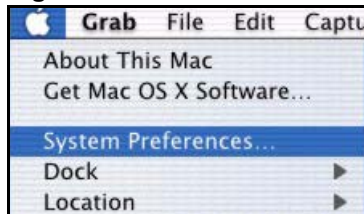
2 Click **Network** in the icon bar.

- 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 381 Macintosh OS X: Network
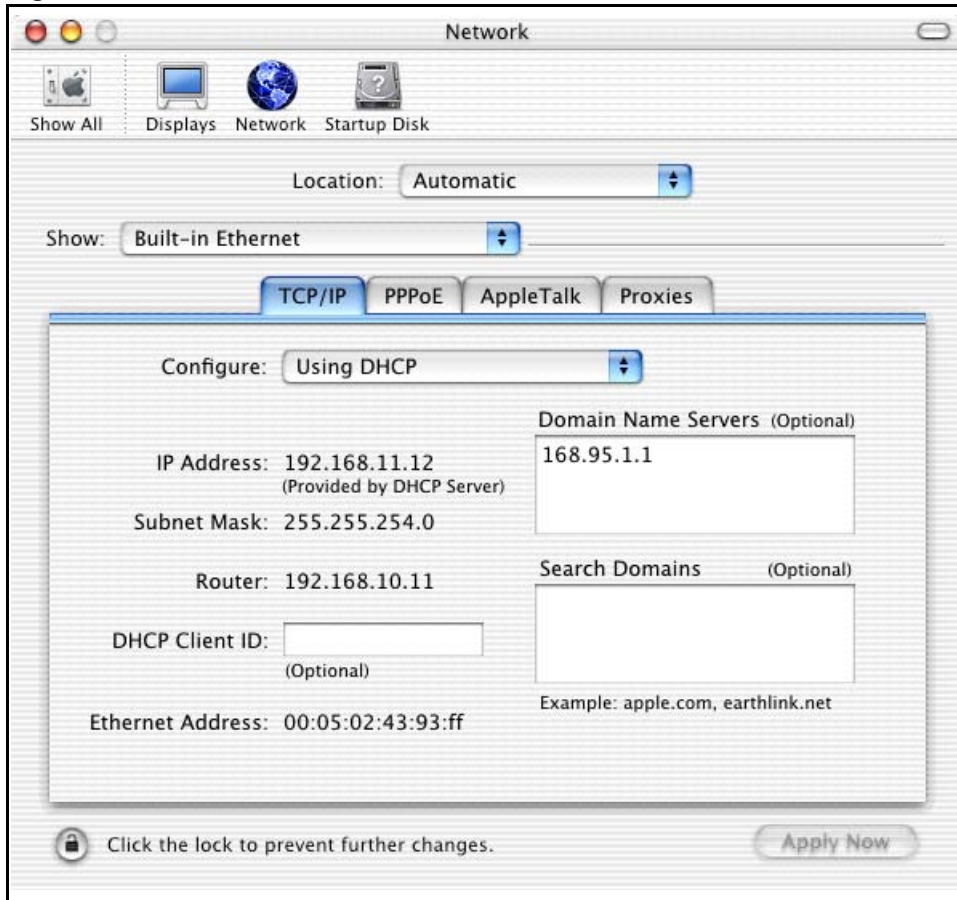
4 For statically assigned settings, do the following:

- 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 C
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 227   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 228   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 229   "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 230 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 231 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 232   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 233   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 234   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 235   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 236   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 237   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 238 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	223	254	255

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

Table 239 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 227) available for subnetting.

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

Table 240 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 D
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 382). 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 382 Single-Computer per Router Hardware Configuration
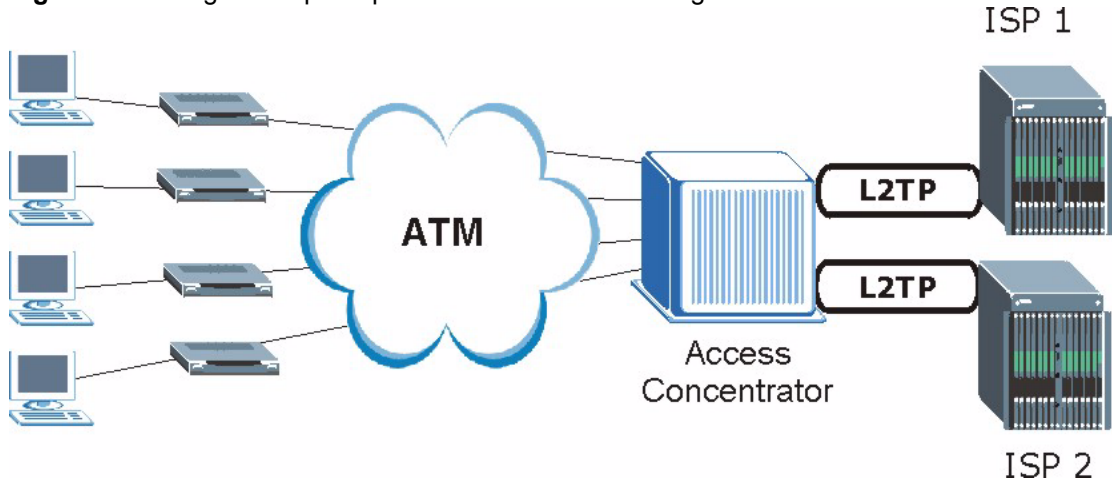
How PPPoE Works

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 383 ZyWALL as a PPPoE Client
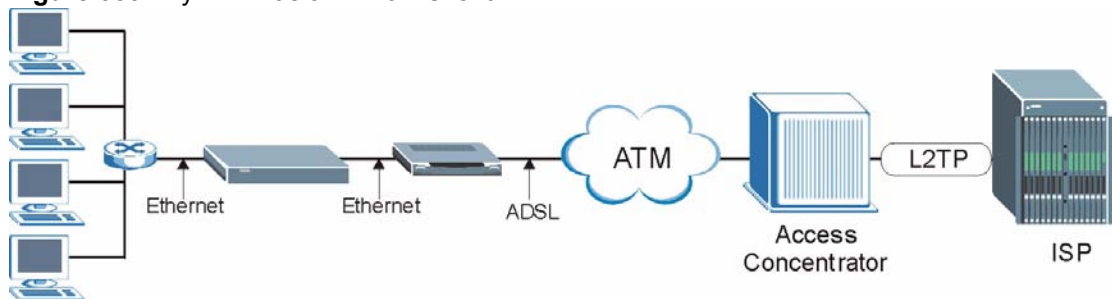
Appendix E
PPTP

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 384   Transport PPP frames over Ethernet
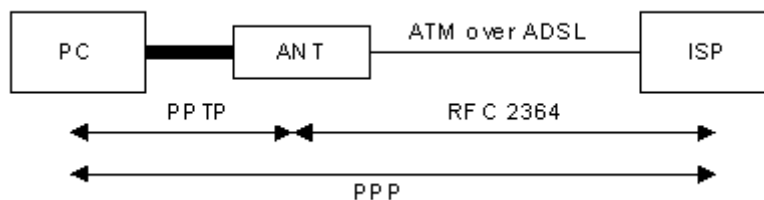
PPTP and the ZyWALL

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 385 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 386 Example Message Exchange between Computer and an ANT
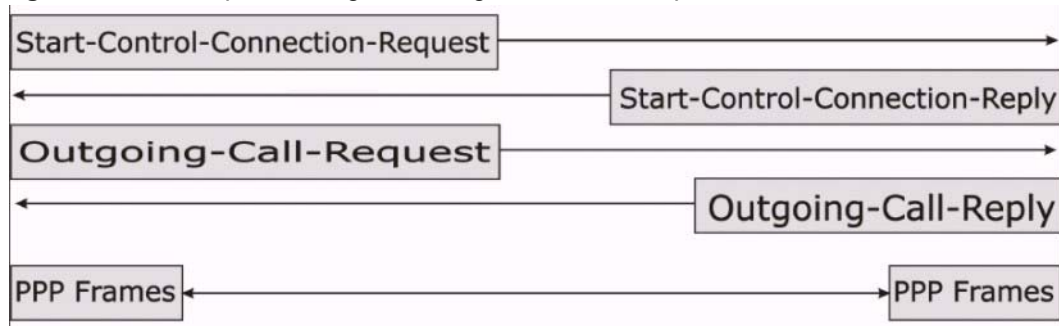
PPP Data Connection

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 F
Wireless LAN and IEEE 802.11

A wireless LAN (WLAN) provides a flexible data communications system that you can use to access various services (navigating the Internet, email, printer services, etc.) without the use of a cabled connection. In effect a wireless LAN environment provides you the freedom to stay connected to the network while roaming around in the coverage area.

Benefits of a Wireless LAN

Wireless LAN offers the following benefits:

It provides you with access to network services in areas otherwise hard or expensive to wire, such as historical buildings, buildings with asbestos materials and classrooms.

It provides healthcare workers like doctors and nurses access to a complete patient's profile on a handheld or notebook computer upon entering a patient's room.

It allows flexible workgroups a lower total cost of ownership for workspaces that are frequently reconfigured.

It allows conference room users access to the network as they move from meeting to meeting, getting up-to-date access to information and the ability to communicate decisions while "on the go".

It provides campus-wide networking mobility, allowing enterprises the roaming capability to set up easy-to-use wireless networks that cover the entire campus transparently.

IEEE 802.11

The 1997 completion of the IEEE 802.11 standard for wireless LANs (WLANs) was a first important step in the evolutionary development of wireless networking technologies. The standard was developed to maximize interoperability between differing brands of wireless LANs as well as to introduce a variety of performance improvements and benefits.

The IEEE 802.11 specifies three different transmission methods for the PHY, the layer responsible for transferring data between nodes. Two of the methods use spread spectrum RF signals, Direct Sequence Spread Spectrum (DSSS) and Frequency-Hopping Spread Spectrum (FHSS), in the 2.4 to 2.4825 GHz unlicensed ISM (Industrial, Scientific and Medical) band. The third method is infrared technology, using very high frequencies, just below visible light in the electromagnetic spectrum to carry data.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless nodes or stations (STA), which is called a Basic Service Set (BSS). In the most basic form, a wireless LAN connects a set of computers with wireless adapters. Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an Ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an Ad-hoc wireless LAN.

Figure 387   Peer-to-Peer Communication in an Ad-hoc Network
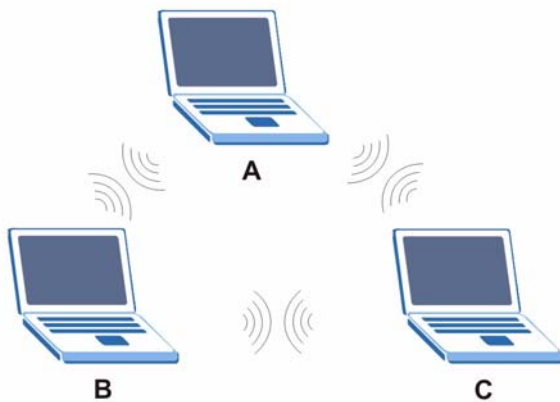
Infrastructure Wireless LAN Configuration

For Infrastructure WLANs, multiple Access Points (APs) link the WLAN to the wired network and allow users to efficiently share network resources. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood. Multiple Access Points can provide wireless coverage for an entire building or campus. All communications between stations or between a station and a wired network client go through the Access Point.

The Extended Service Set (ESS) shown in the next figure consists of a series of overlapping BSSs (each containing an Access Point) connected together by means of a Distribution System (DS). Although the DS could be any type of network, it is almost invariably an Ethernet LAN. Mobile nodes can roam between Access Points and seamless campus-wide coverage is possible.

Figure 388 ESS Provides Campus-Wide Coverage
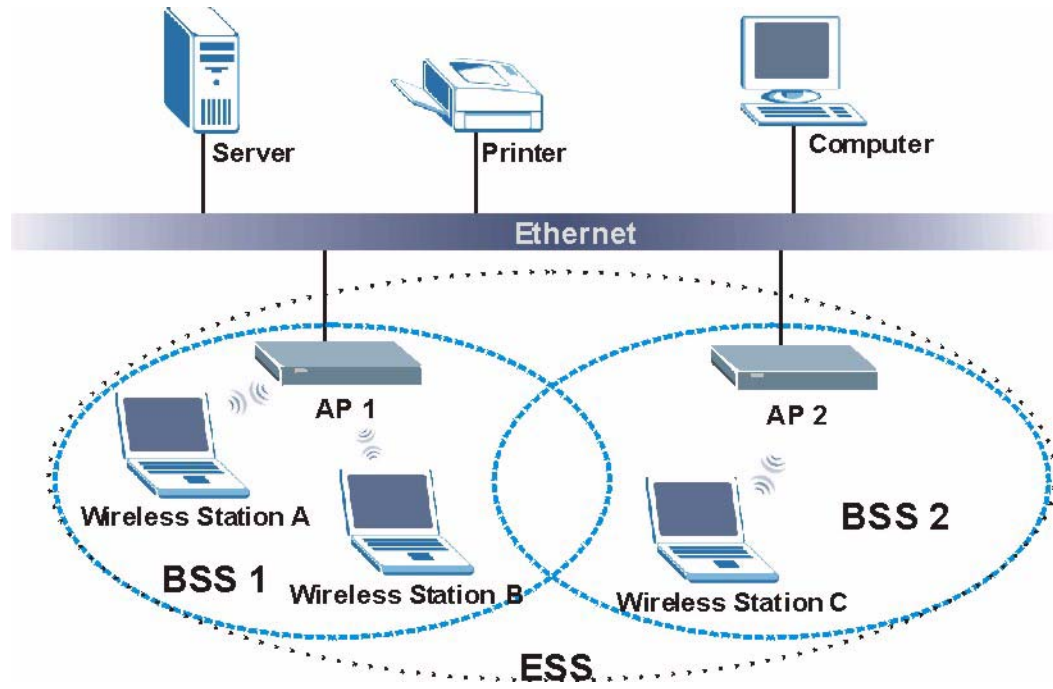
Appendix G
Wireless LAN With IEEE 802.1x

As wireless networks become popular for both portable computing and corporate networks, security is now a priority.

Security Flaws with IEEE 802.11

Wireless networks based on the original IEEE 802.11 have a poor reputation for safety. The IEEE 802.11b wireless access standard, first published in 1999, was based on the MAC address. As the MAC address is sent across the wireless link in clear text, it is easy to spoof and fake. Even the WEP (Wire Equivalent Privacy) data encryption is unreliable as it can be easily decrypted with current computer speed

Deployment Issues with IEEE 802.11

User account management has become a network administrator's nightmare in a corporate environment, as the IEEE 802.11b standard does not provide any central user account management. User access control is done through manual modification of the MAC address table on the access point. Although WEP data encryption offers a form of data security, you have to reset the WEP key on the clients each time you change your WEP key on the access point.

IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices.

Advantages of the IEEE 802.1x

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless clients.

RADIUS Server Authentication Sequence

The following figure depicts a typical wireless network with a remote RADIUS server for user authentication using EAPOL (EAP Over LAN).

Figure 389 Sequences for EAP MD5–Challenge Authentication
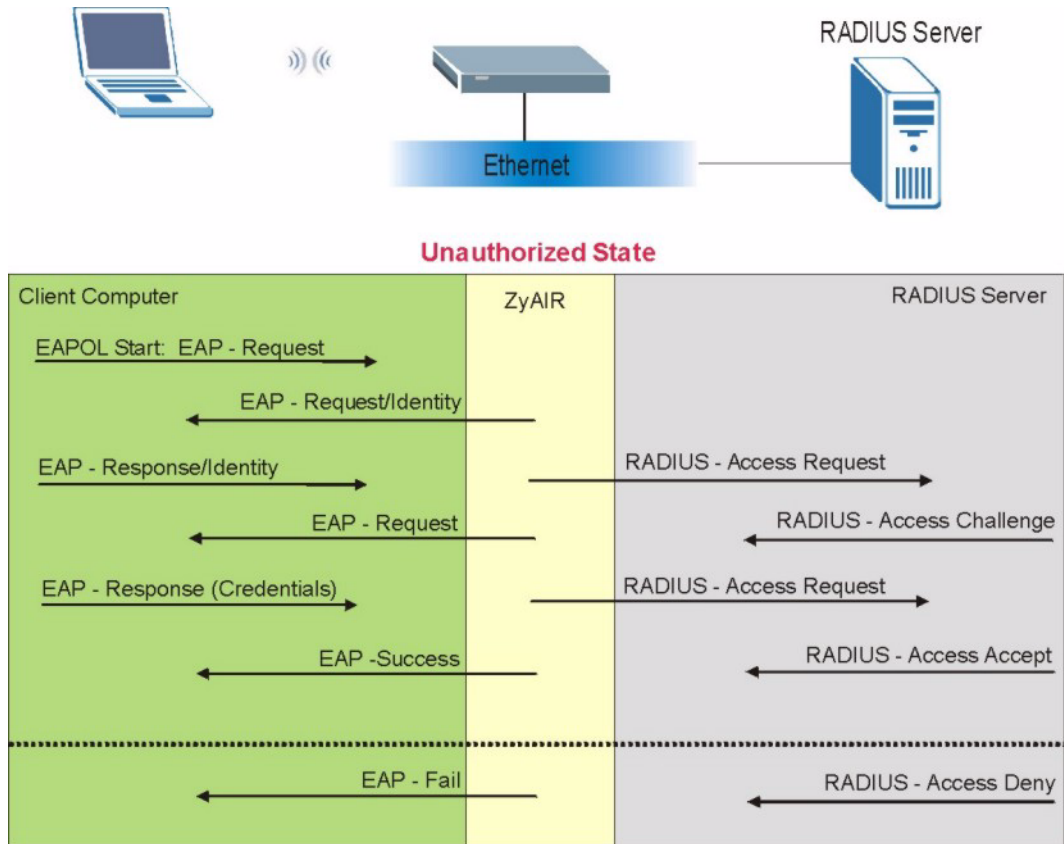
Appendix H
Types of EAP Authentication

This appendix discusses the five popular EAP authentication types: **EAP-MD5**, **EAP-TLS**, **EAP-TTLS**, **PEAP** and **LEAP**.

The type of authentication you use depends on the RADIUS server or the AP. Consult your network administrator for more information.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless station. The wireless station 'proves' that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless stations for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE802.1x.

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of five authentication types.

Table 241 Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

Appendix I
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 390   Ideal Setup
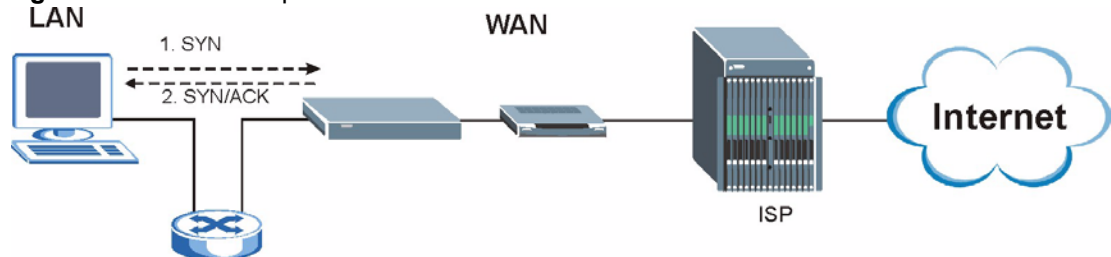
The "Triangle Route" Problem

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 391 "Triangle Route" Problem
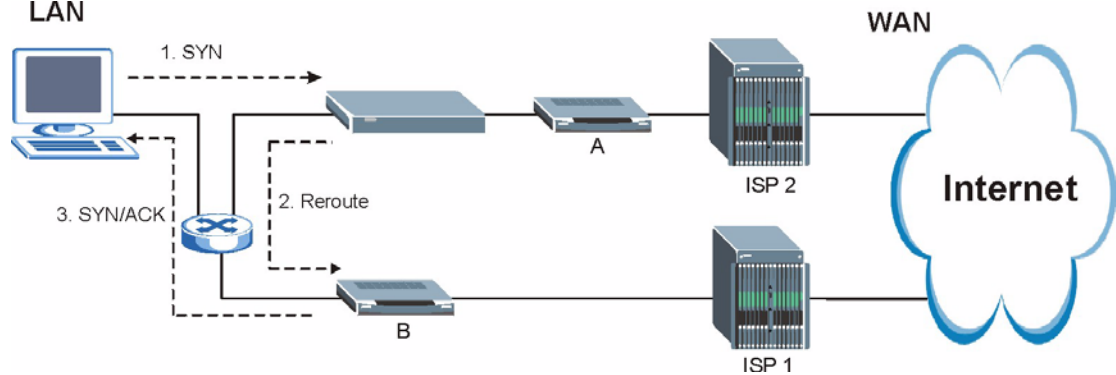
The "Triangle Route" Solutions

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 392 IP Alias
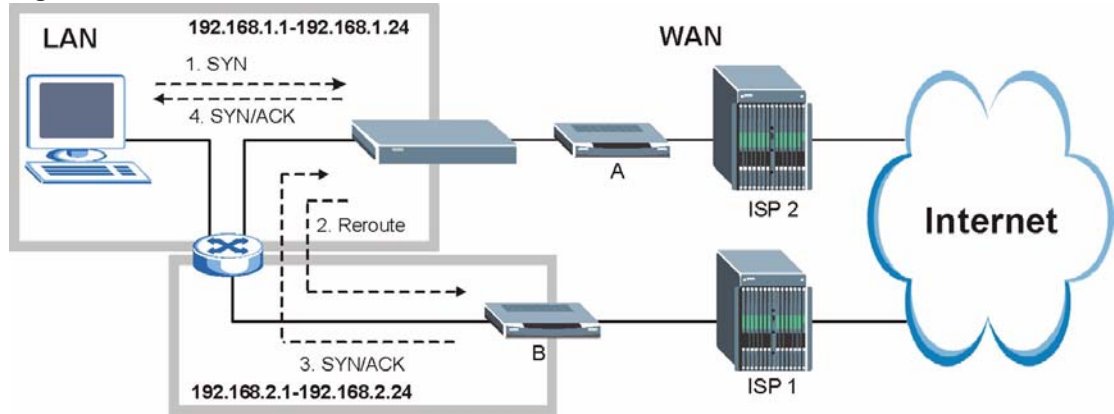
Gateways on the WAN Side

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 393 Gateways on the WAN Side
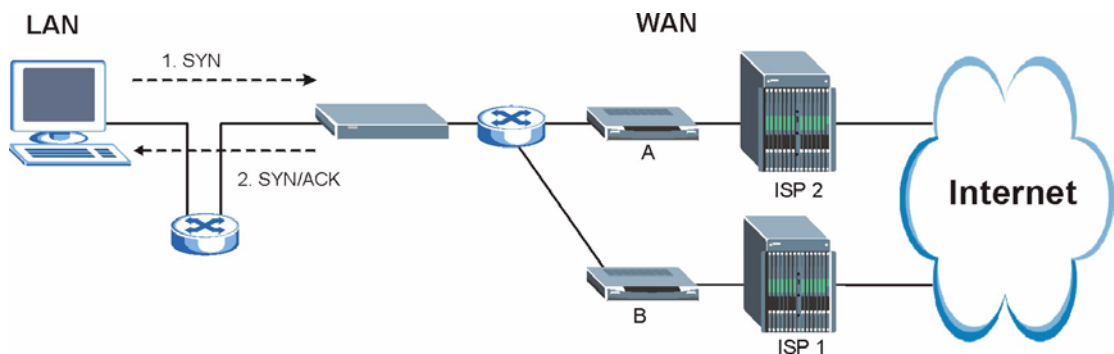
How To Configure Triangle Route

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 J
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 <u>1122334455@VoIP-provider.com</u>, 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 242   SIP Call Progression

A		B
1. INVITE		
		2. Ringing
		3. OK

Table 242 SIP Call Progression (continued)

A		B
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 394 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 395 SIP Proxy Server
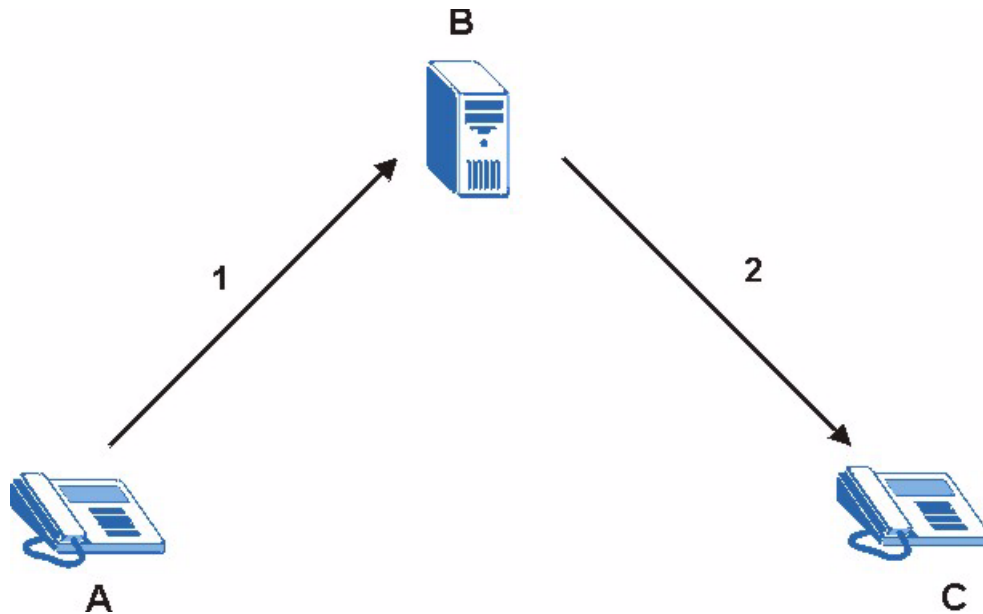
SIP Redirect Server

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 396 SIP Redirect Server
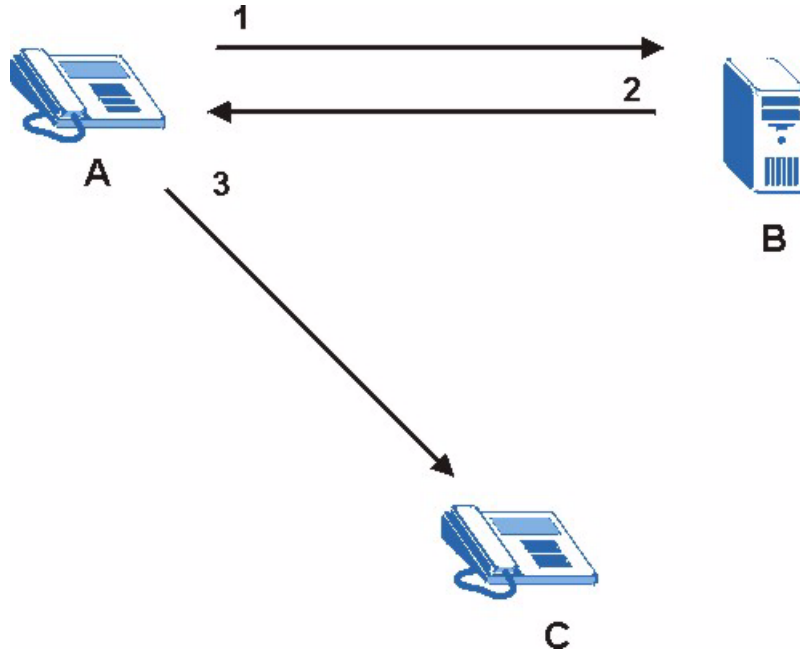
SIP Register Server

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 397 ZyWALL SIP ALG
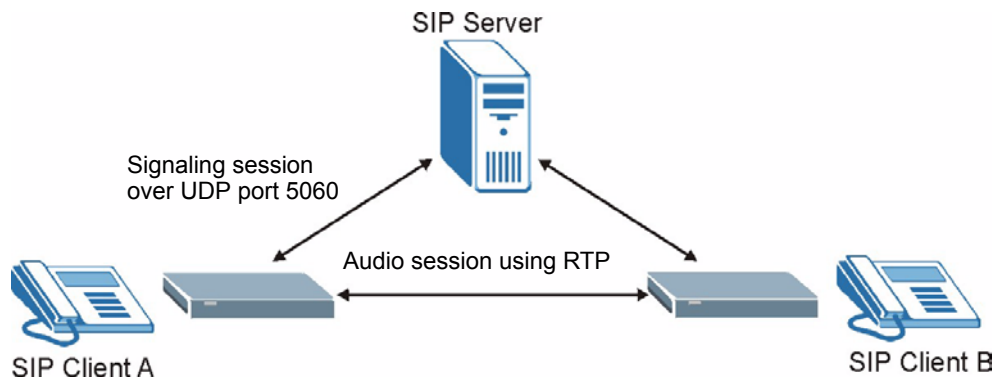
SIP ALG and NAT

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 K
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 Address** 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 398 VPN Rules
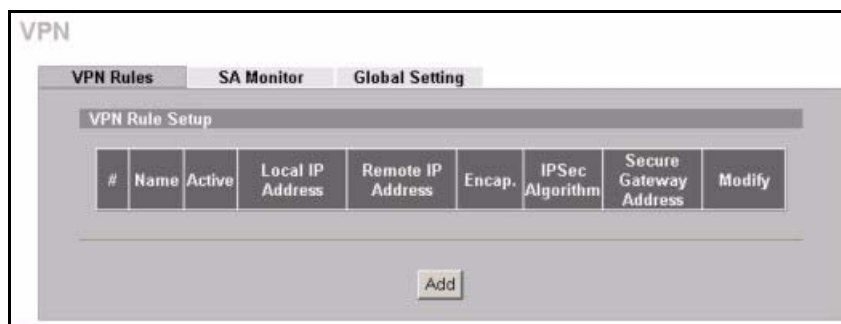
2 Configure the screens in the headquarters and the branch office as follows and click **Apply**.

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 399 Headquarters VPN Rule Edit

Figure 400 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 401 VPN Rule Configured
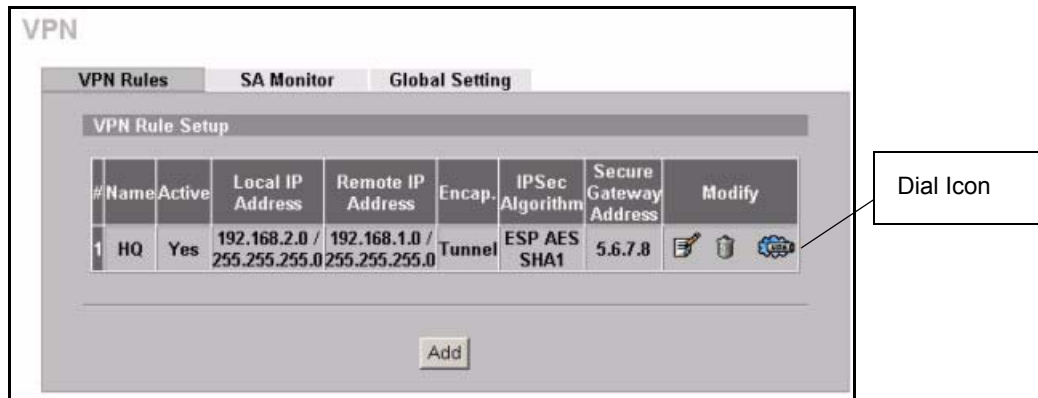
The following screen displays.

Figure 402 VPN Dial
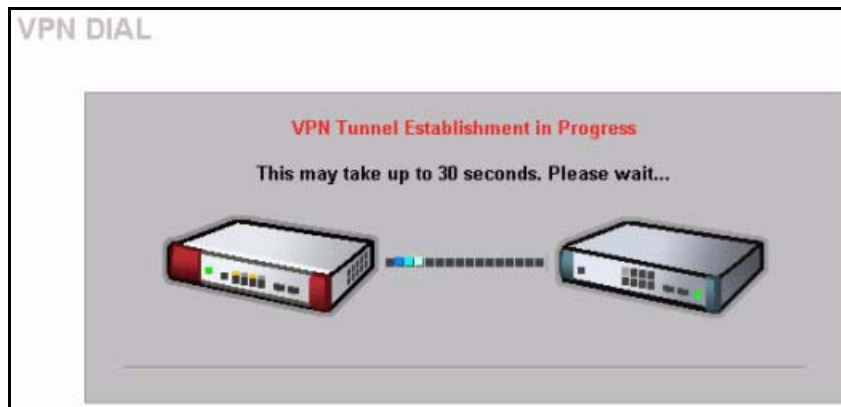
This screen displays later if the IPSec routers can build the VPN tunnel.

---

1. This feature is not available on all ZyWALL models.

Figure 403   VPN Tunnel Established
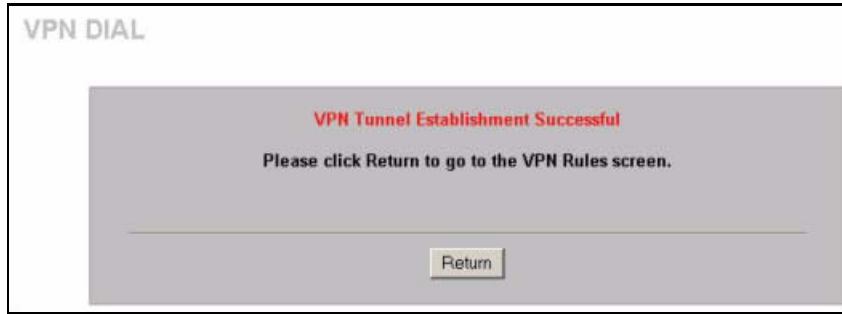
VPN Configuration via SMT

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 404   Menu 27: VPN/IPSec Setup

```
            Menu 27 - VPN/IPSec Setup

                    1. IPSec Summary
                    2. SA Monitor




         Enter Menu Selection Number:
```
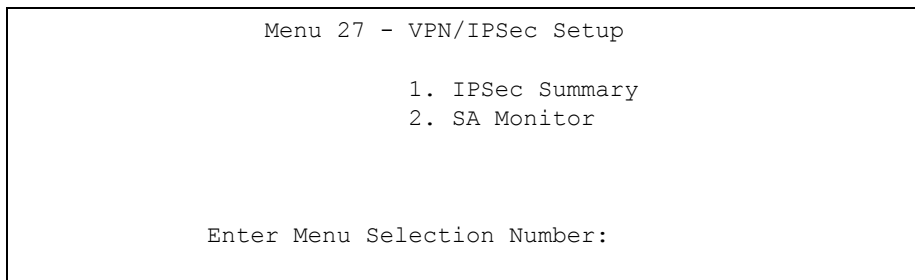
2 Type 1 in menu 27 and then press [ENTER] to display **Menu 27.1 — IPSec Summary**. This is a summary read-only menu of your IPSec rules (tunnels). Select **Edit** in the **Select Command** field; type the index number of a rule in the **Select Rule** field and press [ENTER].

Figure 405   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 406   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 407 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 408   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.

Simultaneously 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 SMT **Menu 24.8**. See Appendix S Boot Commands for information on the log messages.

Figure 409 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 410   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!!!
```

Appendix L
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 411 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 412 Login Screen

2 Click **Install Certificate** to open the **Install Certificate** wizard.

Figure 413 Certificate General Information before Import

3 Click **Next** to begin the **Install Certificate** wizard.

Figure 414 Certificate Import Wizard 1

4 Select where you would like to store the certificate and then click **Next**.

Figure 415 Certificate Import Wizard 2

5 Click **Finish** to complete the **Import Certificate** wizard.

Figure 416 Certificate Import Wizard 3

6 Click **Yes** to add the ZyWALL certificate to the root store.

Figure 417 Root Certificate Store
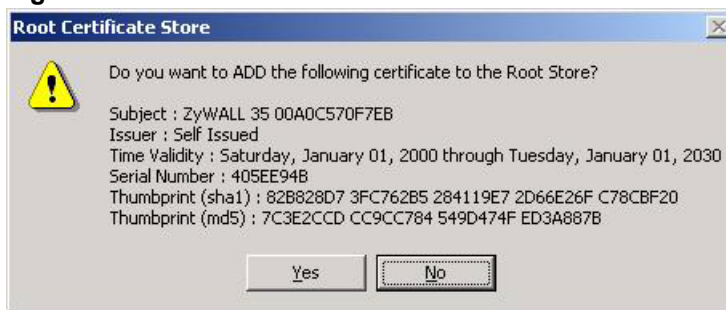
Figure 418 Certificate General Information after Import

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 Chapter 15 Certificates 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 419 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 420 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 421 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 422 Personal Certificate Import Wizard 2

3 Enter the password given to you by the CA.

Figure 423 Personal Certificate Import Wizard 3
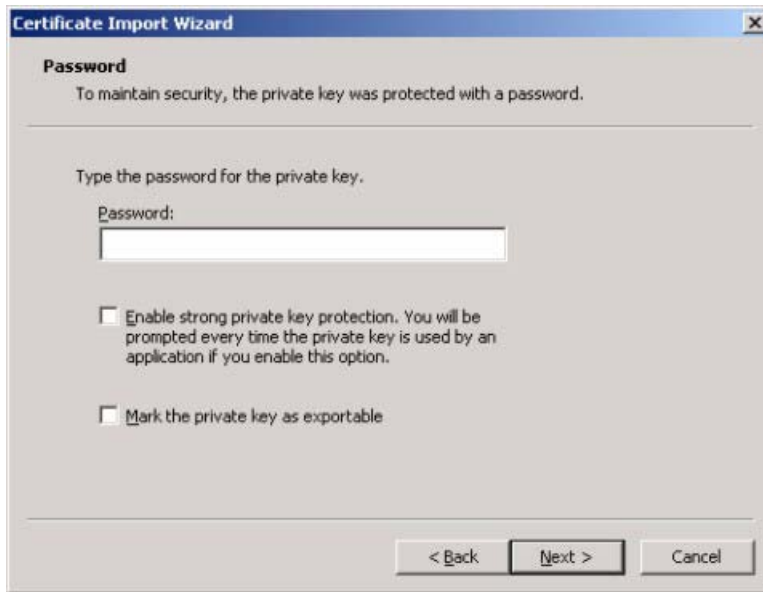
4 Have the wizard determine where the certificate should be saved on your computer or select **Place all certificates in the following store** and choose a different location.

Figure 424 Personal Certificate Import Wizard 4
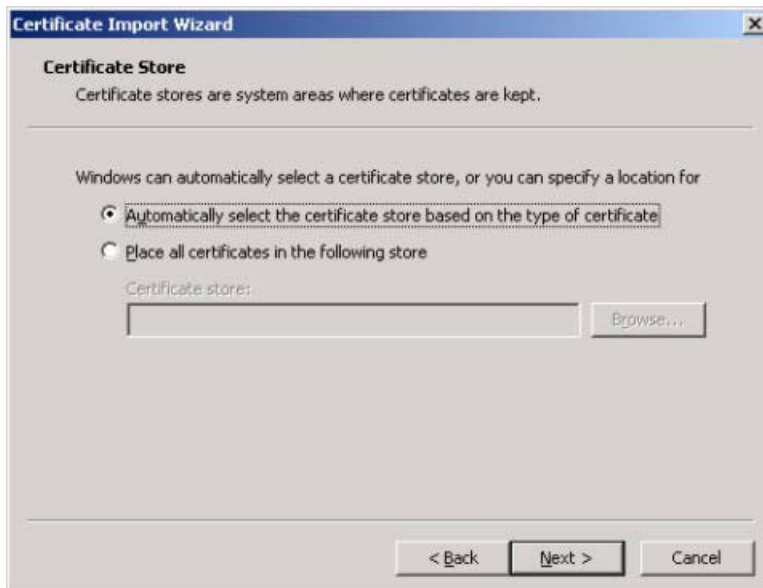
5 Click **Finish** to complete the wizard and begin the import process.

Figure 425   Personal Certificate Import Wizard 5

6 You should see the following screen when the certificate is correctly installed on your computer.

Figure 426   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 427   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 428 SSL Client Authentication

3 You next see the ZyWALL login screen.

Figure 429 ZyWALL Secure Login Screen

Appendix M
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 N
Firewall Commands

The following describes the firewall commands. See Appendix M Command Interpreter for information on the command structure.

Table 243 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 243 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 243 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 243 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 243 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 N Firewall Commands

Appendix O
NetBIOS Filter Commands

The following describes the NetBIOS packet filter commands. See Appendix M Command Interpreter 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 244 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 P
Certificates Commands

The following describes the certificate commands. See Appendix M Command Interpreter for information on the command structure.

All of these commands start with certificates.

Table 245 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 245 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 245 Certificates Commands (continued)

COMMAND	DESCRIPTION		
	replace_fact ory		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 245 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 Q
Brute-Force Password Guessing Protection

The following describes the commands for enabling, disabling and configuring the brute-force password guessing protection mechanism for the password. See Appendix M Command Interpreter for information on the command structure.

Table 246 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 R
Boot Commands

The BootModule AT commands execute from within the router's bootup software, when debug mode is selected before the main router firmware is started. When you start up your ZyWALL, you are given a choice to go into debug mode by pressing a key at the prompt shown in the following screen. In debug mode you have access to a series of boot module commands, for example ATUR (for uploading firmware) and ATLC (for uploading the configuration file). These are already discussed in the **Firmware and Configuration File Maintenance** chapter.

Figure 430 Option to Enter Debug Mode

```
          Bootbase Version: V1.05 | 06/25/2003 19:48:25
          RAM:Size = 32 Mbytes
          DRAM POST: Testing: 32608K OK
          DRAM Test SUCCESS !
          FLASH: Intel 32M

          ZyNOS Version: V3.63(WM.0)b2 | 07/06/2004 13:37:08

          Press any key to enter debug mode within 3 seconds.
          ............................................................
```

Enter ATHE to view all available ZyWALL boot module commands as shown in the next screen. ATBAx allows you to change the console port speed. The x denotes the number preceding the colon to give the console port speed following the colon in the list of numbers that follows; for example ATBA3 will give a console port speed of 9.6 Kbps. ATSE displays the seed that is used to generate a password to turn on the debug flag in the firmware. The ATSH command shows product related information such as boot module version, vendor name, product model, RAS code revision, etc. ATGO allows you to continue booting the system. Most other commands aid in advanced troubleshooting and should only be used by qualified engineers.

Figure 431 Boot Module Commands

```
AT            just answer OK
ATHE          print help
ATBAx         change baudrate. 1:38.4k, 2:19.2k, 3:9.6k 4:57.6k 5:115.2k
ATENx,(y)     set BootExtension Debug Flag (y=password)
ATSE          show the seed of password generator
ATTI(h,m,s)   change system time to hour:min:sec or show current time
ATDA(y,m,d)   change system date to year/month/day or show current date
ATDS          dump RAS stack
ATDT          dump Boot Module Common Area
ATDUx,y       dump memory contents from address x for length y
ATWBx,y       write address x with  8-bit value y
ATWWx,y       write address x with 16-bit value y
ATWLx,y       write address x with 32-bit value y
ATRBx         display the  8-bit value of address x
ATRWx         display the 16-bit value of address x
ATRLx         display the 32-bit value of address x
ATGO(x)       run program at addr x or boot router
ATGR          boot router
ATGT          run Hardware Test Program
AT%Tx         Enable Hardware Test Program at boot up
ATBTx         block0 write enable (1=enable, other=disable)
ATRTw,x,y(,z) RAM test level w, from address x to y (z iterations)
ATWEa(,b,c,d) write MAC addr, Country code, EngDbgFlag, FeatureBit to flash
ROM
ATCUx         write Country code to flash ROM
ATCB          copy from FLASH ROM to working buffer
ATCL          clear working buffer
ATSB          save working buffer to FLASH ROM
ATBU          dump manufacturer related data in working buffer
ATSH          dump manufacturer related data in ROM
ATWMx         set MAC address in working buffer
ATCOx         set country code in working buffer
ATFLx         set EngDebugFlag in working buffer
ATSTx         set ROMRAS address in working buffer
ATSYx         set system type in working buffer
ATVDx         set vendor name in working buffer
ATPNx         set product name in working buffer
ATFEx,y,...   set feature bits in working buffer
ATMP          check & dump memMapTab
ATDOx,y       download from address x for length y to PC via XMODEM
ATTD          download router configuration to PC via XMODEM
ATUPx,y       upload to RAM address x for length y from PC via XMODEM
ATUR          upload router firmware to flash ROM
ATLC          upload router configuration file to flash ROM
ATUXx(,y)     xmodem upload from flash block x to y
ATERx,y       erase flash rom from block x to y
ATWFx,y,z     copy data from addr x to flash addr y, length z
ATXSx         xmodem select: x=0: CRC mode(default); x=1: checksum mode
ATSI          run sieve benchmark
ATDHx         run dhrystone benchmark, 1:ver 1.1, 2:ver 2.1
ATSDx         decompress & load image (name=x)
ATLOa,b,c,d   Int/Trap Log Cmd
ATSR          system reboot
ATBR          Reset to default Romfile
ATDC          Disable check model mechanism
```

Appendix S
Log Descriptions

This appendix provides descriptions of example log messages.

Table 247 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 247 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 248 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 249 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 250 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.Default timeout values:ICMP idle timeout (s): 60UDP idle timeout (s): 60TCP connection (three way handshaking) timeout (s): 30TCP FIN-wait timeout (s): 60TCP idle (established) timeout (s): 3600
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 251 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 252 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 264.
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 264.

Table 252 ICMP Logs (continued)

LOG MESSAGE	DESCRIPTION
`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 253 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 254 PPP Logs

LOG MESSAGE	DESCRIPTION
`ppp:LCP Starting`	The PPP connection's Link Control Protocol stage has started.
`ppp:LCP Opening`	The PPP connection's Link Control Protocol stage is opening.
`ppp:CHAP Opening`	The PPP connection's Challenge Handshake Authentication Protocol stage is opening.
`ppp:IPCP Starting`	The PPP connection's Internet Protocol Control Protocol stage is starting.
`ppp:IPCP Opening`	The PPP connection's Internet Protocol Control Protocol stage is opening.
`ppp:LCP Closing`	The PPP connection's Link Control Protocol stage is closing.
`ppp:IPCP Closing`	The PPP connection's Internet Protocol Control Protocol stage is closing.

Table 255 UPnP Logs

LOG MESSAGE	DESCRIPTION
UPnP pass through Firewall	UPnP packets can pass through the firewall.

Table 256 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.
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 257 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 264.
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 264.
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 264.
icmp echo : ICMP (type:%d, code:%d)	The firewall detected an ICMP echo attack. For type and code details, see Table 264.
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 264.
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 264.
traceroute ICMP (type:%d, code:%d)	The firewall detected an ICMP traceroute attack. For type and code details, see Table 264.

Table 258 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 259 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 259 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 259 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 259 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 260 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 260 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 261 for the corresponding descriptions of the codes.

Table 261 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 261 Certificate Path Verification Failure Reason Codes (continued)

CODE	DESCRIPTION
26	Database method failed.
27	Path was not verified.
28	Maximum path length reached.

Table 262 802.1X 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 263 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 264 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 264 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 265 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 266 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 266 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 M, "") 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.

Figure 432 Displaying Log Categories Example

```
Copyright (c) 1994 - 2004 ZyXEL Communications Corp.
ras> ?
Valid commands are:
sys            ls             exit           ether
aux            ip             ipsec          bridge
bm             certificates   8021x          radius
ras>
```

3 Use sys logs category followed by a log category to display the parameters that are available for the category.

Figure 433 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 Step 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|11/11/2002 15:10:12 |172.22.3.80:137      |172.22.255.255:137   |ACCESS
BLOCK
    Firewall default policy: UDP(set:8)
 1|11/11/2002 15:10:12 |172.21.4.17:138      |172.21.255.255:138   |ACCESS
BLOCK
    Firewall default policy: UDP(set:8)
 2|11/11/2002 15:10:11 |172.17.2.1           |224.0.1.60           |ACCESS
BLOCK
    Firewall default policy: IGMP(set:8)
 3|11/11/2002 15:10:11 |172.22.3.80:137      |172.22.255.255:137   |ACCESS
BLOCK
    Firewall default policy: UDP(set:8)
 4|11/11/2002 15:10:10 |192.168.10.1:520     |192.168.10.255:520   |ACCESS
BLOCK
    Firewall default policy: UDP(set:8)
 5|11/11/2002 15:10:10 |172.21.4.67:137      |172.21.255.255:137   |ACCESS
BLOCK
```

Index

O

P

Q

R