

# *ZyWALL 1*

## *User's Guide*

Version 3.60  
April 2003





# Copyright

Copyright © 2003 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

## **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.

# 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 one year 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.



## **Online Registration**

Don't forget to register your ZyXEL product (fast, easy online registration at [www.zyxel.com](http://www.zyxel.com)) for free future product updates and information.

# 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	E-MAIL SUPPORT/SALES	TELEPHONE/FAX	WEB SITE/ FTP SITE	REGULAR MAIL
LOCATION				
WORLDWIDE	<a href="mailto:support@zyxel.com.tw">support@zyxel.com.tw</a>  <a href="mailto:sales@zyxel.com.tw">sales@zyxel.com.tw</a>	+886-3-578-3942  +886-3-578-2439	<a href="http://www.zyxel.com">www.zyxel.com</a>  <a href="http://www.europe.zyxel.com">www.europe.zyxel.com</a>  <a href="ftp://ftp.europe.zyxel.com">ftp.europe.zyxel.com</a>	ZyXEL Communications Corp., 6 Innovation Road II, Science- Based Industrial Park, Hsinchu 300, Taiwan
NORTH AMERICA	<a href="mailto:support@zyxel.com">support@zyxel.com</a>  <a href="mailto:sales@zyxel.com">sales@zyxel.com</a>	+1-714-632-0882 800-255-4101  +1-714-632-0858	<a href="http://www.zyxel.com">www.zyxel.com</a>  <a href="ftp://ftp.zyxel.com">ftp.zyxel.com</a>	ZyXEL Communications Inc., 1650 Miraloma Avenue, Placentia, CA 92870, U.S.A.
SCANDINAVIA	<a href="mailto:support@zyxel.dk">support@zyxel.dk</a>  <a href="mailto:sales@zyxel.dk">sales@zyxel.dk</a>	+45-3955-0700  +45-3955-0707	<a href="http://www.zyxel.dk">www.zyxel.dk</a>  <a href="ftp://ftp.zyxel.dk">ftp.zyxel.dk</a>	ZyXEL Communications A/S, Columbusvej 5, 2860 Soeborg, Denmark
GERMANY	<a href="mailto:support@zyxel.de">support@zyxel.de</a>  <a href="mailto:sales@zyxel.de">sales@zyxel.de</a>	+49-2405-6909-0  +49-2405-6909-99	<a href="http://www.zyxel.de">www.zyxel.de</a>	ZyXEL Deutschland GmbH, Adenauerstr. 20/A2 D-52146 Wuerselen, Germany

# Table of Contents

Copyright .....	i
ZyXEL Limited Warranty .....	ii
Customer Support .....	iii
List of Figures .....	viii
List of Tables .....	xi
List of Charts .....	xiii
List of Diagrams .....	xiv
Preface .....	xv
Getting Started .....	I
Chapter 1 Getting to Know Your ZyWALL .....	1-1
1.1 The ZyWALL Internet Security Gateway .....	1-1
1.2 Features of the ZyWALL .....	1-1
1.3 ZyWALL Application .....	1-3
Chapter 2 Hardware Installation .....	2-1
2.1 ZyWALL Front Panel .....	2-1
2.2 ZyWALL Rear Panel and Connections .....	2-2
2.3 Additional Installation Requirements .....	2-3
2.4 Turning on Your ZyWALL .....	2-4
2.5 ZyWALL Configuration .....	2-4
Chapter 3 Introducing the Web Configurator .....	3-1
3.1 Accessing the ZyWALL Web Configurator .....	3-1
3.2 Navigating the ZyWALL Web Configurator .....	3-1
3.3 Overview of the ZyWALL Web Configurator .....	3-2
Chapter 4 Wizard Setup .....	4-1
4.1 Introduction to Wizard Screens .....	4-1
4.2 Wizard Setup: Screen 2 .....	4-2

---

4.3	Wizard Setup: Screen 3 .....	4-8
4.4	Basic Setup Complete .....	4-12
Advanced .....		II
Chapter 5	System .....	5-1
5.1	About System Setup .....	5-1
5.2	General Setup .....	5-1
5.3	Dynamic DNS .....	5-2
5.4	Password .....	5-4
5.5	Time Zone .....	5-5
Chapter 6	LAN and WAN .....	6-1
6.1	DHCP Setup .....	6-1
6.2	LAN TCP/IP .....	6-1
6.3	WAN Setup .....	6-5
Chapter 7	SUA/NAT .....	7-1
7.1	The SUA/NAT Screen .....	7-1
Chapter 8	Static Route .....	8-1
8.1	General Information About Static Routes .....	8-1
8.2	IP Static Route Summary .....	8-1
Chapter 9	UPnP .....	9-1
9.1	Introducing Universal Plug and Play .....	9-1
9.2	UPnP and ZyXEL .....	9-2
9.3	Installing UPnP in Windows Example .....	9-3
9.4	Using UPnP in Windows XP Example .....	9-5
Chapter 10	SNMP .....	10-1
10.1	About SNMP .....	10-1
10.2	Supported MIBs .....	10-2
10.3	SNMP Configuration .....	10-2

10.4	SNMP Traps .....	10-3
Advanced Management .....		III
Chapter 11	Firewall .....	11-1
11.1	Introduction.....	11-1
11.2	The Firewall and NAT .....	11-3
11.3	Firewall Settings .....	11-4
11.4	Filter.....	11-6
11.5	Services.....	11-8
Chapter 12	VPN/IPSec .....	12-1
12.1	Introduction.....	12-1
12.2	IPSec Architecture .....	12-2
12.3	IPSec and NAT .....	12-3
12.4	ZyWALL 1 VPN .....	12-4
12.5	VPN/IPSec Screen 1: VPN/IPSec Setup Tab.....	12-4
12.6	VPN/IPSec Setup: IKE .....	12-12
12.7	VPN/IPSec Setup: Manual.....	12-16
12.8	Advanced VPN Setup .....	12-19
12.9	The VPN/IPSec Screen: SA Monitor Tab.....	12-29
12.10	Configuring Global Setting.....	12-31
Chapter 13	Centralized Logs .....	13-1
13.1	View Log .....	13-1
13.2	Log Settings .....	13-3
Maintenance.....		IV
Chapter 14	Maintenance .....	14-1
14.1	Maintenance Overview .....	14-1
14.2	Status Screen.....	14-1
14.3	DHCP Table Screen.....	14-4



---

14.4	F/W Upload Screen .....	14-5
14.5	Configuration Screen .....	14-7
Chapter 15	Firmware and Configuration File Maintenance Commands.....	15-1
15.1	Filename Conventions.....	15-1
15.2	Backup Configuration .....	15-2
15.3	Restore or Upload a Configuration File .....	15-4
15.4	Uploading a Firmware File .....	15-5
Chapter 16	Troubleshooting.....	16-1
16.1	Problems Starting Up the ZyWALL .....	16-1
16.2	Problems with the Password .....	16-1
16.3	Problems with the LAN Interface .....	16-2
16.4	Problems with the WAN Interface .....	16-2
16.5	Problems with Internet Access.....	16-3
16.6	Problems with the Firewall .....	16-3
Appendices and Index .....		V
Appendix A	PPPoE.....	A
Appendix B	PPTP .....	C
Appendix C	IP Subnetting .....	G
Appendix D	Power Adapter Specifications.....	O
Appendix E	Setting up Your Computer's IP Address.....	Q
Appendix F	Log Descriptions .....	CC
Appendix G	Brute-Force Password Guessing Protection .....	SS
Index .....		UU

# List of Figures

Figure 1-1 Internet Access Application .....	1-4
Figure 2-1 Front Panel .....	2-1
Figure 2-2 Rear Panel .....	2-2
Figure 3-1 Change Password Screen .....	3-1
Figure 3-2 The MAIN MENU Screen of the Web Configurator .....	3-2
Figure 3-3 Overview of the ZyWALL Web Configurator .....	3-3
Figure 4-1 Wizard 1 .....	4-2
Figure 4-2 Wizard 2: PPTP Encapsulation .....	4-5
Figure 4-3 Wizard2: PPPoE Encapsulation .....	4-7
Figure 4-4 Wizard 3 .....	4-11
Figure 5-1 System General Setup .....	5-1
Figure 5-2 System DDNS .....	5-3
Figure 5-3 System Password .....	5-4
Figure 5-4 System Time/Date .....	5-5
Figure 6-1 LAN Setup .....	6-3
Figure 6-2 Ethernet Encapsulation .....	6-5
Figure 6-3 PPPoE Encapsulation .....	6-6
Figure 6-4 PPTP Encapsulation .....	6-8
Figure 6-5 IP Setup .....	6-10
Figure 6-6 MAC Setup .....	6-13
Figure 7-1 Multiple Servers Behind NAT Example .....	7-2
Figure 7-2 SUA/NAT Setup .....	7-3
Figure 8-1 Example of Static Routing Topology .....	8-1
Figure 8-2 IP Static Route Summary .....	8-2
Figure 8-3 Edit IP Static Route .....	8-3

---

Figure 9-1 Configuring UPnP .....	9-2
Figure 10-1 SNMP Management Model.....	10-1
Figure 10-2 SNMP Configuration.....	10-3
Figure 11-1 Firewall Rule Directions.....	11-3
Figure 11-2 Firewall Settings.....	11-5
Figure 11-3 Firewall Filter.....	11-7
Figure 11-4 Firewall Service.....	11-9
Figure 12-1 Encryption and Decryption.....	12-2
Figure 12-2 IPSec Architecture.....	12-3
Figure 12-3 NAT Router Between IPSec Routers .....	12-5
Figure 12-4 Telecommuter's ZyWALL Configuration .....	12-8
Figure 12-5 Transport and Tunnel Mode IPSec Encapsulation .....	12-9
Figure 12-6 VPN/IPSec Setup: IKE.....	12-12
Figure 12-7 VPN/IPSec Setup: Manual .....	12-16
Figure 12-8 Two Phases to set up the IPSec SA.....	12-20
Figure 12-9 The ZyWALL, the Secure Remote Gateway and IKE Fields.....	12-21
Figure 12-10 Advanced VPN/IPSec Configuration .....	12-24
Figure 12-11 SA Monitor.....	12-30
Figure 12-12 Global Setting.....	12-31
Figure 13-1 View Log.....	13-2
Figure 13-2 Log Settings.....	13-4
Figure 14-1 System Status .....	14-1
Figure 14-2 System Status: Show Statistics.....	14-3
Figure 14-3 DHCP Table .....	14-4
Figure 14-4 Firmware Upgrade.....	14-5
Figure 14-5 Firmware Upgrade.....	14-6
Figure 14-6 Firmware Upload In Process .....	14-6

Figure 14-7 Network Temporarily Disconnected .....	14-6
Figure 14-8 Firmware Upload Error .....	14-7
Figure 14-9 Configuration .....	14-8
Figure 14-10 Reset Warning Message .....	14-9
Figure 14-11 Configuration Upload Successful.....	14-10
Figure 14-12 Network Temporarily Disconnected .....	14-10
Figure 14-13 Configuration Upload Error .....	14-11
Figure 15-1 FTP Session Example .....	15-2
Figure 15-2 Restore Using FTP Session Example .....	15-5
Figure 15-3 FTP Session Example of Firmware File Upload.....	15-6

# List of Tables

Table 4-1 Wizard 2: Ethernet Encapsulation .....	4-3
Table 4-2 Ethernet Encapsulation .....	4-3
Table 4-3 PPTP Encapsulation.....	4-5
Table 4-4 PPPoE Encapsulation.....	4-7
Table 4-5 Private IP Address Ranges.....	4-8
Table 4-6 Example of Network Properties for LAN Servers with Fixed IP Addresses .....	4-10
Table 4-7 WAN Setup.....	4-11
Table 5-1 System General Setup.....	5-1
Table 5-2 System DDNS.....	5-3
Table 5-3 System Password .....	5-5
Table 5-4 System Time/Date .....	5-6
Table 6-1 LAN Setup.....	6-3
Table 6-2 Ethernet Encapsulation .....	6-5
Table 6-3 PPPoE Encapsulation.....	6-7
Table 6-4 PPTP Encapsulation.....	6-8
Table 6-5 IP Setup.....	6-10
Table 7-1 Services and Port Numbers.....	7-2
Table 7-2 SUA/NAT Setup.....	7-4
Table 8-1 IP Static Route Summary.....	8-2
Table 8-2 Edit IP Static Route .....	8-3
Table 9-1 Configuring UPnP .....	9-3
Table 10-1 SNMP Requests/Responses .....	10-2
Table 10-2 SNMP Configuration Menu Fields .....	10-3
Table 10-3 SNMP Traps .....	10-4
Table 11-1 Firewall Settings .....	11-5
Table 11-2 Firewall Filter .....	11-7

Table 11-3 Firewall Service.....	11-9
Table 12-1 VPN and NAT .....	12-4
Table 12-2 Local ID Type and Content Fields .....	12-6
Table 12-3 Peer ID Type and Content Fields .....	12-7
Table 12-4 Matching ID Type and Content Configuration Example.....	12-7
Table 12-5 Mismatching ID Type and Content Configuration Example.....	12-7
Table 12-6Telecommuter and Headquarters Configuration Example .....	12-8
Table 12-7 AH AND ESP.....	12-10
Table 12-8 VPN/IPSec Setup: IKE.....	12-12
Table 12-9 VPN/IPSec Setup: Manual .....	12-17
Table 12-10 The ZyWALL and the Secure Remote Gateway: IKE Fields.....	12-21
Table 12-11 Advanced VPN Extra Configuration Fields .....	12-22
Table 12-12 Advanced VPN/IPSec Configuration .....	12-25
Table 12-13 SA Monitor Tab Fields.....	12-30
Table 12-14 SA Monitor.....	12-31
Table 13-1 View Log.....	13-2
Table 13-2 Log Settings.....	13-5
Table 14-1 System Status .....	14-2
Table 14-2 System Status: Show Statistics .....	14-3
Table 14-3 DHCP Table .....	14-4
Table 14-4 Restore Configuration .....	14-9
Table 15-1 Filename Conventions.....	15-2
Table 15-2 General Commands for GUI-based FTP Clients .....	15-3
Table 15-3 General Commands for GUI-based TFTP Clients.....	15-4
Table 16-1 Troubleshooting the Start-Up of Your ZyWALL.....	16-1
Table 16-2 Troubleshooting the Password.....	16-1
Table 16-3 Troubleshooting the LAN Interface .....	16-2

---

Table 16-4 Troubleshooting the WAN Interface .....	16-2
Table 16-5 Troubleshooting Internet Access .....	16-3
Table 16-6 Troubleshooting the Firewall.....	16-3

## List of Charts

Chart 1 Classes of IP Addresses.....	G
Chart 2 Allowed IP Address Range By Class .....	H
Chart 3 “Natural” Masks.....	H
Chart 4 Alternative Subnet Mask Notation .....	I
Chart 5 Subnet 1.....	J
Chart 6 Subnet 2.....	J
Chart 7 Subnet 1.....	K
Chart 8 Subnet 2.....	K
Chart 9 Subnet 3.....	K
Chart 10 Subnet 4.....	K
Chart 11 Eight Subnets .....	L
Chart 12 Class C Subnet Planning .....	M
Chart 13 Class B Subnet Planning .....	M
Chart 14 System Error Logs.....	CC
Chart 15 System Maintenance Logs.....	CC
Chart 16 UPnP Logs .....	DD
Chart 17 Content Filtering Logs .....	DD
Chart 18 Attack Logs .....	EE
Chart 19 Access Logs .....	HH
Chart 20 ACL Setting Notes .....	KK
Chart 21 ICMP Notes.....	LL

Chart 22 Sample IKE Key Exchange Logs..... NN  
Chart 23 Sample IPSec Logs During Packet Transmission .....PP  
Chart 24 RFC-2408 ISAKMP Payload Types ..... QQ  
Chart 25 Brute-Force Password Guessing Protection Commands.....SS

## List of Diagrams

Diagram 1 Single-PC per Modem Hardware Configuration..... A  
Diagram 2 ZyWALL as a PPPoE Client..... B  
Diagram 3 Transport PPP frames over Ethernet..... C  
Diagram 4 PPTP Protocol Overview ..... D  
Diagram 5 Example Message Exchange between PC and an ANT ..... D  
Diagram 6 Example VPN Initiator IPSec Log..... MM  
Diagram 7 Example VPN Responder IPSec Log..... NN



# Preface

## ZyWALL

Congratulations on your purchase of the ZyWALL.

The ZyWALL is an integrated firewall solution that features Virtual Private Networking (VPN). By integrating Network Address Translation (NAT) and International Computer Security Association (ICSA) certified firewall capability, ZyXEL's ZyWALL provides not Internet access, but also a complete security solution.

Your ZyWALL is easy to install and to configure. The embedded web configurator is a convenient platform independent GUI (Graphical User Interface) that allows you to access and configure the ZyWALL's management settings.

## About This User's Guide

This user's guide helps you connect your ZyWALL hardware, explains how to access and use the web configurator, as well as background information on the features of your ZyWALL. Advanced users may use the CI commands listed in the support notes.

---

**Screen specific help (embedded help) is included with the web configurator and will guide you through the configuration of your ZyWALL.**

---

## Related Documentation

ZyXEL Glossary and Web Site

Please refer to [www.zyxel.com](http://www.zyxel.com) for an online glossary of networking terms and additional support documentation.

## Syntax Conventions

- Mouse action sequences are denoted using a comma. For example, click **Start, Settings, Control Panel, Network** means first you click **Start**, move the mouse pointer over **Settings**, then move the mouse pointer over **Control Panel** and finally click **Network**.
- “Enter” means for you to type one or more characters. “Select” or “Choose” means for you to use one of the predefined choices.
- Menu titles, field choices and labels are in Bold Times New Roman font.
- A single keystroke is in Arial font and enclosed in square brackets, for instance, [ENTER] means the Enter, or carriage return, key; [ESC] means the Escape key.
- For brevity's sake, we will use “e.g.” as a shorthand for “for instance”, and “i.e.” as a shorthand for “that is” or “in other words” throughout this manual.

- The ZyWALL may also be referred to as the device in this guide.

---

# Part I:

---

## Getting Started

---

This part covers Getting to Know Your ZyWALL, Hardware Installation, Introducing the Web Configurator and Wizard Setup.



# Chapter 1

## Getting to Know Your ZyWALL

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

### 1.1 The ZyWALL Internet Security Gateway

The ZyWALL is an integrated firewall solution that features one Virtual Private Network (VPN) tunnel. The auto-negotiating 10/100Mbps Ethernet ports are available for direct LAN access. By integrating Network Address Translation (NAT) and International Computer Security Association (ICSA) certified firewall capability, ZyWALL 1 provides not only the ease of installation and Internet access, but also a complete security solution for network environments.

### 1.2 Features of the ZyWALL

The following are the main features of the ZyWALL.

#### **IPSec VPN Capability**

Establish a Virtual Private Network (VPN) tunnel to connect one (home) office computer to your company network using data encryption and the Internet thus providing secure communications without the expense of leased site-to-site lines. The ZyWALL's VPN is based on the IPSec standard and is fully interoperable with other IPSec-based VPN products.

#### **Firewall**

The ZyWALL uses 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 protection, real time alerts, NETBIOS packet filtering, and logs.

#### **4-Port Switch**

A combination of switch and router makes your ZyWALL a cost-effective and viable network solution. You can add up to four computers to the ZyWALL without the cost of a hub. Add more than four computers to your LAN by using a hub.

#### **Auto-negotiating LAN 10/100M Ethernet/Fast LAN Interface**

A bandwidth-sensitive 10/100Mbps switch provides greater network efficiency than traditional hubs because the bandwidth is dedicated and not shared. This auto-negotiation feature allows the ZyWALL to detect the speed of incoming transmissions and adjust appropriately without manual intervention. It allows data transfers of either 10 Mbps or 100 Mbps in either half-duplex or full-duplex mode depending on your Ethernet network.

### **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 also block specific URLs by using the keyword feature.

### **Brute-Force Password Guessing Protection**

The ZyWALL has a special protection mechanism to discourage brute-force password guessing attacks on the ZyWALL's management interfaces. You can specify a wait-time that must expire before entering a fourth password after three incorrect passwords have been entered. Please see the appendices for details about this feature.

### **Web Configurator**

Your ZyWALL includes an intuitive web configurator that makes setup and configuration easy. Included with the web configurator is embedded help designed to assist you during setup/configuration.

### **NAT (Network Address Translation)/SUA (Single User Account)**

NAT (RFC 1631) or SUA allows the translation of an Internet Protocol address used within one network to a different IP address known within another network. NAT/SUA allows you to direct traffic to individual computers on your LAN, or to a designated default server computer, based on the port number request of incoming traffic. 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.

### **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).

### **DHCP Support**

DHCP (Dynamic Host Configuration Protocol) allows the individual clients (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 Windows 9X, Windows NT and other 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 real DHCP server to the clients.

### **Dynamic DNS Support**

With Dynamic DNS support, you can have a static host name 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 provider.

## **IP Multicast**

Traditionally, IP packets are transmitted in two ways - unicast or broadcast. Multicast is a third way to deliver IP packets to a group of hosts. 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 versions 1 and 2.

## **PPPoE Support**

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

## **PPTP Support**

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. Use PPTP to connect to a broadband modem to achieve access to high-speed data networks via a familiar "dial-up networking" user interface.

## **Full Network Management**

Your ZyWALL has a convenient web configurator and also supports an FTP (File Transfer Protocol) server for remote management and TFTP (Trivial FTP). Advanced users can also use FTP/TFTP and CI commands for configuration and management.

## **Logging and Tracing**

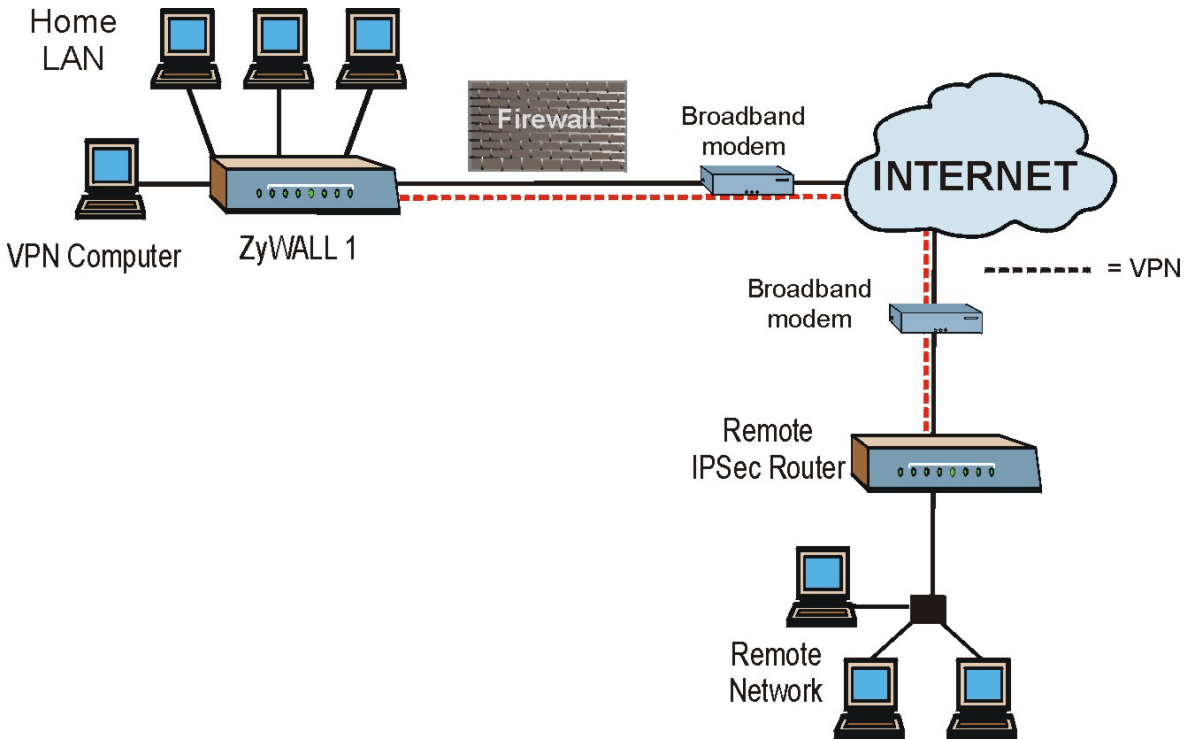
The ZyWALL has built-in message logging and packet tracing.

## **Embedded FTP and TFTP Services**

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

## **1.3 ZyWALL Application**

Connect the ZyWALL to the Internet via a broadband modem. A typical Internet access application is shown next. One computer on the LAN can use a VPN tunnel from the ZyWALL to a remote IPSec router.



**Figure 1-1 Internet Access Application**



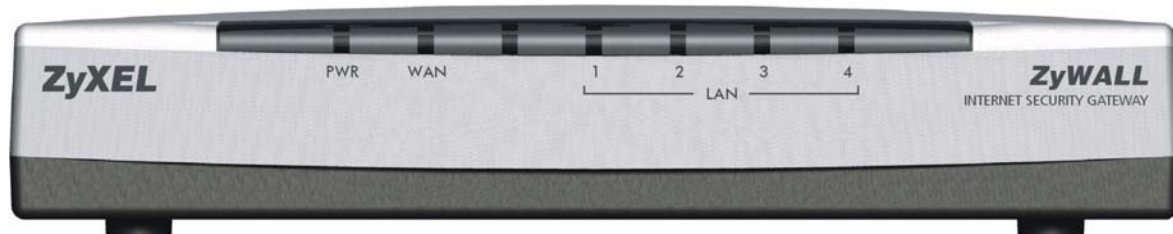
# Chapter 2

## Hardware Installation

*This chapter shows you how to connect hardware and perform the initial setup.*

### 2.1 ZyWALL Front Panel

The LEDs on the front panel indicate the operational status of the ZyWALL.



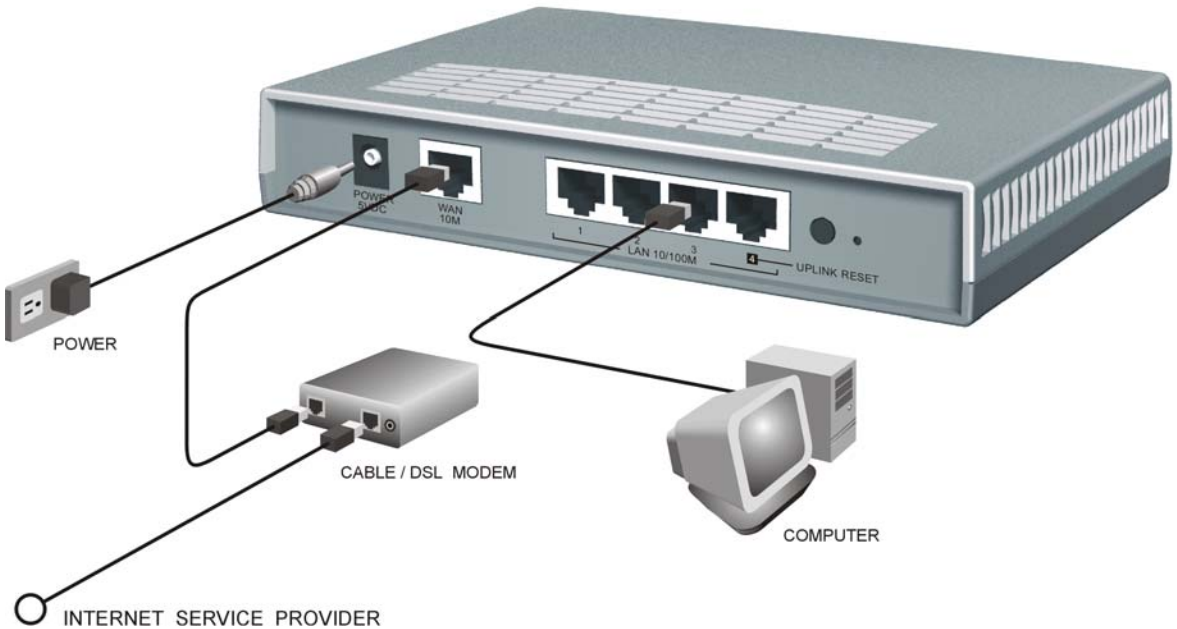
**Figure 2-1 Front Panel**

The following table describes ZyWALL LED functions.

LED	COLOR	STATUS	DESCRIPTION
PWR	Green	On	The ZyWALL is on and receiving power.
		Off	The ZyWALL is not receiving power.
		Flashing	The ZyWALL is performing a self-test.
WAN	Green	On	The WAN link is connected.
		Off	The WAN link is not ready, or has failed.
		Flashing	The 10M WAN link is sending/receiving packets.
LAN 1-4	Green	On	The ZyWALL is connected to a 10M LAN.
		Off	The 10M LAN is not connected.
		Flashing	The 10M LAN is sending/receiving packets.
	Orange	On	The ZyWALL is connected to a 100Mbps LAN.
		Off	The 100M LAN is not connected.
		Flashing	The 100M LAN is sending/receiving packets.

## 2.2 ZyWALL Rear Panel and Connections

The following figure shows the rear panel of your ZyWALL.



**Figure 2-2 Rear Panel**

### 2.2.1 WAN 10M Port

The WAN connection cable should be STP (Shielded Twisted Pair).

#### Connecting the ZyWALL to a Cable Modem

Connect the WAN 10M port on the ZyWALL to the Ethernet port on your cable modem using the Ethernet cable that came with your cable modem. The Ethernet port on a cable modem is sometimes labeled "PC" or "Workstation".

#### Connecting the ZyWALL to a DSL Modem

Connect the WAN 10M port on the ZyWALL to the Ethernet port on your DSL modem using the Ethernet cable that came with your DSL modem.

### 2.2.2 LAN 10/100M 1-4 Ports

You can connect up to four computers directly to the ZyWALL. For each computer, connect a 10/100M LAN port on the ZyWALL to the Network Adapter on the computer using a straight-through Ethernet cable.

If you want to connect more than three computers to your ZyWALL, you must use an external hub. Connect a 10/100M LAN port on the ZyWALL to a port on the hub using a crossover Ethernet cable.

When the ZyWALL is on and correctly connected to a computer or hub, the corresponding LAN LED on the front panel will turn on.

### 2.2.3 POWER 5VDC Port

Connect the round end of the power adapter to the port labeled **POWER 5VDC** on the rear panel of your ZyWALL.

---

**To avoid damage to the ZyWALL, make sure you use the correct power adapter. Refer to the Power Adapter Specification Appendix for this information.**

---

### 2.2.4 RESET Button

If you have forgotten your password or cannot access the ZyWALL you will need to use the RESET button on the rear panel of the ZyWALL to reload the factory-default configuration file. Uploading the configuration file replaces the current configuration file with the default configuration file and deletes all previous ZyWALL configurations. The following are the factory defaults for the ZyWALL.

- IP address: 192.168.1.1
- Password: 1234

### 2.2.5 Procedure To Use The RESET Button

- Step 1.** Use a pen or pointed object to press the RESET button for 5-10 seconds, then release it.
- Step 2.** If the LAN LEDs flash within 30 seconds, the factory defaults have been restored and the ZyWALL restarts. Otherwise, go to step 3.
- Step 3.** Turn the ZyWALL off.
- Step 4.** While pressing the RESET button, turn the ZyWALL on.
- Step 5.** Continue to hold the RESET button for about 30 seconds. The ZyWALL restarts.
- Step 6.** Release the RESET button and wait for the ZyWALL to finish restarting.

## 2.3 Additional Installation Requirements

1. A computer(s) with an installed Ethernet NIC (Network Interface Card).

2. A cable/xDSL modem and an ISP account.

## 2.4 Turning on Your ZyWALL

At this point, you should have connected the LAN port(s), the WAN port and the POWER port to the appropriate devices or lines. Plug the power adapter into an appropriate power source.

The PWR LED turns on. The WAN LED and the LAN LED (s) turn on after the system tests are complete if proper connections have been made to the LAN and WAN ports.

## 2.5 ZyWALL Configuration

### 2.5.1 Using the Web Configurator

The quickest and easiest way to configure the ZyWALL is via the web configurator. Some configuration options are available using FTP/TFTP (for example, you can use FTP to upload firmware) and CI commands, but the web configurator is by far the most comprehensive and user-friendly way to configure your ZyWALL.

### 2.5.2 Using FTP/TFTP

Refer to the *Firmware and Configuration File Maintenance Commands* chapter to learn how to upload firmware and configuration files using FTP/TFTP.

### 2.5.3 Using CI Commands

CI commands are recommended for advanced users only. Refer to the support notes for a list of CI commands.

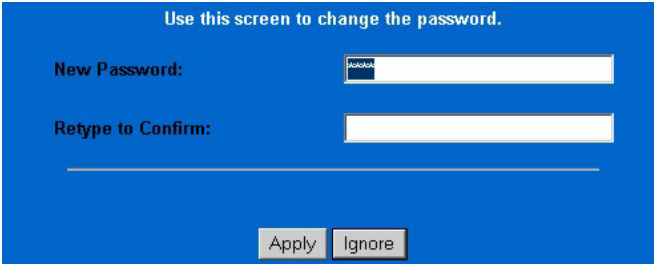
# Chapter 3

## Introducing the Web Configurator

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

### 3.1 Accessing the ZyWALL Web Configurator

- Step 1.** Make sure your ZyWALL hardware is properly connected (refer to instructions in *Chapter 2*).
- Step 2.** Prepare your computer/computer network to connect to the ZyWALL (refer to the *Quick Start Guide*).
- Step 3.** Launch your web browser.
- Step 4.** Type "192.168.1.1" as the URL.
- Step 5.** Type "1234" (default) as the password and click **Login**. In some versions, the default password appears automatically - if this is the case, click **Login**.
- Step 6.** 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**.



Use this screen to change the password.

New Password:

Retype to Confirm:

**Figure 3-1 Change Password Screen**

- Step 7.** You should now see the **MAIN MENU** screen.

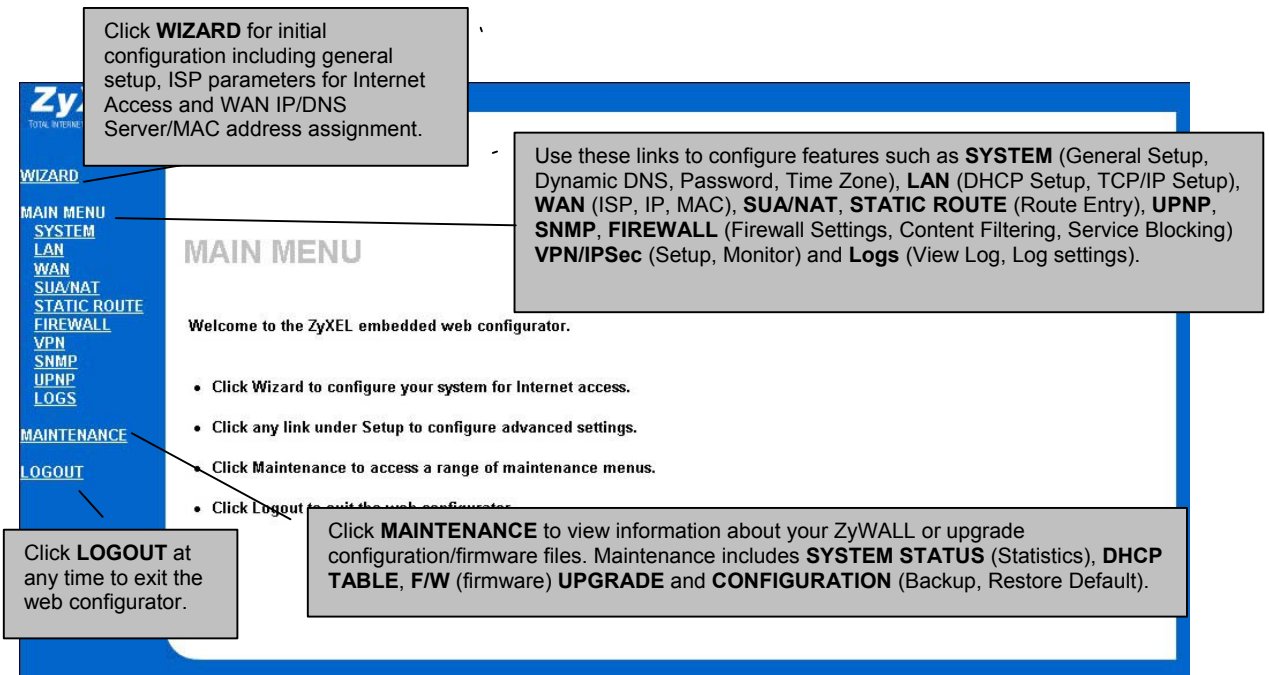
---

**The ZyWALL automatically times out after five minutes of inactivity. Simply log back into the ZyWALL if this happens to you.**

---

### 3.2 Navigating the ZyWALL Web Configurator

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



**Figure 3-2 The MAIN MENU Screen of the Web Configurator**

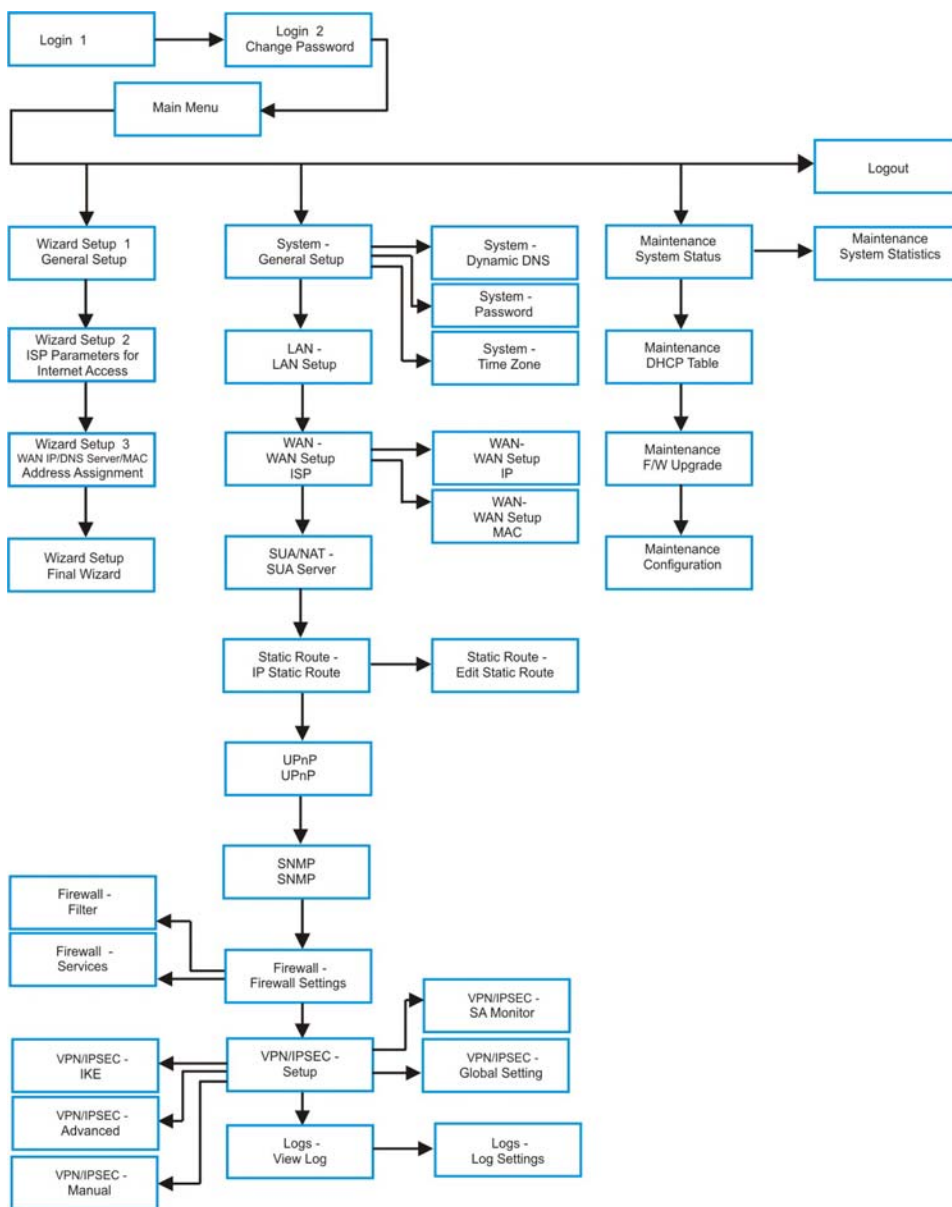
Follow the instructions you see in the **MAIN MENU** screen or click the  icon (located in the top right corner of most screens) to view embedded help.

The  icon does not appear in the **MAIN MENU** screen.

If you forget your password, refer to *section 2.2.4* to reset the default configuration file.

### 3.3 Overview of the ZyWALL Web Configurator

The following figure illustrates an overview of the features of the web configurator.



**Figure 3-3 Overview of the ZyWALL Web Configurator**





# Chapter 4

## Wizard Setup

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

### 4.1 Introduction to Wizard Screens

The Wizard consists of three screens to help you configure your device to access the Internet. The second 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.

#### 4.1.1 General Setup and System Name

**General Setup** contains administrative and system-related information. **System Name** is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name".

- In Windows 95/98 click **Start, Settings, Control Panel, Network**. Click the Identification tab, note the entry for the **Computer Name** field and enter it as the **System Name**.
- In Windows 2000, click **Start, Settings, Control Panel** and then double-click **System**. Click the **Network Identification** tab and then the **Properties** button. Note the entry for the **Computer name** field and enter it as the **System Name**.
- In Windows XP, click **Start, My Computer, View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the **ZyWALL System Name**.

#### 4.1.2 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) on each individual computer, the domain name can be assigned from the ZyWALL via DHCP.

Click **Next** to configure the ZyWALL for Internet access.

**WIZARD**

**General Setup:**  
This information is optional, but may be helpful in accessing services of your Internet Service Provider, such as mail and news servers and customer support web pages.

Enter a descriptive name for identification purposes. We recommend using your computer's name.

System Name:

The ISP's domain name is often sent automatically by the ISP to the router. If you are having difficulty accessing ISP services, you may need to enter the Domain Name manually in the field below.

For example, if the full address of your ISP's mail server is mail.www.my.domain.com, then the Domain Name is www.my.domain.com

Domain Name:

Next

Figure 4-1 Wizard 1

## 4.2 Wizard Setup: Screen 2

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

### 4.2.1 Ethernet

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

WIZARD SETUP

ISP Parameters for Internet Access

Encapsulation	Ethernet
Service Type	Standard
User Name	N/A
Password	N/A
Login Server IP Address	N/A

Back Next

Table 4-1 Wizard 2: Ethernet Encapsulation

Table 4-2 Ethernet Encapsulation

FIELD	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	You must choose the <b>Ethernet</b> option when the WAN port is used as a regular Ethernet. Otherwise, choose <b>PPPoE</b> or <b>PPTP</b> for a dial-up connection.
Service Type	Choose from <b>Standard</b> or <b>RR login</b> . Choose RoadRunner flavor if your ISP is Time Warner's RoadRunner; otherwise choose <b>Standard</b> . The <b>User Name</b> , <b>Password</b> and <b>Login Server IP Address</b> fields are not applicable (N/A) for the latter.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.

**Table 4-2 Ethernet Encapsulation**

<b>FIELD</b>	<b>DESCRIPTION</b>
Login Server IP Address	Type the authentication server IP address here if your ISP gave you one.
Login Server (Telia Login only)	Type the domain name of the Telia login server, for example "login1.telia.com".
Relogin Period (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.
To continue, click <b>Next</b> . To return to the previous screen, click <b>Back</b> .	

### 4.2.2 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 the appendices for more information on PPTP.

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

**WIZARD SETUP**

**ISP Parameters for Internet Access**

Encapsulation: PPTP

User Name: \_\_\_\_\_

Password: \_\_\_\_\_

Nailed-Up Connection

Idle Timeout: 100 (In Second)

---

**PPTP Configuration**

My IP Address: 10.0.0.140

My IP Subnet: 0.0.0.0

Mask: \_\_\_\_\_

Server IP Address: 10.0.0.138

Connection ID/Name: \_\_\_\_\_

Back Next

Figure 4-2 Wizard 2: PPTP Encapsulation

Table 4-3 PPTP Encapsulation

FIELD	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	Select <b>PPTP</b> from the drop-down list box.
User Name	Type the user name given to you by your ISP.

**Table 4-3 PPTP Encapsulation**

<b>FIELD</b>	<b>DESCRIPTION</b>
Password	Type the password associated with the User Name above.
Nailed Up Connection	Select <b>Nailed Up Connection</b> 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. The default is 45 seconds.
PPTP Configuration	
My IP Address	Type the (static) IP address assigned to you by your ISP.
My IP Subnet Mask	Type the subnet mask assigned to you by your ISP (if given).
Server IP Address	Type the IP address of the PPTP server.
Connection ID/Name	Enter the connection ID or connection name in this field. It must follow the "c:id" and "n:name" format. For example, C:12 or N:My ISP. This field is optional and depends on the requirements of your xDSL modem.
To continue, click <b>Next</b> . To return to the previous screen, click <b>Back</b> .	

### 4.2.3 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 the appendices for more information on Pope.

**WIZARD SETUP**

**ISP Parameters for Internet Access**

Encapsulation

Service Name

User Name

Password

Nailed-Up Connection

Idle Timeout  (In Second)

**Figure 4-3 Wizard2: PPPoE Encapsulation**

**Table 4-4 PPPoE Encapsulation**

FIELD	DESCRIPTION
ISP Parameter for Internet Access	
Encapsulation	Choose an encapsulation method from the pull-down list box. PPPoE forms a dial-up connection.
Service Name (Optional)	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.

**Table 4-4 PPPoE Encapsulation**

<b>FIELD</b>	<b>DESCRIPTION</b>
Nailed Up Connection	Select <b>Nailed Up Connection</b> 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 <b>100</b> seconds.
To continue, click <b>Next</b> . To return to the previous screen, click <b>Back</b> .	

## 4.3 Wizard Setup: Screen 3

### 4.3.1 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 4-5 Private IP Address Ranges**

10.0.0.0	-	10.255.255.255
172.16.0.0	-	172.31.255.255
192.168.0.0	-	192.168.255.255

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



---

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

---

## 4.3.2 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.

## 4.3.3 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](http://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.

There are two ways that an ISP disseminates the DNS server addresses.

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, enter them in the DNS Server fields in DHCP Setup.
2. Leave the DNS Server fields in DHCP Setup blank (for example 0.0.0.0). The ZyWALL acts as a DNS proxy when this field is blank.

### 4.3.4 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 digits, 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 workstation 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.

---

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

---

Your ZyWALL WAN Port is always set at half-duplex mode as most cable/DSL modems only support half-duplex mode. Make sure your modem is in half-duplex mode. Your ZyWALL supports full duplex mode on the LAN side.

**Table 4-6 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)

**WIZARD SETUP**

**WAN IP Address Assignment**

Get automatically from ISP (Default)  
 Use fixed IP address

IP Address   
 IP Subnet Mask   
 Gateway IP Address

**DNS Server Address Assignment**

Get automatically from ISP (Default)  
 Use fixed IP Address - DNS Server IP Address

Primary DNS Server   
 Secondary DNS Server

**WAN MAC Address**

Factory default  
 Spoof this computer's MAC Address - IP Address

Back Finish

Figure 4-4 Wizard 3

Table 4-7 WAN Setup

FIELD	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.
IP Address	Enter your WAN IP address in this field if you selected <b>Use Fixed IP Address</b> .
IP Subnet Mask	Enter the IP subnet mask in this field if you selected <b>Use Fixed IP Address</b> .
Gateway IP Address	Enter the gateway IP address in this field if you selected <b>Use Fixed IP Address</b> .
DNS Server Address Assignment	

**Table 4-7 WAN Setup**

<b>FIELD</b>	<b>DESCRIPTION</b>
Get automatically from ISP	Select this option if your ISP does not give you DNS server addresses. This option is selected by default.
Use fixed IP address - DNS Server IP Address	Select this option If your ISP provides you a DNS server address.
Primary/Secondary DNS Server	If you selected the <b>Use fixed IP address – Primary/Secondary DNS Server</b> option, enter the provided DNS addresses in these fields.
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 workstation 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.
To return to the previous screen, click <b>Back</b> . To complete and save the wizard setup, click <b>Finish</b> .	

## 4.4 Basic Setup Complete

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

---

# Part II:

---

## Advanced

---

This part covers System, LAN, WAN, SUA/NAT, Static Route, UPnP and SNMP.



# Chapter 5 System

*This chapter provides information on the System screens in the web configurator.*

## 5.1 About System Setup

See the *Wizard Setup* chapter for more information on the next few screens.

## 5.2 General Setup

From the **MAIN MENU**, click **SYSTEM**. The screen appears as shown next. This is the screen for the **General** tab.

The screenshot shows the 'SYSTEM' configuration page with the 'General' tab selected. The form includes the following fields:

- System Name**: A text input field.
- Domain Name**: A text input field.
- Administrator Inactivity Timer**: A numeric input field with the value '0' and a note '(minutes, 0 means no timeout)'.

Buttons for 'Apply' and 'Reset' are located at the bottom of the form.

**Figure 5-1 System General Setup**

**Table 5-1 System General Setup**

FIELD	DESCRIPTION	EXAMPLE
System Name	Choose a descriptive name for identification purposes. It is recommended you enter your computer's "Computer name" in this field (see the <i>Wizard Setup</i> chapter for how to find your computer's name). This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.	MyComputer

**Table 5-1 System General Setup**

FIELD	DESCRIPTION	EXAMPLE
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.	zyxel.com.tw
Administrator Inactivity Timer	Type how many minutes a management session 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).	5
Click <b>Apply</b> to save your changes back to the ZyWALL. Click <b>Reset</b> to begin configuring this screen afresh.		

## 5.3 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 DNS-like address (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](http://www.dyndns.org). This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a DNS name. The Dynamic DNS service provider will give you a password or key.

### 5.3.1 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.

---

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

---

### 5.3.2 Procedure To Configure Dynamic DNS

From the **MAIN MENU**, click **SYSTEM** and **DDNS**.



**DYNAMIC DNS**

**General**    **DDNS**    **Password**    **Time Zone**

---

Active

Service Provider: WWW.DynDNS.ORG

DDNS Type: Dynamic DNS

Host Name1:

Host Name2:

Host Name3:

User:

Password:

Enable Wildcard

Off Line

Edit Update IP Address:

Server Auto Detect

User Specify

IP Addr:

---

Apply    Reset

Figure 5-2 System DDNS

Table 5-2 System DDNS

FIELD	DESCRIPTION	EXAMPLE
Active	Select this check box to use dynamic DNS.	
Service Provider	Select the name of your Dynamic DNS service provider.	www.dyndns.org
DDNS Type	Select the type of service that you are registered for from your Dynamic DNS service provider.	
Host Names 1~3	Enter the host names in the three fields provided. You can specify up to two host names in each field separated by a comma (",").	
E-Mail Address	Enter the e-mail address of the host in this field.	
User	Enter your user name.	Joe
Password	Enter the password assigned to you.	

Table 5-2 System DDNS

FIELD	DESCRIPTION	EXAMPLE
Enable Wildcard	Select the check box to enable DYNDNS Wildcard.	
Off Line	This option is available when <b>CustomDNS</b> is selected in the <b>DDNS Type field</b> . Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line.	
Edit Update IP Address		
Server Auto Detect	Select this option to update the IP address of the host name(s) automatically by the DDNS server.	
User Specify	Select this option to update the IP address of the host name(s) to the IP address specified below. Use this option if you have a static IP address.	
IP Addr	Enter the IP address if you select the <b>User Specify</b> option.	
Click <b>Apply</b> to save your changes back to the ZyWALL. Click <b>Reset</b> to begin configuring this screen afresh.		

## 5.4 Password

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

The screenshot shows the 'PASSWORD' configuration page. At the top, the word 'PASSWORD' is displayed in a large, light blue font. Below it, there are four tabs: 'General', 'DDNS', 'Password', and 'Time Zone'. The 'Password' tab is currently selected and highlighted in yellow. The main content area has a yellow background and contains three text input fields stacked vertically, labeled 'Old Password', 'New Password', and 'Retype to Confirm'. At the bottom of the page, there are two buttons: 'Apply' and 'Reset'.

Figure 5-3 System Password

Table 5-3 System Password

FIELD	DESCRIPTION
Old Password	Type the default password or the existing password you use to access the system in this field.
New Password	Type the new password in this field.
Retype to Confirm	Type the new password again in this field.
Click <b>Apply</b> to save your changes back to the ZyWALL. Click <b>Reset</b> to begin configuring this screen afresh.	

## 5.5 Time Zone

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

### TIME ZONE

General
DDNS
Password
Time Zone

**Use Time Server when Bootup** NTP (RFC-1305) ▾

**Time Server IP Address** tick.stdtime.gov.tw

**Current Time (hh-mm-ss)** 21 : 47 : 1

**New Time (hh-mm-ss)** 21 : 46 : 54

**Current Date (yyyy-mm-dd)** 2000 / 1 / 1

**New Date (yyyy-mm-dd)** 2000 / 1 / 1

**Time Zone** (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London ▾

**Daylight Savings**

**Start Date (mm-dd)** 0 month 0 day

**End Date (mm-dd)** 0 month 0 day

Apply
Reset

Figure 5-4 System Time/Date

Table 5-4 System Time/Date

FIELD	DESCRIPTION
Use Time Server when Bootup	Enter 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 differences between them are the format. <b>Daytime (RFC 867)</b> format is day/month/year/time zone of the server. <b>Time (RFC-868)</b> format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. <b>NTP (RFC-1305)</b> is similar to <b>Time (RFC-868)</b> . <b>None.</b> If you chose <b>None</b> , then you need to enter the time manually.
Time Server IP Address	Enter the IP address or domain name of your time server. Check with your ISP/network administrator if you are unsure of this information.
Current Time	This field displays an updated time only when you reenter this menu.
New Time	Enter the new time in hour, minute and second format.
Current Date	This field displays an updated date only when you re-enter this menu.
New Date	Enter the new date in year, month and day format.
Time Zone	Select your time zone from the pull down list.
Daylight Savings	Select this option if you use daylight savings time. 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.
Start Date	Enter the month and day that your daylight-savings time starts on if you selected <b>Daylight Savings</b> .
End Date	Enter the month and day that your daylight-savings time ends on if you selected <b>Daylight Savings</b> .
Click <b>Apply</b> to save your changes back to the ZyWALL. Click <b>Reset</b> to begin configuring this screen afresh.	

# Chapter 6

## LAN and WAN

*This chapter describes how to configure LAN and WAN settings using the web configurator.*

### 6.1 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 set to **None**, DHCP service will be disabled and you must have another DHCP server on your LAN, or else the computer must be manually configured.

#### 6.1.1 IP Pool Setup

The ZyWALL is pre-configured with a pool of 32 IP addresses starting from 192.168.1.33 to 192.168.1.64. This configuration leaves 31 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.

#### 6.1.2 Primary and Secondary DNS Server

Refer to the *IP Address and Subnet Mask* section in the **Wizard Setup** chapter.

### 6.2 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.

#### 6.2.1 Factory LAN Defaults

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

**Step 1.** IP address of 192.168.1.1 with subnet mask of 255.255.255.0 (24 bits)

**Step 2.** DHCP server enabled with 32 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.

#### 6.2.2 IP Address and Subnet Mask

Refer to the *IP Address and Subnet Mask* section in the **Wizard Setup** chapter for this information.

### 6.2.3 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**.

### 6.2.4 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.

**LAN SETUP**

**IP**

---

**DHCP Setup**

---

**DHCP Server**

**IP Pool Starting Address**  **Pool Size**

**Primary DNS Server**

**Secondary DNS Server**

---

**LAN TCP/IP**

---

**IP Address**  **RIP Direction**

**IP Subnet Mask**  **RIP Version**

**Multicast**

---

**Windows Networking (NetBIOS) Broadcast Pass Through**

---

**From LAN to WAN**

---

Figure 6-1 LAN Setup

Table 6-1 LAN Setup

FIELD	DESCRIPTION
DHCP Server	This field enables/disables the DHCP server. Select <b>DHCP Server</b> to have your ZyWALL act as a DHCP server; otherwise, the DHCP server will be disabled. When enabled, the following items need to be set:
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.
Primary DNS Server Secondary DNS Server	Type the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.
LAN TCP/IP	

Table 6-1 LAN Setup

FIELD	DESCRIPTION
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	RIP (Routing Information Protocol, RFC1058 and RFC 1389) allows a router to exchange routing information with other routers. The <b>RIP Direction</b> field controls the sending and receiving of RIP packets. Select the RIP direction from <b>Both/In Only/Out Only/None</b> . When set to <b>Both</b> or <b>Out Only</b> , the ZyWALL will broadcast its routing table periodically. When set to <b>Both</b> or <b>In Only</b> , it will incorporate the RIP information that it receives; when set to <b>None</b> , it will not send any RIP packets and will ignore any RIP packets received. <b>Both</b> is the default.
RIP Version	The <b>RIP Version</b> field controls the format and the broadcasting method of the RIP packets that the ZyWALL sends (it recognizes both formats when receiving). <b>RIP-1</b> 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 <b>RIP-2B</b> and <b>RIP-2M</b> sends the routing data in RIP-2 format; the difference being that <b>RIP-2B</b> uses subnet broadcasting while <b>RIP-2M</b> 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 <b>Both</b> and the Version set to <b>RIP-1</b> .
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 ( <b>IGMP-v1</b> ) and version 2 ( <b>IGMP-v2</b> ).
<p>Windows Networking (NetBIOS) Broadcast Pass Through: NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to connect to and communicate with a LAN.</p> <p>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.</p>	
From LAN to WAN	Select this check box to allow NetBIOS packets to pass through to the WAN in order to find a computer on the WAN.
<p>Click <b>Apply</b> to save your changes back to the ZyWALL.</p> <p>Click <b>Reset</b> to begin configuring this screen afresh.</p>	



## 6.3 WAN Setup

To configure the WAN, click **WAN** from the **MAIN MENU**. For more information, refer to the chapter on **Wizard Setup**.

### 6.3.1 WAN Setup: ISP Ethernet Encapsulation

Click the **ISP** tab. The screen shown next is for **Ethernet** encapsulation. The screen differs by the encapsulation.

**Figure 6-2 Ethernet Encapsulation**

**Table 6-2 Ethernet Encapsulation**

FIELD	DESCRIPTION
Encapsulation	You must choose the Ethernet option when the WAN port is used as a regular Ethernet.
Service Type	Choose from <b>Standard</b> , <b>Telstra</b> (RoadRunner Telstra authentication method), <b>RR-Manager</b> (Roadrunner Manager authentication method), <b>RR-Toshiba</b> (Roadrunner Toshiba authentication method) or <b>Telia Login</b> . The following fields do not appear with the <b>Standard</b> service type.
User Name	Type the user name given to you by your ISP.

**Table 6-2 Ethernet Encapsulation**

FIELD	DESCRIPTION
Password	Type the password associated with the user name above.
Login Server IP Address	Type the authentication server IP address here if your ISP gave you one.
Login Server (Telia Login only)	Type the domain name of the Telia login server, for example "login1.telia.com".
Relogin Period (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.
Click <b>Apply</b> to save your changes back to the ZyWALL. Click <b>Reset</b> to begin configuring this screen afresh.	

## PPPoE Encapsulation

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

### WAN SETUP

ISP
IP
MAC

**ISP Parameters for Internet Access**

Encapsulation

Service Name  (optional)

User Name

Password

Idle Timeout  (in seconds)

**Figure 6-3 PPPoE Encapsulation**

**Table 6-3 PPPoE Encapsulation**

FIELD	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. xDSL, 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.
User Name	Type the User Name given to you by your ISP.
Password	Type the password associated with the User Name above.
Idle Timeout	This value specifies the time in seconds that elapses before the router automatically disconnects from the PPPoE server.
Click <b>Apply</b> to save your changes back to the ZyWALL. Click <b>Reset</b> to begin configuring this screen afresh.	

## PPTP Encapsulation

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

**WAN SETUP**

ISP    IP    MAC

---

**ISP Parameters for Internet Access**

---

Encapsulation    PPTP

User Name    \_\_\_\_\_

Password    \_\_\_\_\_

Idle Timeout    100 (in seconds)

---

**PPTP Configuration**

---

My IP Address    0.0.0.0

My IP Subnet Mask    0.0.0.0

Server IP Address    0.0.0.0

Connection ID/Name    \_\_\_\_\_

---

Apply    Reset

**Figure 6-4 PPTP Encapsulation**

**Table 6-4 PPTP Encapsulation**

FIELD	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 My Login and Password fields for a PPP connection and the PPTP parameters for a PPTP connection.
Service Name	Type the PPPoE service name provided to you. PPPoE uses a service name to identify and reach the PPPoE server.
User Name	Type the User Name given to you by your ISP.
Password	Type the password associated with the User Name above.

**Table 6-4 PPTP Encapsulation**

<b>FIELD</b>	<b>DESCRIPTION</b>
Idle Timeout	This value specifies the time in seconds that elapses before the ZyWALL automatically disconnects from the PPTP server.
PPTP Encapsulation	
My IP Address	Type the (static) IP address assigned to you by your ISP.
Server IP Address	Type the IP address of the PPTP server.
Connection ID/Name	Type your identification name for the PPTP server.
Click <b>Apply</b> to save your changes back to the ZyWALL. Click <b>Reset</b> to begin configuring this screen afresh.	

### **6.3.2 WAN Setup: IP**

Click the **IP** tab to display the **IP Setup** screen shown next.

## WAN

ISP
IP
MAC

### WAN IP Address Assignment

Get automatically from ISP (Default)  
 Use fixed IP address

My Wan IP Address   
 My Wan IP Subnet Mask   
 Remote IP Address

---

Network Address Translation   
 RIP Direction   
 RIP Version   
 Multicast

---

### Windows Networking (NetBIOS over TCP/IP)

Allow From WAN to LAN (You also need to create a SUA server!)  
 Allow Trigger Dial

**Figure 6-5 IP Setup**

**Table 6-5 IP Setup**

FIELD	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.
IP Address	Enter your WAN IP address in this field if you selected <b>Use Fixed IP Address</b> .
IP Subnet Mask	Enter the IP subnet mask (if your ISP gave you one) in this field if you selected <b>Use Fixed IP Address</b> .

**Table 6-5 IP Setup**

FIELD	DESCRIPTION
Gateway IP Address	Enter the gateway IP address (if your ISP gave you one) in this field if you selected <b>Use Fixed IP Address</b> .
Network Address Translation	<p>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.</p> <p><b>SUA</b> (Single User Account) is a subset of NAT that supports Many-to-One and Server mappings.</p> <p>Refer to Chapter 7 for more information about NAT.</p>
RIP Direction	<p>RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The <b>RIP Direction</b> field controls the sending and receiving of RIP packets.</p> <p>Choose <b>Both</b>, <b>None</b>, <b>In Only</b> or <b>Out Only</b>.</p> <p>When set to <b>Both</b> or <b>Out Only</b>, the ZyWALL will broadcast its routing table periodically.</p> <p>When set to <b>Both</b> or <b>In Only</b>, the ZyWALL will incorporate RIP information that it receives.</p> <p>When set to <b>None</b>, the ZyWALL will not send any RIP packets and will ignore any RIP packets received.</p> <p>By default, <b>RIP Direction</b> is set to <b>Both</b>.</p>
RIP Version	<p>The <b>RIP Version</b> field controls the format and the broadcasting method of the RIP packets that the ZyWALL sends (it recognizes both formats when receiving).</p> <p>Choose <b>RIP-1</b>, <b>RIP-2B</b> or <b>RIP-2M</b>.</p> <p><b>RIP-1</b> is universally supported; but <b>RIP-2</b> carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both <b>RIP-2B</b> and <b>RIP-2M</b> 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 <b>RIP Version</b> field is set to <b>RIP-1</b>.</p>

Table 6-5 IP Setup

FIELD	DESCRIPTION
Multicast	Choose <b>None</b> (default), <b>IGMP-V1</b> or <b>IGMP-V2</b> . 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.
Windows Networking (NetBIOS over TCP/IP) Pass Through: 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 From WAN to LAN	Select this check box to allow NetBIOS packets from the WAN port to the LAN port. In order to forward NetBIOS packets from the WAN to the LAN, you must also configure the <b>SUA/NAT</b> screen for one of the following. 1. (Recommended) Set a port forwarding entry for ports 137 to 139 and another port forwarding entry for port 445. 2. Set a default server.
Allow Trigger Dial	Select this check box to stop NetBIOS packets from initiating calls.
Click <b>Apply</b> to save your changes back to the ZyWALL. Click <b>Reset</b> to begin configuring this screen afresh.	

### 6.3.3 WAN Setup: MAC

Click on the **MAC** tab to display the **MAC Setup** screen shown next.



The screenshot shows the 'WAN SETUP' interface. At the top, there are three tabs: 'ISP', 'IP', and 'MAC'. The 'MAC' tab is selected. Below the tabs, the 'WAN MAC Address' section is visible. It contains two radio button options: 'Factory default' (which is selected) and 'Spoof this computer's MAC Address - IP Address'. The second option has a text input field next to it containing the IP address '192.168.1.33'. At the bottom of the section, there are two buttons: 'Apply' and 'Reset'.

**Figure 6-6 MAC Setup**

The MAC address screen allows users 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. Choose **Factory Default** to select the factory assigned default MAC Address.

Otherwise, click **Spoof this computer's MAC address - IP 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.



# Chapter 7

## SUA/NAT

*This chapter discusses how to configure SUA/NAT on the ZyWALL*

### 7.1 The SUA/NAT Screen

This section discusses SUA (Single User Account)/NAT (Network Address Translation) applications of the ZyWALL.

#### 7.1.1 Introduction

SUA (Single User Account) is a ZyNOS implementation of a subset of NAT (Network Address Translation).

#### 7.1.2 The SUA Server Screen

A SUA server 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 SUA 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.

#### Default Server IP Address

In addition to the servers for specified services, NAT supports a default server IP address. A default server receives packets from ports that are not specified in this screen.

---

**If you do not assign a Default Server IP Address, then all packets received for ports not specified in this screen will be discarded.**

---

#### 7.1.3 Services and Port Numbers

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 SUA/NAT.

**Table 7-1 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

### 7.1.4 Configuring Servers Behind SUA (Example)

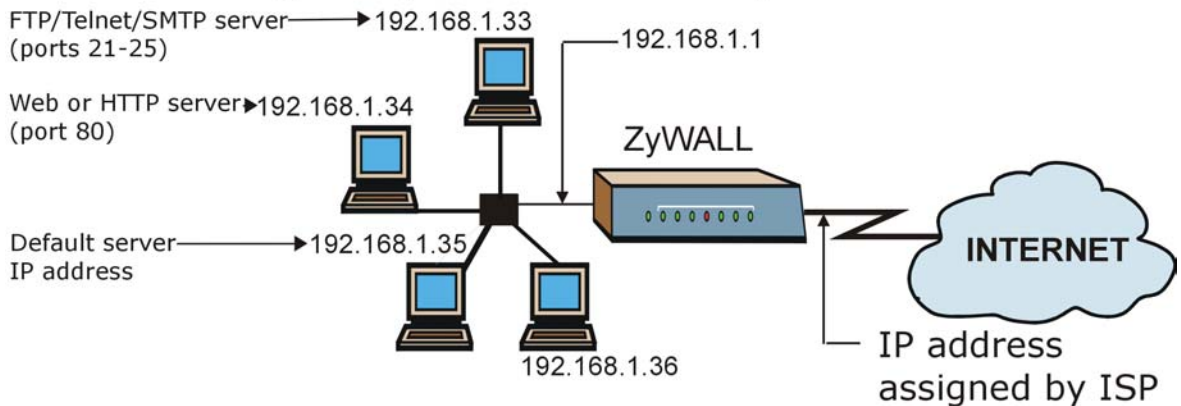
Let's say you want to assign ports 22-25 to one server, port 80 to another and assign a default server IP address of 192.168.1.35 as shown in the next figure.

Private network IP  
addresses assigned by user

FTP/Telnet/SMTP server → 192.168.1.33  
(ports 21-25)

Web or HTTP server → 192.168.1.34  
(port 80)

Default server  
IP address → 192.168.1.35



The NAT network appears as  
a single host on the Internet

**Figure 7-1 Multiple Servers Behind NAT Example**

When you configure NAT port forwarding rules, the firewall automatically allows traffic originating from the WAN (for the services specified) to be forwarded to the LAN IP address(es) configured here.

**If you do not assign a Default Server IP Address, then all packets received for ports not specified in this screen will be discarded.**

SUA/NAT

SUA Server

Default Server

#	Active	Name	Start Port	End Port	Server IP Address
1	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0.0.0.0"/>
2	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0.0.0.0"/>
3	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0.0.0.0"/>
4	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0.0.0.0"/>
5	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0.0.0.0"/>
6	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0.0.0.0"/>
7	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0.0.0.0"/>
8	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0.0.0.0"/>
9	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0.0.0.0"/>
10	<input type="checkbox"/>	<input type="text"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0.0.0.0"/>

Respond to Ping on Internet WAN Port

Figure 7-2 SUA/NAT Setup

Table 7-2 SUA/NAT Setup

FIELD	DESCRIPTION
Default Server	In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in this screen. If you do not assign a default server IP address, then all packets received for ports not specified in this screen will be discarded. Assigning a default server IP address turns off the firewall protection for that IP address.
#	Number of an individual SUA server entry.
Active	Select this check box to enable the SUA server entry. Clear this checkbox 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.
Start Port	Enter a port number here. To forward only one port, enter it again in the <b>End Port</b> field. To specify a range of ports, enter the last port to be forwarded in the <b>End Port No</b> field
End Port	
Server IP Address	Enter the inside IP address of the server here.
Respond to Ping on Internet WAN Port	Select the check box to enable a ping response from the Internet WAN port. Clear the check box to disable a ping response from the Internet WAN port.
Click <b>Apply</b> to save your changes back to the ZyWALL. Click <b>Reset</b> to begin configuring this screen afresh.	

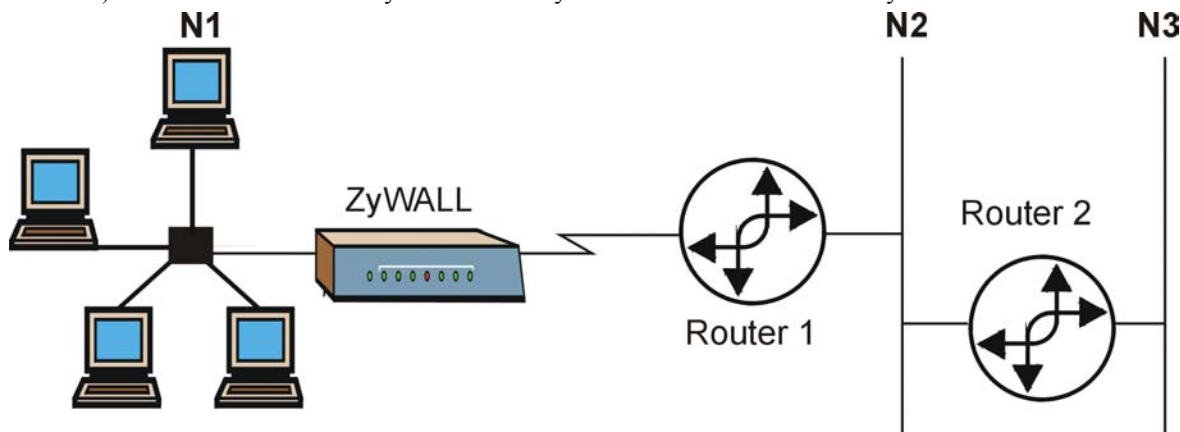
# Chapter 8

## Static Route

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

### 8.1 General Information About Static Routes

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 8-1 Example of Static Routing Topology**

### 8.2 IP Static Route Summary

From the **MAIN MENU**, click **STATIC ROUTE**. The screen shown next appears.

STATIC ROUTE

IP Static Route

Static Route Summary Table

#	Name	Active	Destination	Gateway
1	-	-	...	...
2	-	-	...	...
3	-	-	...	...
4	-	-	...	...
5	-	-	...	...
6	-	-	...	...
7	-	-	...	...
8	-	-	...	...

Edit

Figure 8-2 IP Static Route Summary

Table 8-1 IP Static Route Summary

FIELD	DESCRIPTION
#	This is the index number of an individual IP static route entry.
Name	This is the name given to the IP static route.
Active	This field allows you to activate/deactivate this static route.
Destination	This field displays the destination IP address.
Gateway	This field displays the gateway IP address.
To set up or edit a static route on the ZyWALL, click a static route index number, then click <b>Edit</b> .	

### 8.2.1 Editing IP Static Route

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



**STATIC ROUTE**

**Route Entry**

Route Name  (Leave this field blank to delete this route.)

Active

Destination IP Address

IP Subnet Mask

Gateway IP Address

Metric

Private

Figure 8-3 Edit IP Static Route

Table 8-2 Edit IP Static Route

FIELD	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 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	Metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.

**Table 8-2 Edit IP Static Route**

FIELD	DESCRIPTION
Private	This parameter determines if the ZyWALL will include the route to this remote node in its RIP broadcasts. If set to <b>Yes</b> , this route is kept private and not included in RIP broadcast. If <b>No</b> , the route to this remote node will be propagated to other hosts through RIP broadcasts.
Click <b>Apply</b> to save your changes back to the ZyWALL. Click <b>Reset</b> to begin configuring this screen afresh.	

# Chapter 9

## UPnP

*This chapter introduces the Universal Plug and Play feature.*

### 9.1 Introducing Universal Plug and Play

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.

#### 9.1.1 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.

#### 9.1.2 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 the *SUA/NAT* chapter for further information about NAT.

#### 9.1.3 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.

## 9.2 UPnP and ZyXEL

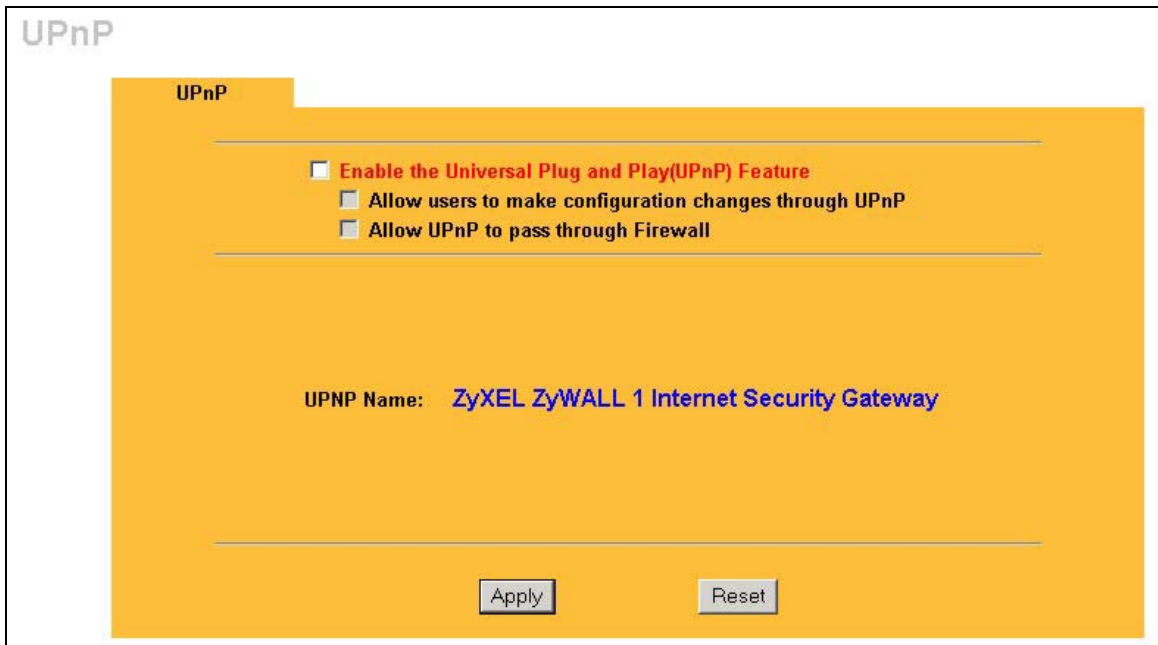
ZyXEL has achieved UPnP certification from the Universal Plug and Play Forum Creates UPnP™ Implementers Corp. (UIC). ZyXEL's UPnP implementation supports IGD 1.0 (Internet Gateway Device). At the time of writing ZyXEL's UPnP implementation supports Windows Messenger 4.6 and 4.7 while Windows Messenger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

UPnP broadcasts are only allowed on the LAN.

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

### 9.2.1 Configuring UPnP

From the **MAIN MENU** click **UPnP** to display the screen shown next.



**Figure 9-1 Configuring UPnP**

**Table 9-1 Configuring UPnP**

FIELD	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).
UPnP Name	This identifies the ZyXEL device in UPnP applications.
Click <b>Apply</b> to save your changes back to the ZyWALL. Click <b>Reset</b> to begin configuring this screen afresh.	

## 9.3 Installing UPnP in Windows Example

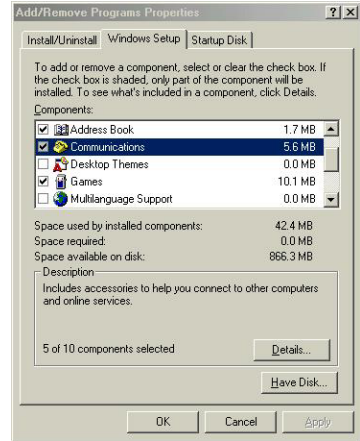
This section shows how to install UPnP in Windows Me and Windows XP.

### Installing UPnP in Windows Me

Follow the steps below to install UPnP in Windows Me.

**Step 1.** Click **Start** and **Control Panel**. Double-click **Add/Remove Programs**.

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

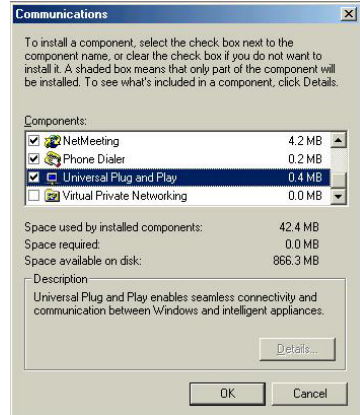


**Step 3.** In the **Communications** window, select the **Universal Plug and Play** check box in the **Components** selection box.

**Step 4.** Click **OK** to go back to the **Add/Remove Programs Properties** window and click **Next**.

**Step 5.** Restart the computer when prompted.

**Step 3.**



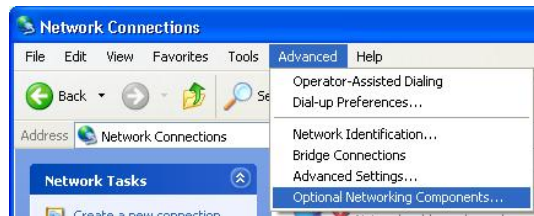
## Installing UPnP in Windows XP

Follow the steps below to install UPnP in Windows XP.

**Step 1.** Click **start** and **Control Panel**.

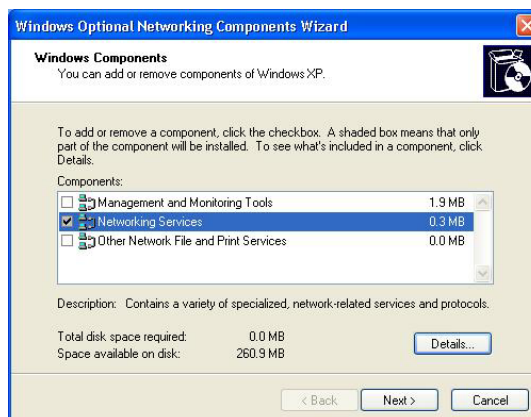
**Step 2.** Double-click **Network Connections**.

**Step 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.



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

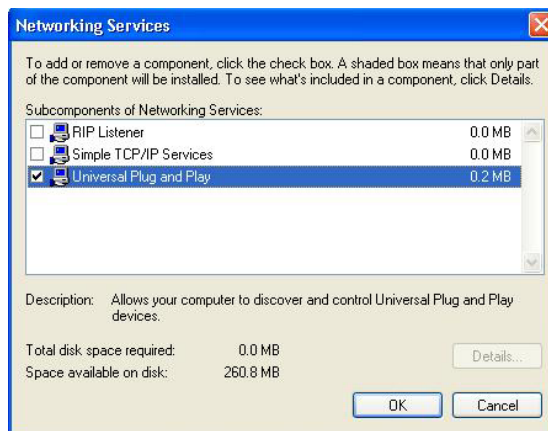
**Step 4.**



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

**Step 6.** Click **OK** to go back to the **Windows Optional Networking Component Wizard** window and click **Next**.

**Step 5.**



## 9.4 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.

## Auto-discover Your UPnP-enabled Network Device

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

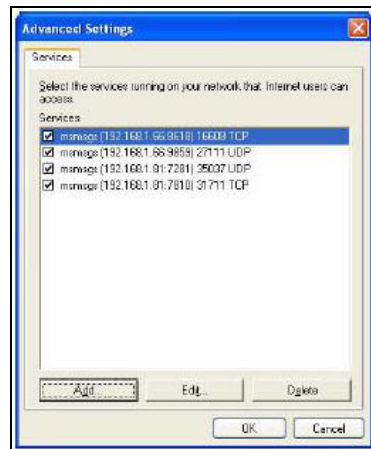
**Step 2.** Right-click the icon and select **Properties**.



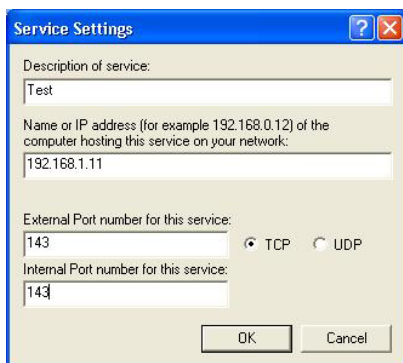
**Step 3.** In the **Internet Connection Properties** window, click **Settings** to see the port mappings that were automatically created.



**Step 4.** You may edit or delete the port mappings or click **Add** to manually add port mappings.





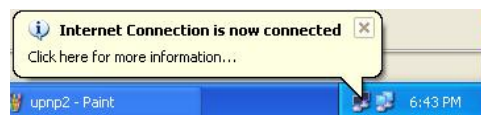



---

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

---

**Step 5.** Select the **Show icon in notification area when connected** check box and click **OK**. An icon displays in the system tray



**Step 6.** Double-click the icon to display your current Internet connection status.

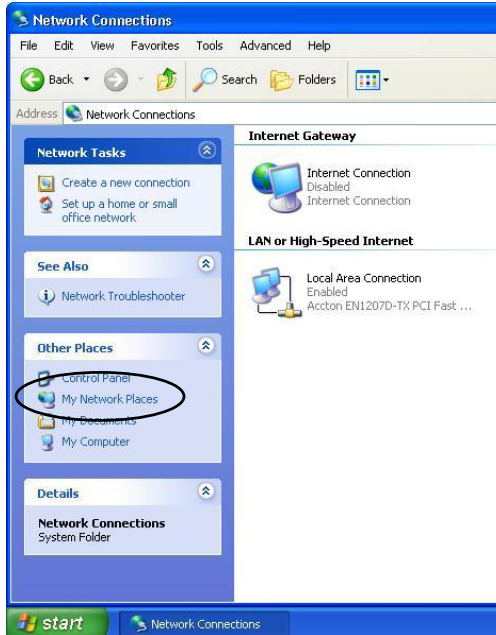


## Web Configurator Easy Access

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.

- Step 1.** Click **start** and then **Control Panel**.
- Step 2.** Double-click **Network Connections**.
- Step 3.** Select **My Network Places** under **Other Places**.



- Step 4.** An icon with the description for each UPnP-enabled device displays under **Local Network**.
- Step 5.** Right-click the icon for your ZyXEL device and select **Invoke**. The web configurator login screen displays.



**Step 6.** Right-click the icon for your ZyXEL device and select **Properties**. A properties window displays with basic information about the ZyXEL device.





# Chapter 10

## SNMP

*This chapter discusses the Simple Network Management Protocol.*

### 10.1 About SNMP

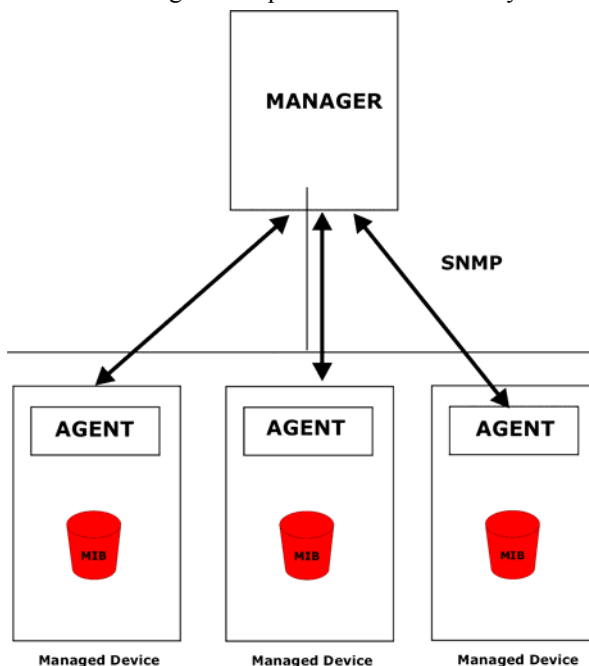
Simple Network Management Protocol is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your ZyWALL supports SNMP agent functionality, which allows a manager station to manage and monitor the ZyWALL through the network. The ZyWALL supports SNMP version one (SNMPv1).

---

**SNMP is only available if TCP/IP is configured.**

---

The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.



**Figure 10-1 SNMP Management Model**

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

An agent is a management software module that resides in a managed device (the ZyWALL). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

**Table 10-1 SNMP Requests/Responses**

<b>SNMP REQUESTS/RESPONSES</b>	<b>DESCRIPTION</b>
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.

## 10.2 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.

## 10.3 SNMP Configuration

From the **MAIN MENU**, click **SNMP** to display the **SNMP** screen shown next. Use this screen to configure the ZyWALL's SNMP settings.

**SNMP**

**SNMP**

Get Community: public

Set Community: public

Trusted Host: 0.0.0.0

Trap Community: public

Trap Destination: 0.0.0.0

Apply      Reset

**Figure 10-2 SNMP Configuration**

The following table describes the SNMP configuration parameters.

**Table 10-2 SNMP Configuration Menu Fields**

FIELD	DESCRIPTION	EXAMPLE
Get Community	Type the Get community, which is the password for the incoming Get- and GetNext requests from the management station.	public
Set Community	Type the Set community, which is the password for incoming Set requests from the management station.	public
Trusted Hosts	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.	0.0.0.0
Trap Community	Type the Trap community, which is the password sent with each trap to the SNMP manager.	trap-comm
Trap Destination	Type the IP address of the station to send your SNMP traps to.	0.0.0.0

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

## 10.4 SNMP Traps

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

**Table 10-3 SNMP Traps**

<b>TRAP #</b>	<b>TRAP NAME</b>	<b>DESCRIPTION</b>
0	coldStart (defined in <i>RFC-1215</i> )	A trap is sent after booting (power on).
1	warmStart (defined in <i>RFC-1215</i> )	A trap is sent after booting (software reboot).
4	authenticationFailure (defined in <i>RFC-1215</i> )	A trap is sent to the manager when receiving any SNMP get or set requirements with 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 (warmstart).
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, CLI 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.



---

---

# Part III:

---

---

## Advanced Management

---

This part covers the Firewall, VPN/IPSec and Logs.



# Chapter 11

## Firewall

*This chapter gives some background information on firewalls and explains how to get started with the ZyWALL firewall.*

### 11.1 Introduction

#### What is a Firewall?

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.

#### The ZyWALL is a Stateful Inspection Firewall.

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

#### About the ZyWALL Firewall

The ZyWALL firewall is a stateful inspection firewall and is designed to protect against Denial of Service attacks when activated (click **LOG SETTINGS** and then click the **Firewall Active** check box). 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 is installed between the LAN and a broadband modem connecting to the Internet. This allows it to act as a secure gateway for all data passing between the Internet and the LAN.

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

- The WAN (Wide Area Network) port attaches to the broadband (cable or DSL) modem to the Internet.

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

### **11.1.1 Guidelines For Enhancing Security With Your Firewall**

- Change the default password via web configurator.
- Think about access control before you connect to the network in any way, including attaching a modem to the port.
- Limit who can access your router.
- 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.
- 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.
- Protect against IP spoofing by making sure the firewall is active.
- Keep the firewall in a secured (locked) room.

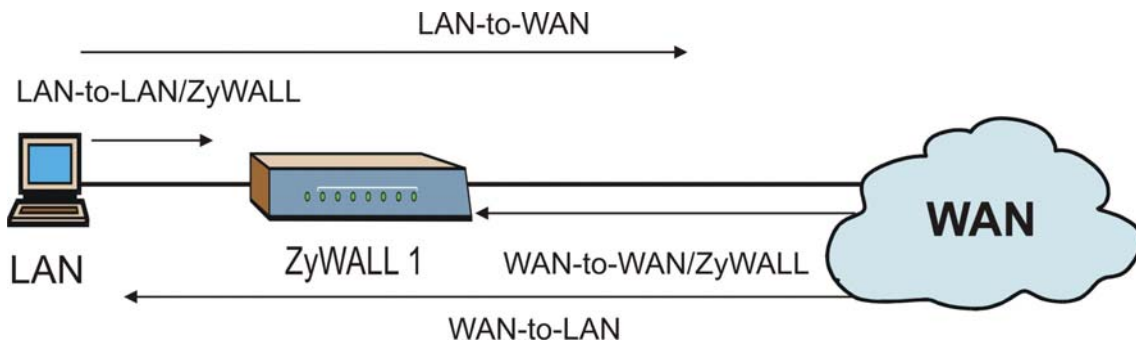
### **11.1.2 Security In General**

You can never be too careful! Factors outside your firewall, filtering or NAT can cause security breaches. Below are some generalizations about what you can do to minimize them.

- Encourage your company or organization to develop a comprehensive security plan. Good network administration takes into account what hackers can do and prepares against attacks. The best defense against hackers and crackers is information. Educate all employees about the importance of security and how to minimize risk. Produce lists like this one!
- DSL or cable modem connections are "always-on" connections and are particularly vulnerable because they provide more opportunities for hackers to crack your system. Turn your computer off when not in use.
- Never give out a password or any sensitive information to an unsolicited telephone call or e-mail.
- Never e-mail sensitive information such as passwords, credit card information, etc., without encrypting the information first.
- Never submit sensitive information via a web page unless the web site uses secure connections. You can identify a secure connection by looking for a small "key" icon on the bottom of your browser (Internet Explorer 3.02 or better or Netscape 3.0 or better). If a web site uses a secure connection, it is safe to submit information. Secure web transactions are quite difficult to crack.

- Never reveal your IP address or other system networking information to people outside your company. Be careful of files e-mailed to you from strangers. One common way of getting BackOrifice on a system is to include it as a Trojan horse with other files.
- Change your passwords regularly. Also, use passwords that are not easy to figure out. The most difficult passwords to crack are those with upper and lower case letters, numbers and a symbol such as % or #.
- Upgrade your software regularly. Many older versions of software, especially web browsers, have well known security deficiencies. When you upgrade to the latest versions, you get the latest patches and fixes.
- If you use "chat rooms" or IRC sessions, be careful with any information you reveal to strangers.
- If your system starts exhibiting odd behavior, contact your ISP. Some hackers will set off hacks that cause your system to slowly become unstable or unusable.
- Always shred confidential information, particularly about your computer, before throwing it away. Some hackers dig through the trash of companies or individuals for information that might help them in an attack.

## 11.2 The Firewall and NAT



**Figure 11-1 Firewall Rule Directions**

### 11.2.1 LAN-to-WAN rules

**LAN-to-WAN** rules are local network to Internet firewall rules. The default is to forward all traffic from your local network to the Internet.

How can you block certain LAN to WAN traffic?

You may choose to block certain **LAN-to-WAN** traffic in the **Services** screen (click the **Services** tab). All services displayed in the **Blocked Services** list box are **LAN-to-WAN** firewall rules that block those services originating from the LAN.

Blocked **LAN-to-WAN** packets trigger alerts. An alert is a report about an event that is immediately e-mailed to the e-mail address you configured in the **Log Settings** screen.

LAN-to-LAN/ZyWALL means the LAN to the ZyWALL LAN interface. This is always allowed, as this is how you manage the ZyWALL from your local computer.

### **11.2.2 WAN-to-LAN rules**

**WAN-to-LAN** rules are Internet to your local network firewall rules. The default is to block all traffic from the Internet to your local network.

How can you forward certain WAN to LAN traffic? You may allow traffic originating from the WAN to be forwarded to the LAN by configuring NAT port forwarding rules in the web configurator **SUA Server** screen.

Forwarded **WAN-to-LAN** packets do not trigger alerts. An alert is a report about an event that is immediately e-mailed to the e-mail address you configured in the **Log Settings** screen.

## **11.3 Firewall Settings**

From the **MAIN MENU**, click **FIREWALL**. The screen shown next is the **Firewall Settings** tab.

**FIREWALL**

Settings   **Filter**   Services

---

**Enable Firewall**  
 Make sure this check box is selected to have the firewall protect your LAN from Denial of Service (DoS) attacks.

1. **LAN to WAN**  
 All traffic originating from the LAN is forwarded unless you block certain services in the Services screen. All blocked LAN-to-WAN packets are considered alerts.  
 Packets to Log:

2. **WAN to LAN**  
 All traffic originating from the WAN is blocked unless you configure port forwarding rules. Forwarded WAN-to-LAN packets are not considered alerts.  
 Packets to Log:

---

A trusted computer has full access to all blocked resources. 0.0.0.0 means there is no trusted computer.  
 Trusted Computer IP Address:

Figure 11-2 Firewall Settings

Table 11-1 Firewall Settings

FIELD	DESCRIPTION
Firewall Active	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.
Log Packets From LAN to WAN	Choose whether to log LAN to WAN packets that match firewall rules that block ( <b>Log Blocked</b> ), forward or block ( <b>Log ALL</b> ) or none ( <b>No Log</b> ).
Log Packets From WAN to LAN	Choose whether to log WAN to LAN packets that match firewall rules that forward ( <b>Log Forwarded</b> ), forward or block ( <b>Log All</b> ), or none ( <b>No Log</b> ).

**Table 11-1 Firewall Settings**

FIELD	DESCRIPTION
Allow one specific computer full access to all blocked resources.	
Trusted Computer	You can allow a specific computer to access all Internet resources without restriction. Enter the IP address of the trusted computer in this field.
Click <b>Apply</b> to save your changes back to the ZyWALL. Click <b>Reset</b> to begin configuring this screen afresh.	

## 11.4 Filter

Click the **Filter** tab. The **Firewall Filter** screen appears as shown next. Use this screen to restrict web features (Active X, Java, Cookies, Web Proxy), enable URL keyword blocking, enter/delete/modify keywords you want to block and the date/time you want to block them.



**CONTENT FILTERING**

**Settings**   **Filter**   **Services**

---

Restrict Web Features    ActiveX    Java    Cookies    Web Proxy

---

Enable URL Keyword Blocking

Keyword

\_\_\_\_\_

Keyword List

|

Add   Delete   Clear All

---

**Date to Block**

Everyday

Sun    Mon    Tue    Wed    Thu    Fri    Sat

**Time of Day to Block (24-Hour Format)**

All day

Start  (hour)  (min)   End  (hour)  (min)

---

Apply   Reset

Figure 11-3 Firewall Filter

Table 11-2 Firewall Filter

FIELD	DESCRIPTION
Restricted Web Features	
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 11-2 Firewall Filter**

<b>FIELD</b>	<b>DESCRIPTION</b>
Cookies	Web servers that track usage and provide service based on ID use cookies.
Web Proxy	This is a server that acts as an intermediary between a user and the Internet to provide security, administrative control, and caching service. When a proxy server is located on the WAN it is possible for LAN users to circumvent content filtering by pointing to this proxy server.
Enable URL Keyword Blocking	Select this option to block the URL containing the keywords in the keyword list.
Keyword	Type a keyword in this field. You may use any character (up to 64 characters). Wildcards are not allowed.
Keyword List	This is a list of keywords that will be inaccessible to computers on your LAN once you enable URL keyword blocking.
Add	Type a keyword in the <b>Keyword</b> field and click then <b>Add</b> to add a keyword to the Keyword List.
Delete	Select a keyword from the <b>Keyword List</b> and then click <b>Delete</b> to remove this keyword from the list.
Clear All	Click <b>Clear All</b> to empty the <b>Keyword List</b> .
Date to Block	Select everyday or the day(s) of the week to activate blocking.
Time of Day to Block	Select <b>All Day</b> or enter the start and end times in the hour-minute format to activate blocking.
Click <b>Apply</b> to save your changes back to the ZyWALL. Click <b>Reset</b> to begin configuring this screen afresh.	

## 11.5 Services

Click the **Services** tab. The screen appears as shown next. Use this screen to enable service blocking, enter/delete/modify the services you want to block and the date/time you want to block them.

**FIREWALL**

**Settings** | **Filter** | **Services**

**Enable Services Blocking**

**Available Services**

- Custom Port...
- Any(TCP)
- Any(UDP)
- IPSEC\_TUNNEL(ESP:0)
- MULTICAST(IGMP:0)
- PING(ICMP:0)
- PPTP\_TUNNEL(GRE:0)
- BGP(TCP:179)

**Blocked Services**

Select "Custom Port", you can give new port range for blocking

Type	Port Number
TCP	0 - 0

Add Delete Clear All

**Day to Block**

Everyday

Sun  Mon  Tue  Wed  Thu  Fri  Sat

**Time of Day to Block (24-Hour Format)**

All day

Start 0 (hour) 0 (min) End 0 (hour) 0 (min)

Apply Reset

Figure 11-4 Firewall Service

Table 11-3 Firewall Service

I ELD	DESCRIPTION
-------	-------------

Table 11-3 Firewall Service

FIELD	DESCRIPTION
Enable Services Blocking	Select this check box to enable this feature.
Available Services	This is a list of pre-defined services (ports) you may prohibit your LAN computers from using. Select the port you want to block using the drop-down list and click <b>Add</b> to add the port to the <b>Blocked Service</b> field.
Blocked Services	This is a list of services (ports) that will be inaccessible to computers on your LAN once you enable service blocking. Choose the IP port ( <b>TCP</b> , <b>UDP</b> or <b>TCP/UDP</b> ) that defines your customized port from the drop down list box.
Custom Port	A custom port is a service that is not available in the pre-defined <b>Available Services</b> list. Use the next two fields to define custom ports.
Type	Services are either <b>TCP</b> and/or <b>UDP</b> . Select from either <b>TCP</b> or <b>UDP</b> .
Port Number	Enter the port number range that defines the service. For example, suppose you want to define the Gnutella service. Select TCP type and enter a port range from 6345-6349.
Add	Select a service from the <b>Available Services</b> drop-down list and then click <b>Add</b> to add the service to the <b>Blocked Services</b> list.
Delete	Select a service from the <b>Blocked Services</b> list and then click <b>Delete</b> to remove this service from the list.
Clear All	Click <b>Clear All</b> to empty the <b>Blocked Services</b> list.
Date to Block	Select everyday or the day(s) of the week to activate blocking.
Time of Day to Block (24-Hour Format)	Select the time of day you want service blocking to take effect. Configure blocking to take effect all day by selecting the <b>All Day</b> check box. You can also configure specific times that by entering the start time in the <b>Start (hr)</b> and <b>Start (min)</b> fields and the end time in the <b>End (hr)</b> and <b>End (min)</b> fields. Enter times in 24-hour format; for example, "3:00pm" should be entered as "15:00".
<p>Click <b>Apply</b> to save your changes back to the ZyWALL.</p> <p>Click <b>Reset</b> to begin configuring this screen afresh.</p>	

# Chapter 12

## VPN/IPSec

### 12.1 Introduction

The ZyWALL allows you to establish one Virtual Private Network (VPN) tunnel from the VPN port to a remote IPSec router. The ZyWALL VPN is based on the IPSec standard and is fully interoperable with other IPSec-based VPN products.

#### 12.1.1 VPN

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 and access control used to transport traffic over the Internet or any insecure network that uses the TCP/IP protocol suite for communication.

#### 12.1.2 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.

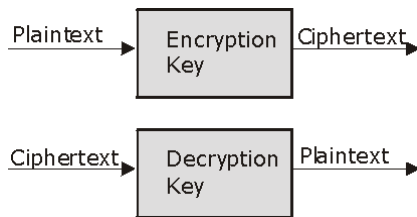
#### 12.1.3 Security Association

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

#### 12.1.4 Other Terminology

##### 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 12-1 Encryption and Decryption**

### **Data Confidentiality**

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

### **Data Integrity**

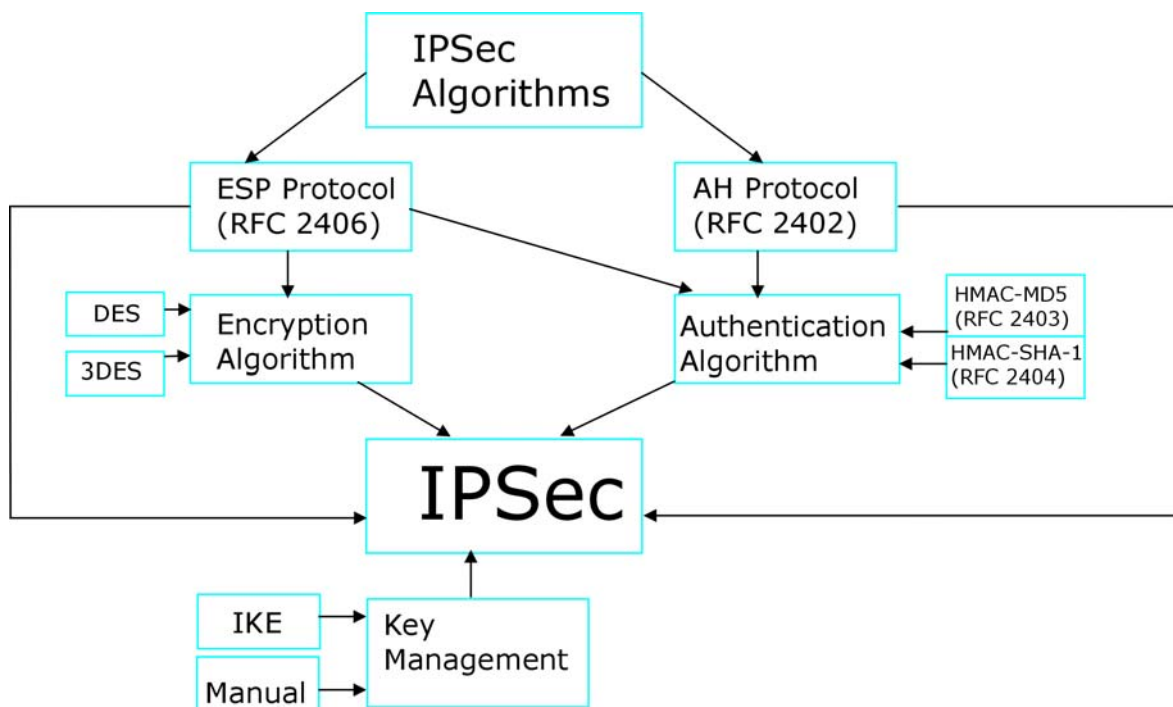
The IPSec receiver can validate packets sent by the IPSec sender to ensure that the data has not been altered during transmission.

### **Data Origin Authentication**

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

## **12.2 IPSec Architecture**

The overall IPSec architecture is shown as follows:



**Figure 12-2 IPsec Architecture**

### 12.2.1 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) 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.

## 12.3 IPsec and NAT

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

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

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

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

Tunnel mode ESP with authentication is compatible with NAT because integrity checks are performed over the combination of the "original header plus original payload," which is unchanged by a NAT device.

**Transport** mode **ESP** with authentication is not compatible with NAT, although NAT traversal provides a way to use **Transport** mode **ESP** when there is a NAT router between the IPSec endpoints (see *section 12.5.1* for details).

**Table 12-1 VPN and NAT**

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

## 12.4 ZyWALL 1 VPN

The ZyWALL provides one VPN connection for a single computer connected to one LAN port.

---

**You may create one IPSec connection in the ZyWALL 1.**

---

## 12.5 VPN/IPSec Screen 1: VPN/IPSec Setup Tab

To access the **VPN/IPSec Setup** screen, click **VPN/IPSec**. This section describes the fields in the **VPN/IPSec Setup** screen. Fields in this screen vary depending on what you select in the **IPSec Keying Mode** field.

### 12.5.1 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 *section 12.8.2* 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.

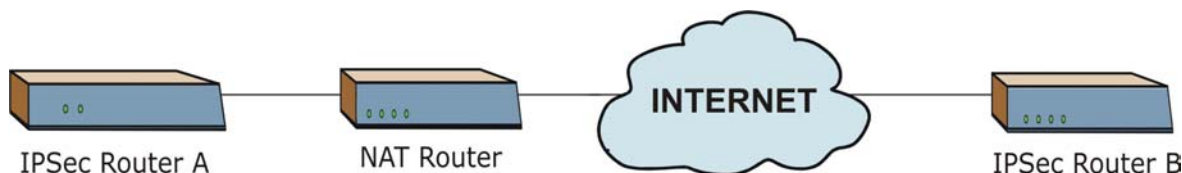
---

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

---

## 12.5.2 NAT Traversal

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



**Figure 12-3 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.

## 12.5.3 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.

## 12.5.4 Negotiation Mode

Select **Main** or **Aggressive** from the drop-down list box. The 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.

Make sure the remote gateway uses the same negotiation mode.

### 12.5.5 ID Type and Content

With aggressive negotiation mode (see *section 12.5.4*), the ZyWALL identifies an incoming SA by ID type and content since this identifying information is not encrypted. This enables remote IPSec routers to distinguish between multiple rules for SAs that connect from that have dynamic WAN IP addresses. Telecommuters that use IPSec routers with dynamic IP addresses can use separate passwords to simultaneously connect to a remote IPSec router.

With main mode (see *section 12.5.4*), the ID type and content are encrypted to provide identity protection. In this case the remote IPSec router can only distinguish between up to eight different incoming SAs that connect from remote IPSec routers that have dynamic WAN IP addresses. The remote IPSec router can distinguish up to eight incoming SAs because you can select between two encryption algorithms (DES and 3DES), two authentication algorithms (MD5 and SHA1) and two key groups (DH1 and DH2) when you configure a VPN rule. 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 12-2 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 <b>Content</b> field is used for identification purposes only and does not need to be a real domain name or e-mail address.	

**Table 12-3 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 <b>Secure Gateway</b> 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.
The domain name or e-mail address that you use in the <b>Content</b> 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 <b>Secure Gateway Address</b> field below.	

### 12.5.6 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 12-4 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 12-5 Mismatching ID Type and Content Configuration Example**

ZYWALL A	ZYWALL B
Local ID type: IP	<b>Local ID type: IP</b>
Local ID content: 1.1.1.10	Local ID content: 1.1.1.10

**Table 12-5 Mismatching ID Type and Content Configuration Example**

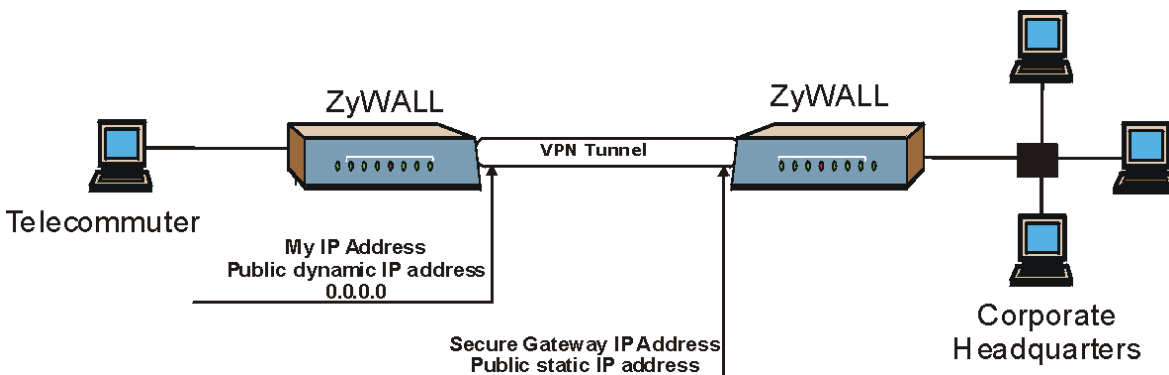
ZYWALL A	ZYWALL B
Peer ID type: E-mail	Peer ID type: IP
Peer ID content: aa@yahoo.com	Peer ID content: N/A

### 12.5.7 Secure Gateway IP Address

**Secure Gateway IP Address** is the WAN IP address of the remote IPSec router. Normally it is a static public IP address (for traffic going through the Internet) but if the peer has a dynamic WAN IP address, set this field to 0.0.0.0. This may be useful for telecommuters initiating a VPN tunnel to headquarters where headquarters does not know the WAN IP address of the telecommuter's device. Only the telecommuter may initiate the VPN tunnel in this case. See the following table for an example configuration.

**Table 12-6 Telecommuter and Headquarters Configuration Example**

	TELECOMMUTER	HEADQUARTERS
My IP address:	0.0.0.0 (dynamic IP address assigned by the ISP)	Public static IP address.
Secure Gateway IP Address:	Public static IP address.	0.0.0.0 With this IP address only the telecommuter can initiate the IPSec tunnel.



**Figure 12-4 Telecommuter's ZyWALL Configuration**

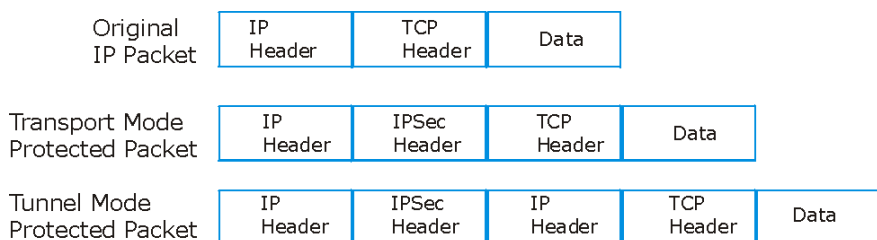
---

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

---

## 12.5.8 Encapsulation Mode

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



**Figure 12-5 Transport and Tunnel Mode IPSec Encapsulation**

### 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.

### 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.

## 12.5.9 IPsec Protocol

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.

### 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.

### 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 12-7 AH AND ESP**

<b>ESP</b>	<b>AH</b>
Select DES for minimal security and 3DES for maximum.	Select MD5 for minimal security and SHA-1 for maximum security.
Data Encryption Standard (DES, the default) is a widely used method of data encryption using a private (secret) key. DES applies a 56-bit key to each 64-bit block of data.	MD5 (Message Digest 5, the default) produces a 128-bit digest to authenticate packet data.
Triple DES (3DES) is a variant of DES, which iterates three times with three separate keys ( $3 \times 56 = 168$ bits), effectively doubling the strength of DES.	SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.

## 12.5.10 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.

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.

### 12.5.11 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. ZyWALL DES encryption algorithm uses a 56-bit key.

Strong Encryption, or 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.

Press the [SPACE BAR] to choose from **3DES** or **DES** and then press [ENTER].

### 12.5.12 Authentication Algorithm

Authentication algorithms offer 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. Choices are MD5 (default - 128 bits) and SHA1 (160 bits).

Using an authentication algorithm and ESP increases the ZyWALL's processing requirements and communications latency (delay).

---

**These fields must contain the same parameters as your secure remote gateway:**

---

<b>Encapsulation Mode</b>	<b>IPSec Protocol</b>	<b>Pre-Shared Key</b>
<b>Encryption Algorithm</b>	<b>Negotiation Mode</b>	<b>Authentication Algorithm</b>

## 12.6 VPN/IPSec Setup: IKE

VPN

Rule Setup **SA Monitor** Global Setting

Active
  Keep Alive

NAT Traversal

IPSec Keying Mode: IKE

Local Address: 0.0.0.0

Remote Address Start: 0.0.0.0

Remote Address End/Mask: 0.0.0.0

My IP Address: 0.0.0.0

Local ID Type: IP

Local Content:

Secure Gateway Address: 0.0.0.0

Peer ID Type: IP

Peer Content:

Encapsulation Mode: Tunnel

IPSec Protocol: ESP

Pre-Shared Key:

Encryption Algorithm: DES

Authentication Algorithm: SHA1

Advanced...

Apply Reset

Figure 12-6 VPN/IPSec Setup: IKE

Table 12-8 VPN/IPSec Setup: IKE

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



**Table 12-8 VPN/IPSec Setup: IKE**

LABEL	DESCRIPTION
Keep Alive	Select this check box 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	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 <b>ESP</b> protocol using <b>Transport</b> or <b>Tunnel</b> mode, but not with <b>AH</b> 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.
IPSec Keying Mode	Select <b>IKE</b> or <b>Manual</b> from the drop-down list box. <b>IKE</b> is the preferred choice as the key is generated automatically; <b>Manual</b> is useful for troubleshooting. Make sure the remote gateway has the same configuration in this field.
Local Address	Enter the IP address of the computer using the VPN IPSec feature of your ZyWALL. Your ZyWALL supports one VPN tunnel and therefore there can be only one local address.
Remote Address Start	Enter the beginning IP address (in a range) of computers on the remote network behind the remote IPSec gateway.
Remote Address End/Mask	Enter the end IP address (in a range) of computers on the remote network behind the remote IPSec gateway.
My IP Address	<b>My IP Address</b> is the ZyWALL's WAN IP address. If this field is configured as 0.0.0.0, then the ZyWALL will use the current ZyWALL WAN IP address (static or dynamic) to set up the VPN tunnel. If the <b>My IP Address</b> changes after setup, then the VPN tunnel will have to be rebuilt.
Local ID Type	Choose from <b>IP</b> , <b>DNS</b> , or <b>E-mail</b> . <ul style="list-style-type: none"> <li>➤ Select <b>IP</b> to identify this ZyWALL by its IP address.</li> <li>➤ Select <b>DNS</b> to identify this ZyWALL by a domain name.</li> <li>➤ Select <b>E-mail</b> to identify this ZyWALL by an e-mail address.</li> </ul>

Table 12-8 VPN/IPSec Setup: IKE

LABEL	DESCRIPTION
Local Content	<p>Don't enter any information in this field when you select <b>IP</b> in the <b>Local ID Type</b> field (the ZyWALL uses the IP address in the <b>My IP Address</b> field).</p> <p>When you select <b>DNS</b> in the <b>Local ID Type</b> field, type a domain name (up to 31 characters) by which to identify this ZyWALL.</p> <p>When you select <b>E-mail</b> in the <b>Local ID Type</b> field, type an e-mail address (up to 31 characters) by which to identify this ZyWALL.</p> <p>The domain name or e-mail address that you use in the <b>Content</b> field is used for identification purposes only and does not need to be a real domain name or e-mail address.</p>
Secure Gateway Address	<p>Type the WAN IP address or the URL (up to 31 characters) of the remote secure gateway with which you're making the VPN connection. Set this field to 0.0.0.0 if the remote secure gateway has a dynamic WAN IP address (the <b>Key Management</b> field must be set to <b>IKE</b>).</p>
Peer ID Type	<p>Choose from <b>IP</b>, <b>DNS</b>, or <b>E-mail</b>.</p> <ul style="list-style-type: none"> <li>➤ Select <b>IP</b> to identify the remote IPSec router by its IP address.</li> <li>➤ Select <b>DNS</b> to identify the remote IPSec router by a domain name.</li> <li>➤ Select <b>E-mail</b> to identify the remote IPSec router by an e-mail address.</li> </ul>
Peer Content	<p>Don't enter any information in this field when you select <b>IP</b> in the <b>Peer ID Type</b> field (the ZyWALL uses the IP address in the <b>Secure Gateway Address</b> field).</p> <p>When you select <b>DNS</b> in the <b>Peer ID Type</b> field, type a domain name (up to 31 characters) by which to identify the remote IPSec router.</p> <p>When you select <b>E-mail</b> in the <b>Peer ID Type</b> field, type an e-mail address (up to 31 characters) by which to identify the remote IPSec router.</p> <p>The domain name or e-mail address that you use in the <b>Content</b> 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 <b>Secure Gateway Address</b> field below.</p>
Encapsulation Mode	<p>Select <b>Tunnel</b> mode or <b>Transport</b> mode from the drop-down list box. The ZyWALL's encapsulation mode should be identical to the secure remote gateway.</p>

Table 12-8 VPN/IPSec Setup: IKE

LABEL	DESCRIPTION
IPSec Protocol	<p>Select <b>ESP</b> or <b>AH</b> from the drop-down list box. The ZyWALL's IPSec Protocol should be identical to the secure remote gateway. The ESP (Encapsulation Security Payload) protocol (RFC 2406) provides encryption as well as the authentication offered by AH. If you select ESP here, you must select options from the Encryption Algorithm and Authentication Algorithm fields (described below). The AH protocol (Authentication Header 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 <b>AH</b> here, you must select options from the <b>Authentication Algorithm</b> field.</p>
Pre-Shared Key	<p>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.</p> <p>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.</p> <p>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.</p>
Encryption Algorithm	<p>Select <b>DES</b> or <b>3DES</b> from the drop-down list box. The ZyWALL's encryption algorithm should be identical to the secure remote gateway. 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. 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.</p>
Authentication Algorithm	<p>Select <b>SHA1</b> or <b>MD5</b> from the drop-down list box. The ZyWALL's authentication algorithm should be identical to the secure remote gateway. MD5 (Message Digest 5) and SHA1 (Secure Hash Algorithm) are hash algorithms used to authenticate the source and integrity of packet data. The SHA1 algorithm is generally considered stronger than MD5, but is slower. Select <b>SHA-1</b> for maximum security.</p>
Advanced	<p>Click <b>Advanced</b> to go to the advanced VPN configuration screen.</p>
<p>Click <b>Apply</b> to save your changes back to the ZyWALL.  Click <b>Reset</b> to begin configuring this screen afresh.</p>	

## 12.7 VPN/IPSec Setup: Manual

When you select **Manual** in the **IPSec Keying Mode** field the following screen appears. **IKE** is the preferred choice as the key is generated automatically; **Manual** is useful for troubleshooting.

VPN

Rule Setup SA Monitor Global Setting

Active

IPSec Keying Mode Manual

Protocol Number 0

Local Address 0.0.0.0

Local Port Start 0

Local Port End 0

Remote Address Start 0.0.0.0

Remote Address End/Mask 0.0.0.0

Remote Port Start 0

Remote Port End 0

My IP Address 0.0.0.0

Secure Gateway IP Address 0.0.0.0

SPI 0

Encapsulation Mode Transport

Enable Replay Detection No

IPSec Protocol ESP

Encryption Algorithm DES

Encryption Key

Authentication Algorithm SHA1

Authentication Key

Apply Reset

Figure 12-7 VPN/IPSec Setup: Manual

**Table 12-9 VPN/IPSec Setup: Manual**

FIELD	DESCRIPTION
Active	Select this check box to activate this VPN policy.
IPSec Keying Mode	Select <b>IKE</b> or <b>Manual</b> from the drop-down list box. <b>Manual</b> is a useful option for troubleshooting if you have problems using IKE key management.
Protocol Number	Enter 1 for ICMP, 6 for TCP, 17 for UDP, etc. 0 is the default and signifies any protocol.
Local Address	This is the IP address of the computer for which you are configuring the VPN connection (the VPN host computer). This IP address must correspond to the remote secure gateway's configured remote IP address in order for the remote secure gateway to initiate the VPN connection. Enter an IP address on the LAN behind your ZyWALL; 0.0.0.0 is a dynamic IP address.
Local 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
Local Port 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 (or equal to it for configuring an individual port).
Remote Address Start	Enter the beginning (static) IP address, in a range of computers behind your remote secure gateway. This address should be specific to the remote computer using the VPN tunnel. If you wish to configure the tunnel for a single IP address, enter it in this field and again in the <b>Remote Address End/Mask</b> field.
Remote Address End/Mask	Enter the end (static) IP address, in a range of computers on behind your remote secure gateway. This address should be specific to the remote computer using the VPN tunnel. If you wish to configure the tunnel for a single IP address, enter it in both the <b>Remote Address Start</b> field and here.

**Table 12-9 VPN/IPSec Setup: Manual**

FIELD	DESCRIPTION
Remote 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
Remote Port 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 (or equal to it for configuring an individual port).
My IP Address	Enter the WAN IP address of your ZyWALL. The ZyWALL uses its current WAN IP address (static or dynamic) in setting up the VPN tunnel if you leave this field as 0.0.0.0. The VPN tunnel has to be rebuilt if this IP address changes.
Secure Gateway IP 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.
SPI	Type a unique SPI from one to four characters long. Valid Characters are "0, 1, 2, 3, 4, 5, 6, 7, 8, and 9".
Encapsulation Mode	Select <b>Tunnel</b> mode or <b>Transport</b> mode from the drop-down list box.
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 <b>Yes</b> . Choose <b>Yes</b> from the drop-down list box to enable replay detection.
IPSec Protocol	Select <b>ESP</b> or <b>AH</b> from the drop-down list box. The ZyWALL's IPSec Protocol should be identical to the secure remote gateway. The ESP (Encapsulation Security Payload) protocol (RFC 2406) provides encryption as well as the authentication offered by AH. If you select ESP here, you must select options from the Encryption Algorithm and Authentication Algorithm fields (described below). The AH protocol (Authentication Header 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 <b>AH</b> here, you must select options from the <b>Authentication Algorithm</b> field.

**Table 12-9 VPN/IPSec Setup: Manual**

FIELD	DESCRIPTION
Encryption Algorithm	<p>Select <b>DES</b> or <b>3DES</b> from the drop-down list box.</p> <p>When <b>DES</b> 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 <b>DES</b> encryption algorithm uses a 56-bit key.</p> <p>Triple DES (<b>3DES</b>) is a variation on DES that uses a 168-bit key. As a result, <b>3DES</b> is more secure than DES. It also requires more processing power, resulting in increased latency and decreased throughput.</p>
Encryption Key (only with ESP)	<p>With <b>DES</b>, type a unique key 8 characters long. With <b>3DES</b>, type a unique key 24 characters long. Any characters may be used, including spaces, but trailing spaces are truncated.</p>
Authentication Algorithm	<p>Select <b>SHA1</b> or <b>MD5</b> from the drop-down list box. <b>MD5</b> (Message Digest 5) and <b>SHA1</b> (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The <b>SHA1</b> algorithm is generally considered stronger than <b>MD5</b>, but is slower. Select <b>MD5</b> for minimal security and <b>SHA1</b> for maximum security.</p>
Authentication Key	<p>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.</p>
<p>Click <b>Apply</b> to save your changes back to the ZyWALL.</p> <p>Click <b>Reset</b> to begin configuring this screen afresh.</p>	

## 12.8 Advanced VPN Setup

Advanced VPN setup distinguishes between the two phases of IKE negotiation as discussed next.

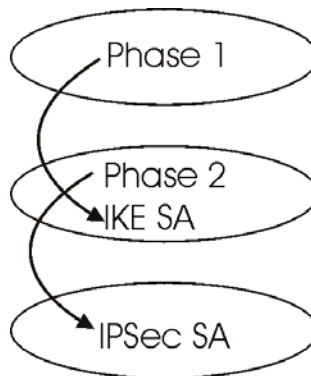
---

**This screen is for advanced VPN setup using IKE only.**

---

### 12.8.1 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 12-8 Two Phases to set up the IPsec SA**

In phase 1 you must:

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

In phase 2 you must:

- Choose which protocol to use (**ESP** or **AH**) for the IKE key exchange.
- Choose an encryption algorithm.
- Choose an authentication algorithm
- Choose whether to enable Perfect Forward Secrecy (PFS) using Diffie-Hellman public-key cryptography – see *section 12.8.4*. 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.

The ZyWALL checks IKE configuration compatibility against its peer (secure remote gateway). If the configuration is incompatible, for example the ZyWALL and its peer have different algorithms, the

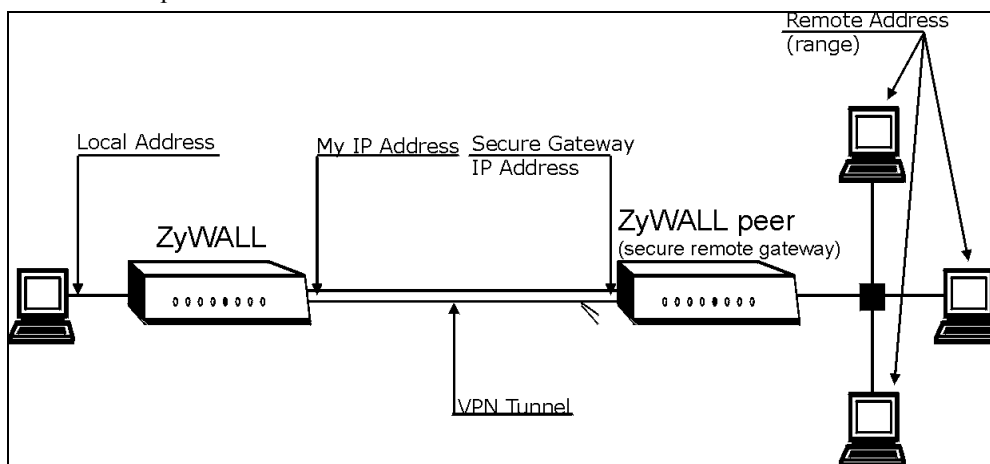


ZyWALL will reject the connection and record the rejection as a VPN log. The following table shows how fields in this screen need to be configured in relation to the secure remote gateway in order to achieve a successful connection.

**Table 12-10 The ZyWALL and the Secure Remote Gateway: IKE Fields**

FIELD	CONFIGURATION
IPSec Protocol	Identical to the secure remote gateway
Encryption/Authentication Algorithm	Identical to the secure remote gateway
Encapsulation Mode	Identical to the secure remote gateway
Negotiation Mode	Identical to the secure remote gateway
Pre-Shared Key	Identical to the secure remote gateway
Local Address	Specific to the local computer using the VPN tunnel
Remote Address Start	Specific to the remote computer using the VPN tunnel
Remote Address End	Specific to the remote computer using the VPN tunnel
My IP Address	Specific to the ZyWALL IP address
Secure Gateway IP Address	Specific to the secure remote gateway IP address.
SA Life Time	May be different than the secure remote gateway

The following figure shows the ZyWALL and its peer (secure remote gateway) relative to some of the IKE fields described in the previous table



**Figure 12-9 The ZyWALL, the Secure Remote Gateway and IKE Fields**

## 12.8.2 SA Life Time

Define the length of time before an IKE SA automatically renegotiates in this field. It may range from 60 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.

## 12.8.3 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.

## 12.8.4 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).

## 12.8.5 Advanced VPN Extra Configuration Fields

These are the extra fields you need to configure if you choose advanced VPN setup (Options >>).

**Table 12-11 Advanced VPN Extra Configuration Fields**

Keep Alive
Local ID Type
Local Content
Peer ID Type
Peer Content
IKE Phase 1 SA Life Time
IKE Phase 1 Key Group
IKE Phase 1 Encryption Algorithm

**Table 12-11 Advanced VPN Extra Configuration Fields**

IKE Phase 1 Authentication Algorithm
IKE Phase 2 SA Life Time
IKE Phase 2 Perfect Forward Secrecy (PFS)

To access the **Advanced VPN/IPSec Configuration** screen, click **VPN/IPSec**, make sure the **IPSec Keying Mode** field is set to **IKE** and then select the **Options >>** checkbox. The screen appears as shown next.

VPN

Rule Setup **SA Monitor** Global Setting

Active
  Keep Alive

NAT Traversal

IPSec Keying Mode: IKE

Protocol Number: 0

Enable Replay Detection: No

---

Local Address: 0.0.0.0

Local Port Start: 0

Local Port End: 0

---

Remote Address Start: 0.0.0.0

Remote Address End/Mask: 0.0.0.0

Remote Port Start: 0

Remote Port End: 0

---

My IP Address: 0.0.0.0

Local ID Type: IP

Local Content:

Secure Gateway Address: 0.0.0.0

Peer ID Type: IP

Peer Content:

---

**IKE Phase 1:**

Negotiation Mode: Main

Encryption Algorithm: DES

Authentication Algorithm: MD5

SA Life Time: 28800

Key Group: DH1

Pre-Shared Key:

---

**IKE Phase 2:**

Encapsulation Mode: Tunnel

IPSec Protocol: ESP

Encryption Algorithm: DES

Authentication Algorithm: SHA1

SA Life Time: 28800

Perfect Forward Secrecy(PFS): None

Basic...

Figure 12-10 Advanced VPN/IPSec Configuration

**Table 12-12 Advanced VPN/IPSec Configuration**

LABEL	DESCRIPTION
Active	Select this check box to activate this VPN/IPSec policy.
Keep Alive	Select this check box 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 Transversal	<p>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.</p> <p>You can use NAT traversal with <b>ESP</b> protocol using <b>Transport</b> or <b>Tunnel</b> mode, but not with <b>AH</b> 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.</p>
IPSec Keying Mode	You can only configure advanced VPN/IPSec settings with <b>IKE</b> key management, thus <b>Manual</b> is not available in this screen.
Protocol Number	Enter 1 for ICMP, 6 for TCP, 17 for UDP, etc. 0 is the default and signifies any protocol.
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 <b>Yes</b> .
Local Address	<p>This is the IP address of the computer for which you are configuring the VPN connection (the VPN host computer). This IP address must correspond to the remote secure gateway's configured remote IP address in order for the remote secure gateway to initiate the VPN connection.</p> <p>Enter an IP address on the LAN behind your ZyWALL; 0.0.0.0 is a dynamic IP address.</p>
Local 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; and 110, POP3.
Local Port 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 (or equal to it for configuring an individual port).

Table 12-12 Advanced VPN/IPSec Configuration

LABEL	DESCRIPTION
Remote Address Start	Enter the beginning (static) IP address, in a range of computers behind the remote secure gateway. This address should be specific to the remote computer using the VPN tunnel. If you wish to configure the tunnel for a single IP address, enter it in this field and again in the <b>Remote Address End/Mask</b> field.
Remote Address End/Mask	Enter the end (static) IP address, in a range of computers behind the remote secure gateway. This address should be specific to the remote computer using the VPN tunnel. If you wish to configure the tunnel for a single IP address, enter it in both the <b>Remote Address Start</b> field and here.
Remote 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; and 110, POP3.
Remote Port 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 (or equal to it for configuring an individual port).
My IP Address	Enter the WAN IP address of your ZyWALL. The ZyWALL uses its current WAN IP address (static or dynamic) in setting up the VPN tunnel if you leave this field as 0.0.0.0. The VPN tunnel has to be rebuilt if this IP address changes.
Local ID Type	<p>Choose from <b>IP</b>, <b>DNS</b>, or <b>E-mail</b>.</p> <ul style="list-style-type: none"> <li>➤ Select <b>IP</b> to identify this ZyWALL by its IP address.</li> <li>➤ Select <b>DNS</b> to identify this ZyWALL by a domain name.</li> <li>➤ Select <b>E-mail</b> to identify this ZyWALL by an e-mail address.</li> </ul>
Local Content	<p>Don't enter any information in this field when you select <b>IP</b> in the <b>Local ID Type</b> field (the ZyWALL uses the IP address in the <b>My IP Address</b> field).</p> <p>When you select <b>DNS</b> in the <b>Local ID Type</b> field, type a domain name (up to 31 characters) by which to identify this ZyWALL.</p> <p>When you select <b>E-mail</b> in the <b>Local ID Type</b> field, type an e-mail address (up to 31 characters) by which to identify this ZyWALL.</p> <p>The domain name or e-mail address that you use in the <b>Content</b> field is used for identification purposes only and does not need to be a real domain name or e-mail address.</p>

**Table 12-12 Advanced VPN/IPSec Configuration**

LABEL	DESCRIPTION
Secure Gateway Address	Type the WAN IP address or the URL (up to 31 characters) of the remote secure gateway with which you're making the VPN connection. Set this field to 0.0.0.0 if the remote secure gateway has a dynamic WAN IP address (the <b>Key Management</b> field must be set to <b>IKE</b> ).
Peer ID Type	Choose from <b>IP</b> , <b>DNS</b> , or <b>E-mail</b> . <ul style="list-style-type: none"> <li>➤ Select <b>IP</b> to identify the remote IPSec router by its IP address.</li> <li>➤ Select <b>DNS</b> to identify the remote IPSec router by a domain name.</li> <li>➤ Select <b>E-mail</b> to identify the remote IPSec router by an e-mail address.</li> </ul>
Peer Content	Don't enter any information in this field when you select <b>IP</b> in the <b>Peer ID Type</b> field (the ZyWALL uses the IP address in the <b>Secure Gateway Address</b> field). When you select <b>DNS</b> in the <b>Peer ID Type</b> field, type a domain name (up to 31 characters) by which to identify the remote IPSec router. When you select <b>E-mail</b> in the <b>Peer ID Type</b> field, type an e-mail address (up to 31 characters) by which to identify the remote IPSec router. The domain name or e-mail address that you use in the <b>Content</b> 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 <b>Secure Gateway Address</b> field below.
IKE Phase 1	A phase 1 exchange establishes an IKE SA (Security Association).
Negotiation Mode	Select <b>Main</b> or <b>Aggressive</b> from the drop-down list box. The ZyWALL's negotiation mode should be identical to that on the remote secure gateway.
Encryption Algorithm	Select <b>DES</b> or <b>3DES</b> from the drop-down list box. The ZyWALL's encryption algorithm should be identical to the remote secure gateway. 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. 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.
Authentication Algorithm	Select <b>SHA1</b> or <b>MD5</b> from the drop-down list box. The ZyWALL's authentication algorithm should be identical to the remote secure gateway. MD5 (Message Digest 5) and SHA1 (Secure Hash Algorithm) are hash algorithms used to authenticate the source and integrity of packet data. The SHA1 algorithm is generally considered stronger than MD5, but is slower. Select <b>SHA-1</b> for maximum security.

**Table 12-12 Advanced VPN/IPSec Configuration**

LABEL	DESCRIPTION
SA Life Time	Define the length of time before an IKE SA automatically renegotiates in this field. It may range from 60 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.
Pre-Shared Key	<p>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.</p> <p>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.</p> <p>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.</p>
IKE Phase 2	A phase 2 exchange uses the IKE SA established in phase 1 to negotiate the SA for IPSec.
Encapsulation Mode	Select <b>Tunnel</b> mode or <b>Transport</b> mode from the drop down list-box. The ZyWALL's encapsulation mode should be identical to the remote secure gateway.
IPSec Protocol	Select <b>ESP</b> or <b>AH</b> from the drop-down list box. The ZyWALL's IPSec Protocol should be identical to the remote secure gateway. The ESP (Encapsulation Security Payload) protocol (RFC 2406) provides encryption as well as the authentication offered by AH. If you select ESP here, you must select options from the Encryption Algorithm and Authentication Algorithm fields (described below). The AH protocol (Authentication Header 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 <b>AH</b> here, you must select options from the <b>Authentication Algorithm</b> field.



**Table 12-12 Advanced VPN/IPSec Configuration**

LABEL	DESCRIPTION
Encryption Algorithm	The encryption algorithm for the ZyWALL and the secure remote gateway should be identical. When <b>DES</b> 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. The DES encryption algorithm uses a 56-bit key. Triple DES ( <b>3DES</b> ) 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.
Authentication Algorithm	Select <b>SHA1</b> or <b>MD5</b> 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	Define the length of time before an IKE SA automatically renegotiates in this field. It may range from 60 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.
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 from DH1 or DH2 to enable PFS. <b>DH1</b> 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).
Basic	Click <b>Basic</b> to go to the previous VPN configuration screen.
<p>To save your changes, click <b>Apply</b>.</p> <p>To begin configuring this screen afresh, click <b>Reset</b>.</p>	

## 12.9 The VPN/IPSec Screen: SA Monitor Tab

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.

When there is outbound traffic but no inbound traffic, the SA times out automatically after two minutes. A tunnel with no outbound or inbound traffic is "idle" and does not timeout until the SA lifetime period expires. See *section 12.5.1* on keep alive to have the ZyWALL renegotiate an IPsec SA when the SA lifetime expires, even if there is no traffic.

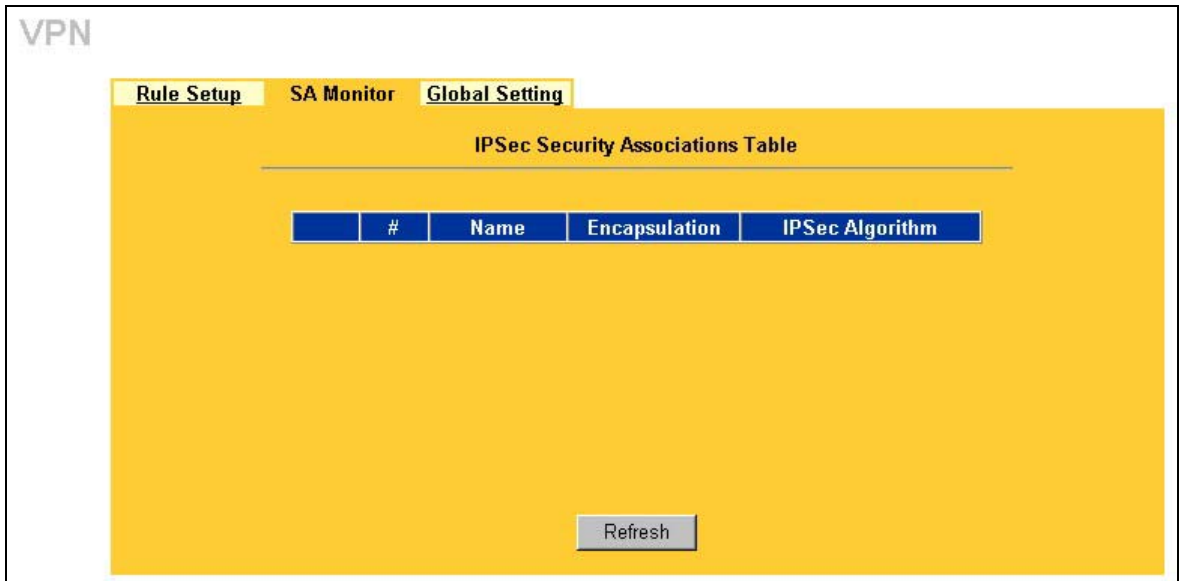


Figure 12-11 SA Monitor

Table 12-13 SA Monitor Tab Fields

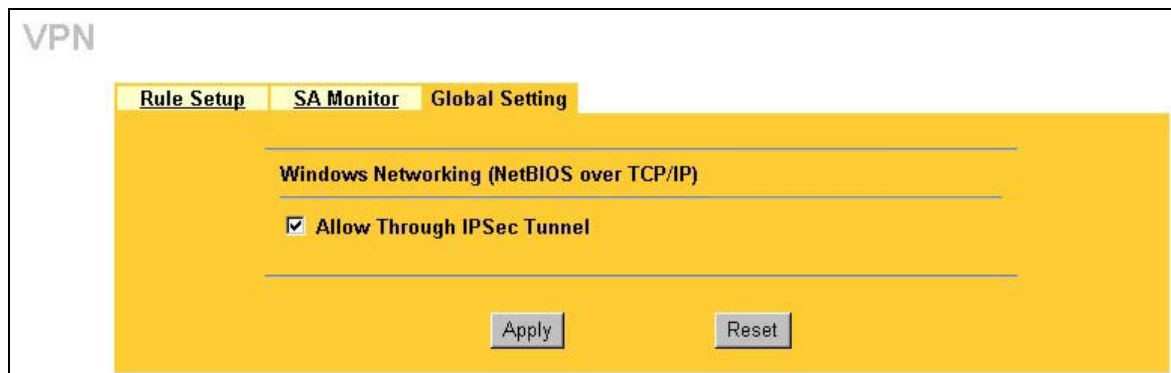
FIELD	DESCRIPTION	EXAMPLE
#	This is the security association index number.	
Name	This field displays the identification name for this VPN policy.	Taiwan
Encapsulation	This field displays <b>Tunnel</b> mode or <b>Transport</b> mode. See previous for discussion.	Tunnel

**Table 12-13 SA Monitor Tab Fields**

FIELD	DESCRIPTION	EXAMPLE
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 and 168-bit 3DES. 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 SHA1 (160 bits).	ESP DES MD5
Refresh	Click <b>Refresh</b> to display the current active VPN connection(s).	

## 12.10 Configuring Global Setting

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

**Figure 12-12 Global Setting**

The following table describes the fields in this screen.

**Table 12-14 SA Monitor**

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.

**Table 12-14 SA Monitor**

LABEL	DESCRIPTION
Allow Through IP/Sec Tunnel	Select this check box to send NetBIOS packets through the VPN connection.
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

# Chapter 13

## Centralized Logs

*This chapter contains information about configuring general log settings and viewing the ZyWALL's logs. Refer to the appendices for example log message explanations.*

### 13.1 View Log

The web configurator allows you to look at all of the ZyWALL's logs in one location.

Click the **LOGS** in the navigation panel to open the **View Log** screen.

Use the **View Log** screen to see the logs for the categories that you selected in the **Log Settings** screen (see *section 13.2*). 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.

View Log

View Log **Log Settings**

Display: All Logs

#	Time ▲	Message	Source	Destination	Notes
1	01/01/2000 02:56:16	Firewall default policy: IGMP (set:8)	0.0.0.0	224.0.0.12	ACCESS BLOCK
2	01/01/2000 02:56:16	Firewall default policy: IGMP (set:8)	0.0.0.0	224.0.0.1	ACCESS BLOCK
3	01/01/2000 02:56:16	Firewall default policy: UDP(set:8)	172.21.4.17:137	172.21.255.255:137	ACCESS BLOCK
4	01/01/2000 02:56:16	Firewall default policy: IGMP (set:8)	172.21.10.8	224.0.0.9	ACCESS BLOCK
5	01/01/2000 02:56:15	Firewall default policy: IGMP (set:8)	172.21.0.2	224.0.1.22	ACCESS BLOCK
6	01/01/2000 02:56:15	Firewall default policy: UDP(set:8)	172.21.4.17:137	172.21.255.255:137	ACCESS BLOCK
7	01/01/2000 02:56:15	Firewall default policy: ICMP (type:10, code:0)	172.21.4.17	224.0.0.2	ACCESS BLOCK
8	01/01/2000 02:56:15	Firewall default policy: UDP(set:8)	172.21.4.17:137	172.21.255.255:137	ACCESS BLOCK
9	01/01/2000 02:56:15	Firewall default policy: UDP(set:8)	172.21.4.17:137	172.21.255.255:137	ACCESS BLOCK
10	01/01/2000 02:56:15	Firewall default policy: UDP(set:8)	172.21.4.17:137	172.21.255.255:137	ACCESS BLOCK
11	01/01/2000 02:56:15	Firewall default policy: UDP(set:8)	172.21.4.17:137	172.21.255.255:137	ACCESS BLOCK

Figure 13-1 View Log

Table 13-1 View Log

FIELD	DESCRIPTION
Display	The categories that you select in the <b>Log Settings</b> page (see <i>section 13.2</i> ) display in the drop-down list box. Select a category of logs to view; select <b>All Logs</b> to view logs from all of the log categories that you selected in the <b>Log Settings</b> page.
Time	This field displays the time the log was recorded. See the chapter on system maintenance and information 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.

**Table 13-1 View Log**

FIELD	DESCRIPTION
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 <b>Email Log Now</b> to send the log screen to the e-mail address specified in the <b>Log Settings</b> page (make sure that you have first filled in the <b>Address Info</b> fields in <b>Log Settings</b> , see <i>section 13.2</i> ).
Refresh	Click <b>Refresh</b> to renew the log screen.
Clear Log	Click <b>Clear Log</b> to delete all the logs.

## 13.2 Log Settings

You can configure the ZyWALL's general log settings in one location.

Click the **LOGS** in the navigation panel and then the **Log Settings** tab to open the **Log Settings** screen.

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.

## LOGS

View Log
Log Settings

---

**Address Info:**

**Mail Server:**

**Mail Subject**

**Send log to:**

**Send alerts to:**

(Outgoing SMTP Server Name or IP Address)

(E-Mail Address)

(E-Mail Address)

---

**UNIX Syslog:**

Active

**Syslog IP Address:**

**Log Facility:**

(Server Name or IP Address)

---

**Send Log:**

**Log Schedule:**

**Day for Sending Log:**

**Time for Sending Log:**  (hour):  (minute)

---

Log	Send immediate alert
<input checked="" type="checkbox"/> System Maintenance	<input type="checkbox"/> System Errors
<input checked="" type="checkbox"/> System Errors	<input type="checkbox"/> Access Control
<input checked="" type="checkbox"/> Access Control	<input type="checkbox"/> Blocked Web Sites
<input checked="" type="checkbox"/> UPnP	<input type="checkbox"/> Blocked Java etc.
<input checked="" type="checkbox"/> Forward Web Sites	<input type="checkbox"/> Attacks
<input checked="" type="checkbox"/> Blocked Web Sites	<input type="checkbox"/> IPSec
<input checked="" type="checkbox"/> Blocked Java etc.	<input type="checkbox"/> IKE
<input checked="" type="checkbox"/> Attacks	
<input checked="" type="checkbox"/> IPSec	
<input checked="" type="checkbox"/> IKE	

---

Figure 13-2 Log Settings



Table 13-2 Log Settings

FIELD	DESCRIPTION
Address Info	
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.
Send Log To	The ZyWALL sends logs to the e-mail address specified in this field. If this field is left blank, the ZyWALL does not send logs via e-mail.
Send Alerts To	Alerts are real-time notifications that are sent as soon as an event, such as a DoS attack, system error, or forbidden web access attempt occurs. Enter the e-mail address where the alert messages will be sent. Alerts include system errors, attacks and attempted access to blocked web sites. If this field is left blank, alert messages will not be sent via e-mail.
UNIX Syslog	UNIX syslog sends a log to an external UNIX server used to store logs.
Active	Click <b>Active</b> to enable UNIX syslog.
Syslog IP Address	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 your UNIX manual for more information.
Send Log	
Log Schedule	<p>This drop-down menu is used to configure the frequency of log messages being sent as E-mail:</p> <ul style="list-style-type: none"> <li>• <b>Daily</b></li> <li>• <b>Weekly</b></li> <li>• <b>Hourly</b></li> <li>• <b>When the Log is Full</b></li> <li>• <b>None.</b></li> </ul> <p>If you select <b>Weekly</b> or <b>Daily</b>, specify a time of day when the E-mail should be sent. If you select <b>Weekly</b>, then also specify which day of the week the E-mail should be sent. If you select <b>When Log is Full</b>, an alert is sent when the log fills up. If you select <b>None</b>, no log messages are sent</p>

**Table 13-2 Log Settings**

FIELD	DESCRIPTION
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.
Log	Select the categories of logs that you want to record.
Send Immediate Alert	Select log categories for which you want the ZyWALL to send e-mail alerts immediately.
To save your changes, click <b>Apply</b> . To begin configuring this screen afresh, click <b>Reset</b> .	

---

---

# Part IV:

---

---

## Maintenance

---

This part covers the maintenance web configurator screens and troubleshooting.



# Chapter 14

## Maintenance

*This chapter displays system information such as ZyNOS firmware, port IP addresses and port traffic statistics.*

### 14.1 Maintenance Overview

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

### 14.2 Status Screen

Click **MAINTENANCE** to open the **Status** screen, where you can use to monitor your ZyWALL. Note that these fields are READ-ONLY and meant to be used for diagnostic purposes.

**MAINTENANCE**

[Status](#)
[DHCP Table](#)
[F/W Upload](#)
[Configuration](#)

System Name :

ZyNOS Firmware Version: V3.60(WD.0)b5 | 02/25/2003  
Routing Protocols : IP

WAN Port :

IP Address : 0.0.0.0                      DHCP : None  
IP Subnet Mask : 0.0.0.0

LAN Port :

IP Address : 192.168.1.1                      DHCP : Server  
IP Subnet Mask : 255.255.255.0

Show Statistics

**Figure 14-1 System Status**

The following table describes the fields in this screen.

**Table 14-1 System Status**

LABEL	DESCRIPTION
System Name	This is the <b>System Name</b> you chose in the first Internet Access Wizard screen. It is for identification purposes
ZyNOS Firmware Version:	This is the ZyNOS Firmware version and the date created. ZyNOS is ZyXEL's proprietary Network Operating System design.
Routing Protocols	This shows the routing protocol - <b>IP</b> for which the ZyWALL is configured. This field is not configurable in all ZyWALL router models.
WAN Port	
IP Address	This is the WAN port IP address.
IP Subnet Mask	This is the WAN port subnet mask.
DHCP	This is the WAN port DHCP role - <b>Client</b> or <b>None</b> .
LAN Port	
IP Address	This is the LAN port IP address.
IP Subnet Mask	This is the LAN port subnet mask.
DHCP	This is the LAN port DHCP role - <b>Server</b> , <b>Relay</b> (not all ZyWALL models) or <b>None</b> .
Show Statistics	Click <b>Show Statistics</b> to see router performance statistics such as number of packets sent and number of packets received for each port.

### 14.2.1 System Statistics

Read-only information here includes port status and packet specific statistics. Also provided are "system up time" and "poll interval(s)". The **Poll Interval(s)** field is configurable.

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	Down	0	0	0	0	0	00:00:00
LAN	100M/Full	1522	1625	0	5729	979	0:12:45

System Up Time : 0:12:51

Poll Interval(s) :

**Figure 14-2 System Status: Show Statistics**

The following table describes the fields in this screen.

**Table 14-2 System Status: Show Statistics**

LABEL	DESCRIPTION
Port	This is the WAN or LAN port.
Status	This displays the port speed and duplex setting if you're using Ethernet encapsulation and <b>down</b> (line is down), <b>idle</b> (line (ppp) idle), <b>dial</b> (starting to trigger a call) and <b>drop</b> (dropping a call) if you're using PPPoE encapsulation.
TxPkts	This is the number of transmitted packets on this port.
RxPkts	This is the number of received packets on this port.
Collisions	This is the number of collisions on this port.
Tx B/s	This displays the transmission speed in bytes per second on this port.
Rx B/s	This displays the reception speed in bytes per second on this port.
Up Time	This is the total amount of time the line has been up.
System Up Time	This is the total time the ZyWALL has been on.
Poll Interval(s)	Enter the time interval for refreshing statistics in this field.
Set Interval	Click this button to apply the new poll interval you entered in the <b>Poll Interval(s)</b> field.

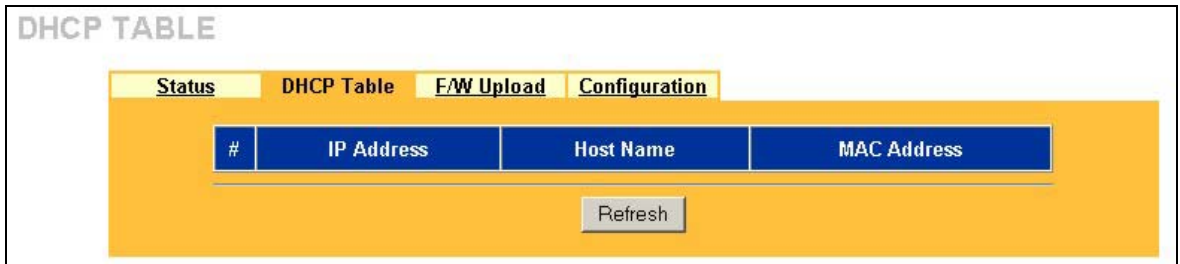
**Table 14-2 System Status: Show Statistics**

LABEL	DESCRIPTION
Stop	Click <b>Stop</b> to stop refreshing statistics, click <b>Stop</b> .

## 14.3 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 set to **None**, DHCP service will be disabled and you must have another DHCP server on your LAN, or else the computer must be manually configured.

Click **MAINTENANCE**, and then the **DHCP Table** tab. 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 DHCP server.

**Figure 14-3 DHCP Table**

The following table describes the fields in this screen.

**Table 14-3 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.



Table 14-3 DHCP Table

LABEL	DESCRIPTION
MAC Address	This field shows the MAC address of the computer with the name in the <b>Host Name</b> field.  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 digits, for example, 00:A0:C5:00:00:02.
Refresh	Click <b>Refresh</b> to renew the screen.

## 14.4 F/W Upload Screen

Find firmware at [www.zyxel.com](http://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 FTP (File Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot. See *Chapter 15* 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. Hierarchy

**FIRMWARE UPLOAD**

Status
DHCP Table
F/W Upload
Configuration

---

**To upgrade the internal router firmware, browse to the location of the binary (.BIN) upgrade file and click Upload. Upgrade files can be downloaded from website. If the upgrade file is compressed (.ZIP file), you must first extract the binary (.BIN) file. In some cases, you may need to reconfigure the router after upgrading.**

File Path:  Browse...

Upload

Figure 14-4 Firmware Upgrade

The following table describes the fields in this screen.

**Figure 14-5 Firmware Upgrade**

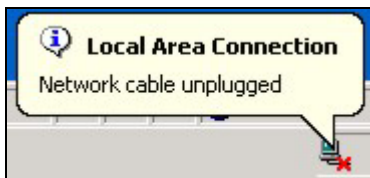
LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click <b>Browse ...</b> to find it.
Browse...	Click <b>Browse...</b> to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click <b>Upload</b> to begin the upload process. This process may take up to two minutes.

**Do not turn off the device while firmware upload is in progress!**

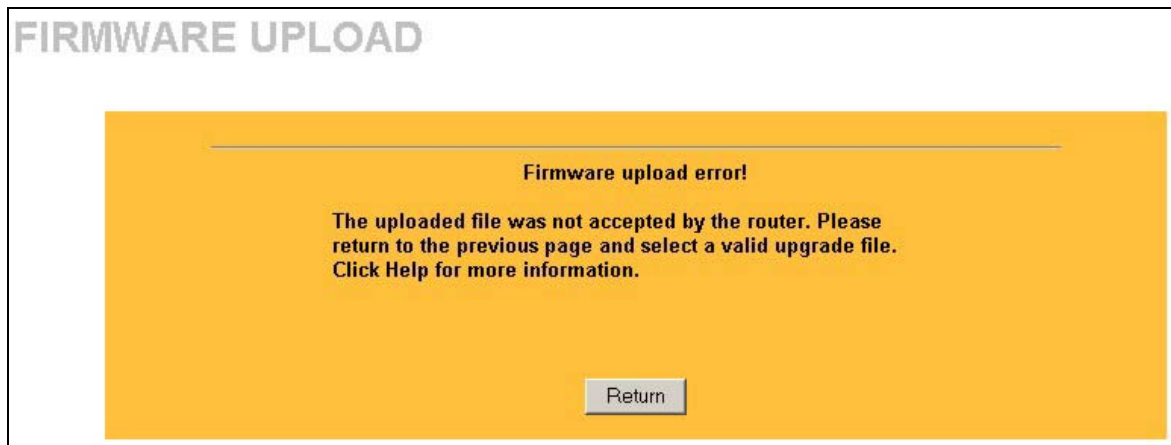
After you see the **Firmware Upload in Process** screen, wait two minutes before logging into the device again.

**Figure 14-6 Firmware Upload In Process**

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

**Figure 14-7 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 14-8 Firmware Upload Error**

## 14.5 Configuration Screen

The web configurator uses TFTP to transfer files. See *Chapter 15* for transferring configuration files using FTP/TFTP commands.

Click **MAINTENANCE**, and then the **Configuration** tab to open the **Configuration** screen as shown next. The following sections provide information related to restoring factory defaults, backing up configuration, restoring configuration and restarting the ZyWALL.

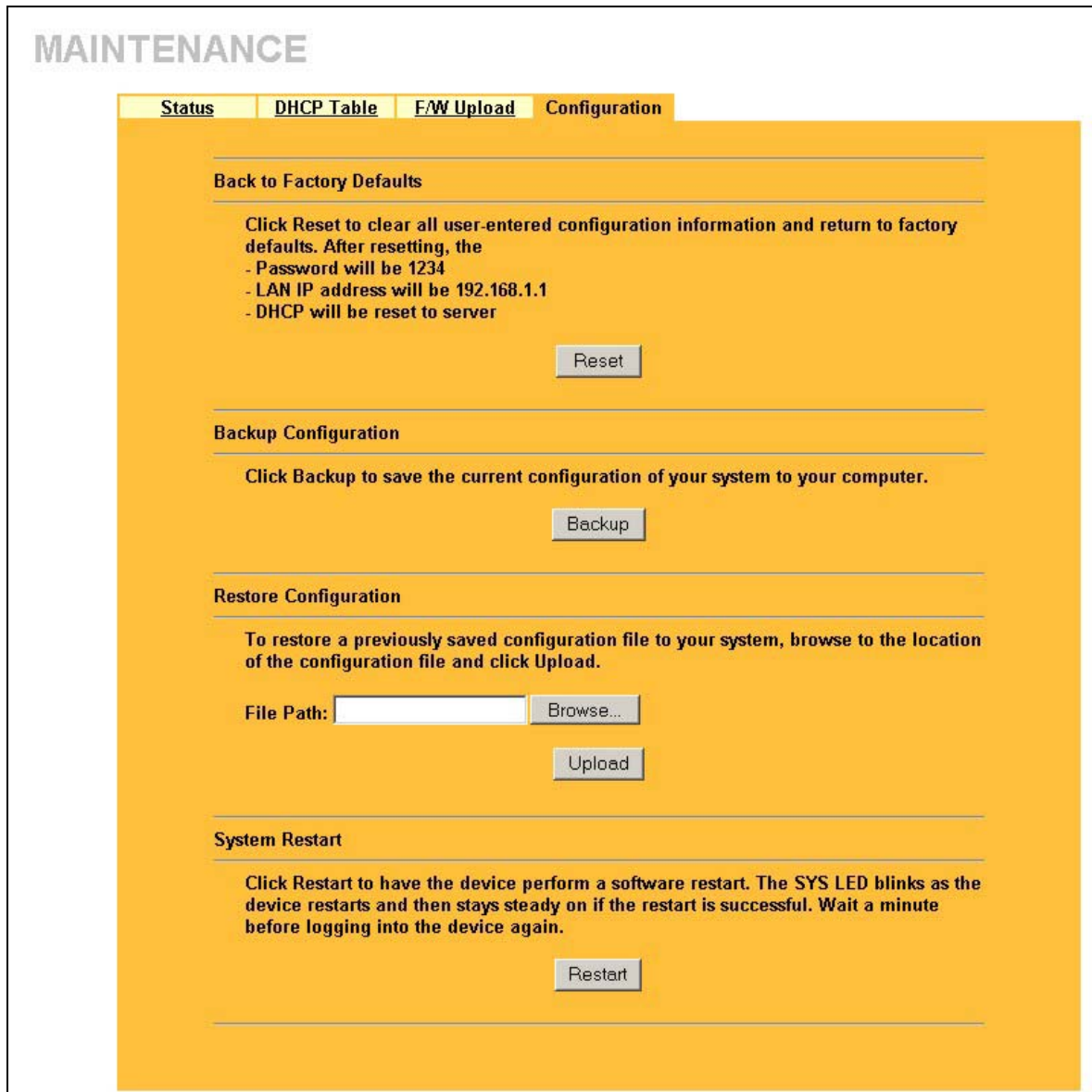
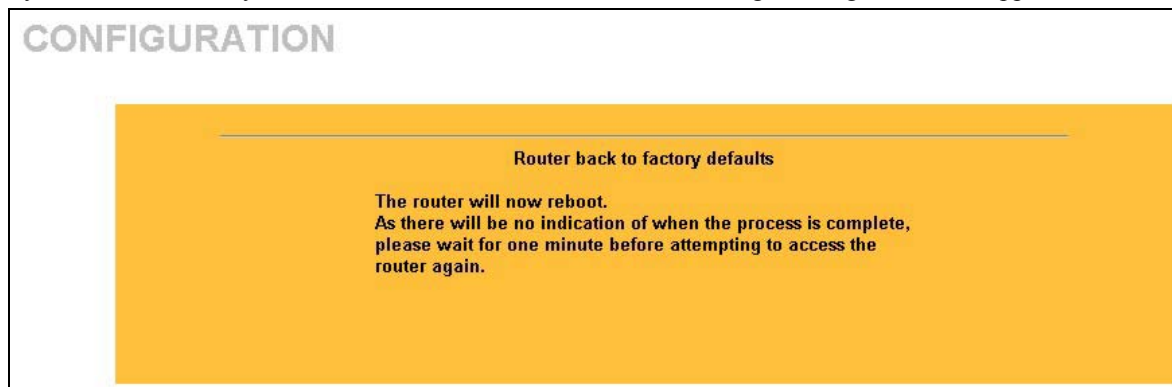


Figure 14-9 Configuration

## 14.5.1 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 14-10 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 *Hardware Installation* chapter for more information on the **RESET** button.

## 14.5.2 Backup Configuration

Backup Configuration allows you to backup (save) the current system (ZyWALL) configuration to your computer. Backup is highly recommended once your ZyWALL is functioning properly.

Click **Backup** to save your current ZyWALL configuration to your computer.

## 14.5.3 Restore Configuration

Restore Configuration allows you to restore a previously saved configuration file from your computer to your ZyWALL.

**Table 14-4 Restore Configuration**

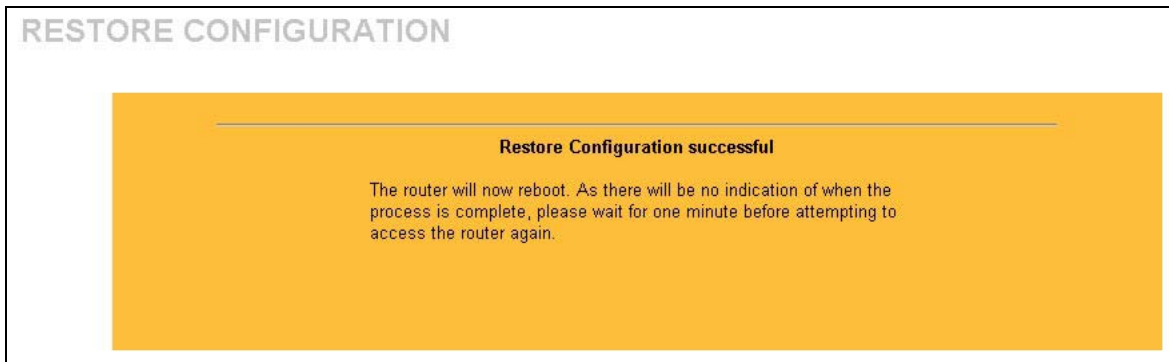
LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click <b>Browse ...</b> to find it.
Browse...	Click <b>Browse...</b> to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click <b>Upload</b> to begin the upload process.

---

**Do not turn off the device while configuration file upload is in progress.**

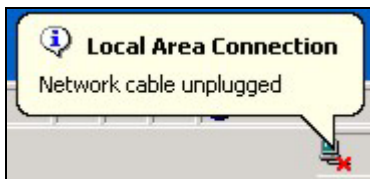
---

After you see a “configuration upload successful” screen, you must then wait one minute before logging into the device again.



**Figure 14-11 Configuration Upload Successful**

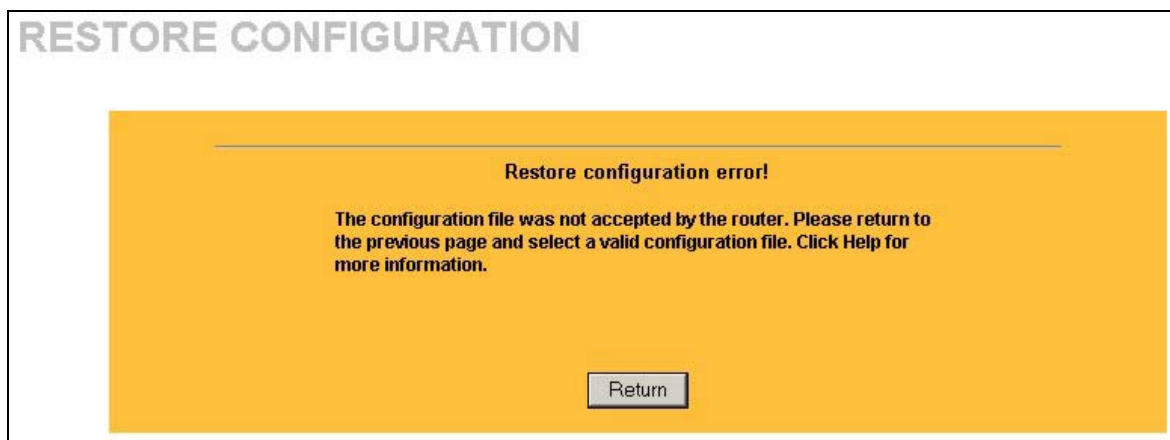
The device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.



**Figure 14-12 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).

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **Configuration** screen.



**Figure 14-13 Configuration Upload Error**

#### **14.5.4 System Restart**

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

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





# Chapter 15

## Firmware and Configuration File Maintenance Commands

*This chapter tells you how to back up and restore your configuration file as well as upload new firmware and a new configuration file using FTP/TFTP.*

It is strongly recommended that you use the web configurator to perform functions mentioned in this chapter (refer to *Chapter 14*). The web configurator is less technical and more intuitive than using FTP/TFTP. Refer to the *Introducing the Web Configurator* chapter to connect to the web configurator. If you wish to use FTP/TFTP, then follow the instructions in this chapter.

### 15.1 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 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 ZyWALL and the external filename refers to the filename not on the ZyWALL, that is, on your computer, local network or FTP site and so the name (but not the extension) may vary. After uploading new firmware, see the ZyNOS **Firmware Version** field in the web configurator by clicking **MAINTENANCE, SYSTEM STATUS** to confirm that you have uploaded the correct firmware version.

**Table 15-1 Filename Conventions**

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	Rom-0	*.rom	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.
Firmware	Ras	*.bin	This is the generic name for the ZyNOS firmware on the ZyWALL.

## 15.2 Backup Configuration

FTP is the preferred method for backing up your current configuration to your computer because it is very fast. 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.

### 15.2.1 Using the FTP Command from the Command Line

- Step 1.** Launch the FTP client on your computer.
- Step 2.** Enter "open", followed by a space and the IP address of your ZyWALL.
- Step 3.** Press [ENTER] when prompted for a username.
- Step 4.** Enter your password as requested (the default is "1234").
- Step 5.** Enter "bin" to set transfer mode to binary.
- Step 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.
- Step 7.** Enter "quit" to exit the ftp prompt.

### 15.2.2 Example of FTP Commands from the Command Line

```
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
```

**Figure 15-1 FTP Session Example**

### 15.2.3 GUI-based FTP Clients

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

**Table 15-2 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.
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

### 15.2.4 Backup Configuration Using TFTP

The ZyWALL supports the up/downloading of the firmware and the configuration file using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To backup the configuration file, follow the procedure shown next.

- Step 1.** 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.
- Step 2.** Launch the TFTP client on your computer and connect to the ZyWALL. Set the transfer mode to binary before starting data transfer.
- Step 3.** Use the TFTP client (see the next example) to transfer files between the ZyWALL and the computer. The file name for the configuration file is "rom-0" (rom-zero, not capital letter "O").

---

**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.**

---

### 15.2.5 TFTP Command Example

The following is an example TFTP command:

```
tftp [-i] host get rom-0 config.rom
```

where "i" specifies binary image transfer mode (use this mode when transferring binary files), "host" is the ZyWALL's 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.

## 15.2.6 GUI-based TFTP Clients

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

**Table 15-3 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.

## 15.3 Restore or Upload a Configuration File

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 file transfer is fast. Please note that you must wait for the system to automatically restart after the file transfer is complete.

---

### **WARNING!**

**DO NOT INTERRUPT THE FILE TRANSFER PROCESS AS THIS MAY PERMANENTLY DAMAGE YOUR ZYWALL. WHEN THE RESTORE CONFIGURATION PROCESS IS COMPLETE, THE ZYWALL WILL AUTOMATICALLY RESTART.**

---

### 15.3.1 Restore Using FTP

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

**Step 1.** Launch the FTP client on your computer.

- Step 2.** Enter "open", followed by a space and the IP address of your ZyWALL.
- Step 3.** Press [ENTER] when prompted for a username.
- Step 4.** Enter your password as requested (the default is "1234").
- Step 5.** Enter "bin" to set transfer mode to binary.
- Step 6.** Find the "rom" file (on your computer) that you want to restore to your ZyWALL.
- Step 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.
- Step 8.** Enter "quit" to exit the ftp prompt. The ZyWALL will automatically restart after a successful restore process.

### 15.3.2 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.
Typ>quit
```

**Figure 15-2 Restore Using FTP Session Example**

## 15.4 Uploading a Firmware File

This section shows you how to upload a firmware file. You can upload a configuration file by following the procedure in section 15.3.

---

### WARNING!

**DO NOT INTERRUPT THE FILE TRANSFER PROCESS AS THIS MAY PERMANENTLY DAMAGE YOUR ZYWALL.**

---

### 15.4.1 Firmware File Upload

FTP is the preferred method for uploading firmware and configuration files. To use this feature, your computer must have an FTP client.

### 15.4.2 FTP File Upload Command from the DOS Prompt Example

- Step 1.** Launch the FTP client on your computer.
- Step 2.** Enter "open", followed by a space and the IP address of your ZyWALL.
- Step 3.** Press [ENTER] when prompted for a username.
- Step 4.** Enter your password as requested (the default is "1234").



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.

### **15.4.5 TFTP Upload Command Example**

The following is an example TFTP command:

```
tftp [-i] host put firmware.bin ras
```

where "i" specifies binary image transfer mode (use this mode when transferring binary files), "host" is the ZyWALL's IP address, "put" transfers the file source on the computer (firmware.bin - name of the firmware on the computer) to the file destination on the remote host (ras - name of the firmware on the ZyWALL).

Commands that you may see in GUI-based TFTP clients are listed earlier in this chapter.





# Chapter 16

## 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. See the Supporting CD for further information.*

### 16.1 Problems Starting Up the ZyWALL

**Table 16-1 Troubleshooting the Start-Up of Your ZyWALL**

PROBLEM	CORRECTIVE ACTION
None of the LEDs are on when I turn on the ZyWALL.	<p>Make sure that you have the correct 5 VDC power adapter connected to the ZyWALL and plugged in to an appropriate power source.</p> <p>If the error persists, you may have a hardware problem. In this case, you should contact your vendor.</p>

### 16.2 Problems with the Password

**Table 16-2 Troubleshooting the Password**

PROBLEM	CORRECTIVE ACTION
I forgot my password	The default password is "1234". Enter it in the <b>Login</b> screen.
	If you have changed your password and cannot remember it, reset the ZyWALL using the procedure in the <i>Procedure to Use the RESET Button</i> section.
	If the error persists, you may have a hardware problem. In this case, you should contact your vendor.

## 16.3 Problems with the LAN Interface

**Table 16-3 Troubleshooting the LAN Interface**

PROBLEM	CORRECTIVE ACTION
I cannot access the ZyWALL from the LAN.	<p>Check your Ethernet cable type and connections. Refer to the <i>LAN 10/100M Ports 1-4</i> section for LAN connection instructions.</p> <p>Make sure your NIC (Network Interface Card) is installed and functioning properly.</p>
I cannot ping any computer on the LAN.	<p>If all of the 10/100M LAN LEDs are off, check the cables between the ZyWALL and your computer or hub.</p> <p>Verify that the IP addresses and subnet masks of the ZyWALL and the computers on the LAN are on the same subnet.</p>

## 16.4 Problems with the WAN Interface

**Table 16-4 Troubleshooting the WAN Interface**

PROBLEM	CORRECTIVE ACTION
I cannot get a WAN IP address from the ISP.	<p>The WAN IP is provided after the ISP verifies the MAC address, host name or user ID.</p> <p>Find out the verification method used by your ISP.</p> <p>If the ISP checks the WAN MAC Address, click <b>MAINTENANCE</b> and then <b>DHCP Table</b> to display the ZyWALL's WAN MAC address. Send it to the ISP.</p> <p>If the ISP does not allow you to use a new MAC, click <b>WAN</b> and then the <b>MAC</b> tab. Clone the MAC from the LAN as the WAN. ZyXEL recommends that you configure this menu even if your ISP presently does not require MAC address authentication.</p> <p>If the ISP checks the host name, enter your computer's name (refer to the <i>Wizard Setup</i> chapter in the User's Guide) in the <b>System Name</b> field in the first screen of the <b>WIZARD SETUP</b>.</p> <p>If the ISP checks the user ID, click <b>WAN</b> and the <b>ISP</b> tab. Check your service type, user name, and password.</p>

## 16.5 Problems with Internet Access

**Table 16-5 Troubleshooting Internet Access**

PROBLEM	CORRECTIVE ACTION
I cannot access the Internet.	<p>Check the ZyWALL's connection to the cable/xDSL device.</p> <p>Check whether your cable/xDSL device requires a crossover or straight-through cable.</p> <p>Click WAN and verify your settings.</p>

## 16.6 Problems with the Firewall

**Table 16-6 Troubleshooting the Firewall**

PROBLEM	CORRECTIVE ACTION
I cannot configure the firewall.	<p>You will not be able to access the web configurator from the WAN if:</p> <p>The firewall is activated, as the firewall, by default, blocks all WAN to LAN traffic. To access the web configurator from the WAN when the firewall is activated, you will need to create a firewall rule to allow web traffic initiated from the WAN.</p> <p>You have blocked a critical web service. Click <b>FIREWALL, SERVICES</b> to review what services are currently blocked.</p>



---

---

# Part V:

---

---

## Appendices and Index

---

This part provides appendices and an index of key terms.



# Appendix A

## PPPoE

### PPPoE in Action

An ADSL modem bridges a PPP session over Ethernet (PPP over Ethernet, RFC 2516) from your PC to an ATM PVC (Permanent Virtual Circuit) that connects to an xDSL Access Concentrator where the PPP session terminates (see the next figure). 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:

- Step 1.** It provides you with a familiar dial-up networking (DUN) user interface.
- Step 2.** 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 & ISDN), the switching fabric is already in place.
- Step 3.** 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 PCs use traditional dial-up networking.

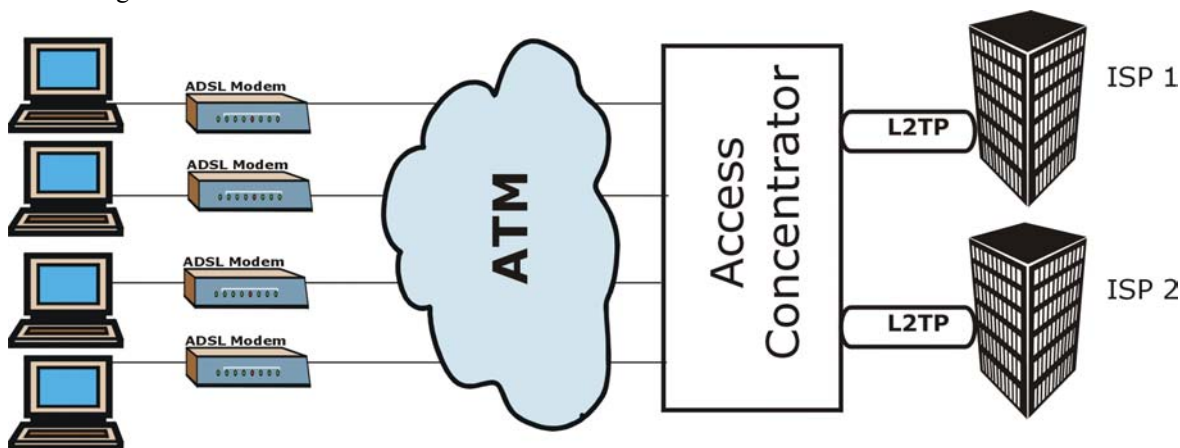


Diagram 1 Single-PC per Modem Hardware Configuration

## How PPPoE Works

The PPPoE driver makes the Ethernet appear as a serial link to the PC and the PC 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 PC and the ISP.

## The ZyWALL as a PPPoE Client

When using the ZyWALL as a PPPoE client, the PCs 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 PCs.

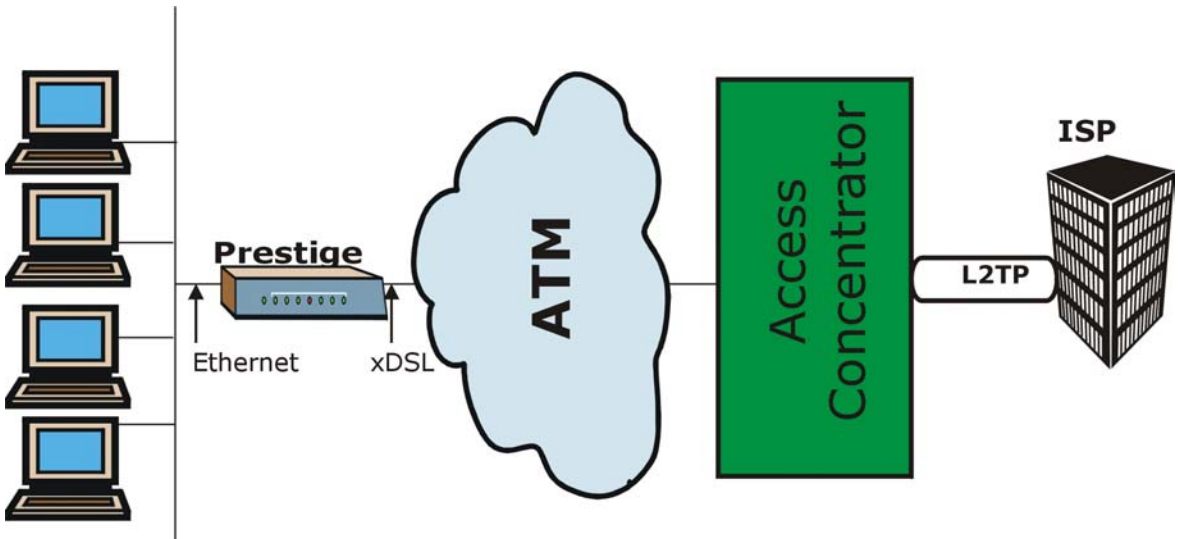


Diagram 2 ZyWALL as a PPPoE Client



# Appendix B

## 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 PC 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 PC 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 PC 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.

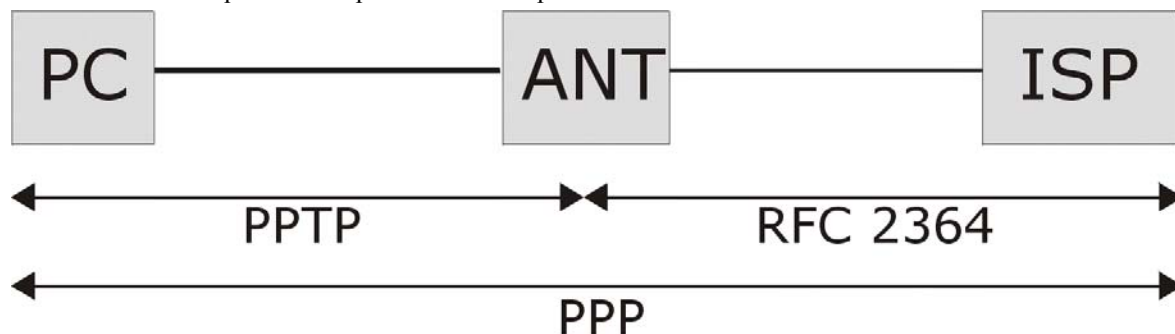


Diagram 3 Transport PPP frames over Ethernet

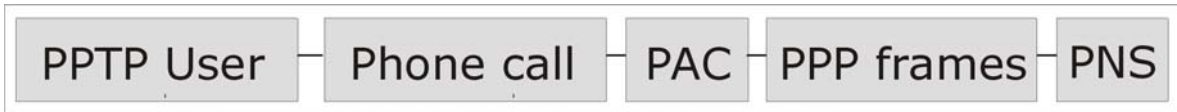
### PPTP and the ZyWALL

When the ZyWALL is deployed in such a setup, it appears as a PC to the ANT (ADSL Network Termination).

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 NAT mode, the ZyWALL is able to pass the PPTP packets to the internal PPTP server (for example NT server) behind the NAT. In the case above as the PPTP connection is initialized by the remote PPTP Client, 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.



**Diagram 4 PPTP Protocol Overview**

Microsoft includes PPTP as a part of the Windows OS. In Microsoft's implementation, the PC, 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.

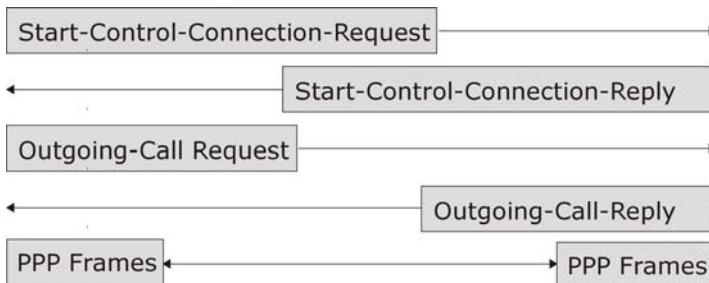
## Control and PPP Connections

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 PC and an ANT.



**Diagram 5 Example Message Exchange between PC 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 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.)

**Chart 1 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

---

**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.

**Chart 2 Allowed IP Address Range By Class**

<b>CLASS</b>	<b>ALLOWED RANGE OF FIRST OCTET (BINARY)</b>	<b>ALLOWED RANGE OF FIRST OCTET (DECIMAL)</b>
Class A	00000000 to 01111111	0 to 127
Class B	10000000 to 10111111	128 to 191
Class C	11000000 to 11011111	192 to 223
Class D	11100000 to 11101111	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 bits; each bit of the mask corresponds to a bit of the IP address. If a bit in the subnet mask 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.

**Chart 3 “Natural” Masks**

<b>CLASS</b>	<b>NATURAL MASK</b>
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.

**Chart 4 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.

	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.

---

**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.**

**Chart 5 Subnet 1**

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	10000000
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

**Chart 6 Subnet 2**

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	10000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	10000000
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



(11111111.11111111.11111111.11000000) 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).

**Chart 7 Subnet 1**

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
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	

**Chart 8 Subnet 2**

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	01000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
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	

**Chart 9 Subnet 3**

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	10000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
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	

**Chart 10 Subnet 4**

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192

IP Address (Binary)	11000000.10101000.00000001.	<b>11</b> 000000
Subnet Mask (Binary)	11111111.11111111.11111111.	<b>11</b> 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.

**Chart 11 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.

**Chart 12 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 *Chart 1*) available for subnetting.

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

**Chart 13 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

**Chart 13 Class B Subnet Planning**

<b>NO. "BORROWED" HOST BITS</b>	<b>SUBNET MASK</b>	<b>NO. SUBNETS</b>	<b>NO. HOSTS PER SUBNET</b>
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

## Power Adapter Specifications

<b>JAPAN, TAIWAN AND USA PLUG STANDARDS</b>	
Model Number	DSA-0151A-05A
Input Power	AC100-120V 50/60Hz
Output Power	5VDC, 2.4A
Power Consumption	12 W
Safety Standards	UL, FCC, CE
<b>EUROPEAN PLUG STANDARDS</b>	
Model Number	DSA-0151A-05A (U)
Input Power	AC200-240V 50-60Hz 0.4A
Output Power	5VDC, 2.4A
Power Consumption	12W
Safety Standards	UL, FCC, CE
<b>UNITED KINGDOM PLUG STANDARDS</b>	
Model Number	DSA-0151A-05A (K)
Input Power	AC200-240Volts/50Hz/0.2A
Output Power	5VDC, 2.4A
Power Consumption	12w
Safety Standards	UL, FCC, CE



# Appendix E

## 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.

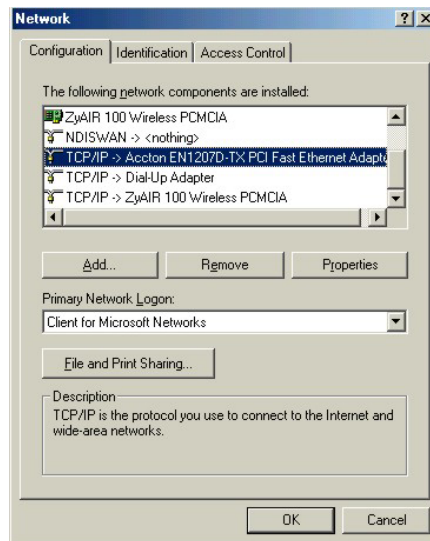
TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

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.



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:

- a. In the **Network** window, click **Add**.
- b. Select **Adapter** and then click **Add**.
- c. Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

- a. In the **Network** window, click **Add**.
- b. Select **Protocol** and then click **Add**.
- c. Select **Microsoft** from the list of **manufacturers**.
- d. Select **TCP/IP** from the list of network protocols and then click **OK**.

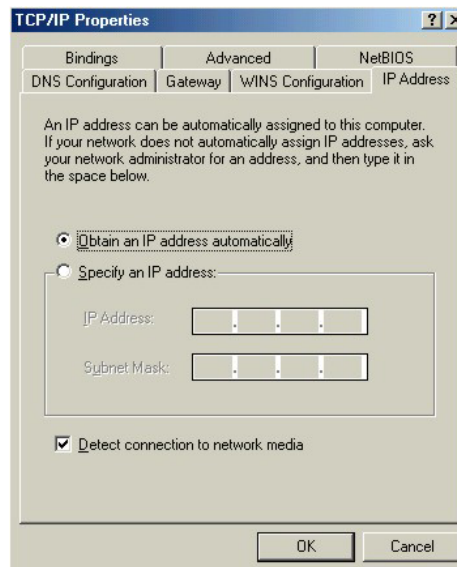
If you need Client for Microsoft Networks:

- a. Click **Add**.
- b. Select **Client** and then click **Add**.
- c. Select **Microsoft** from the list of manufacturers.
- d. Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.
- e. Restart your computer so the changes you made take effect.

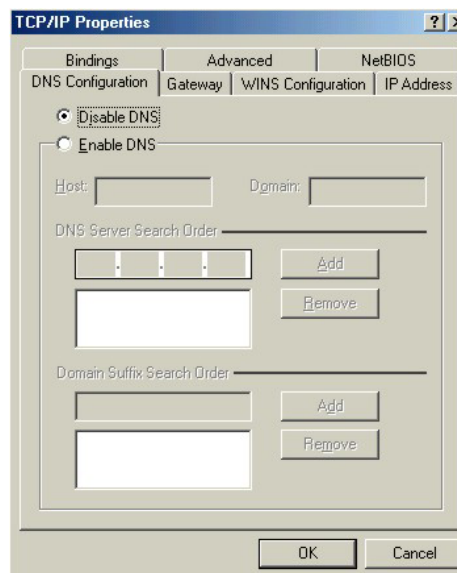
In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**.



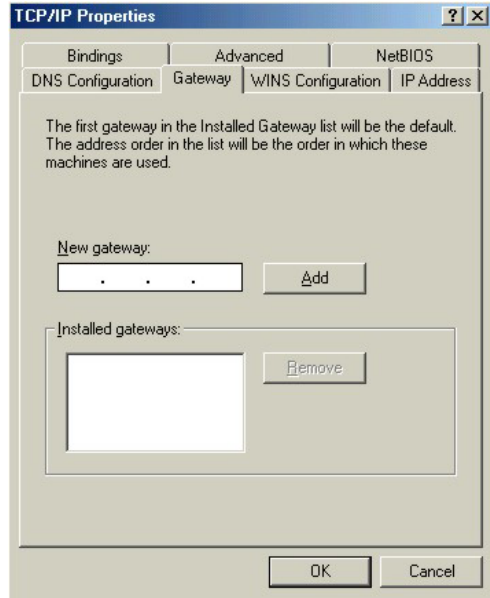
1. Click the **IP Address** tab.
  - If your IP address is dynamic, select **Obtain an IP address automatically**.
  - If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.



2. 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).



3. 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**.



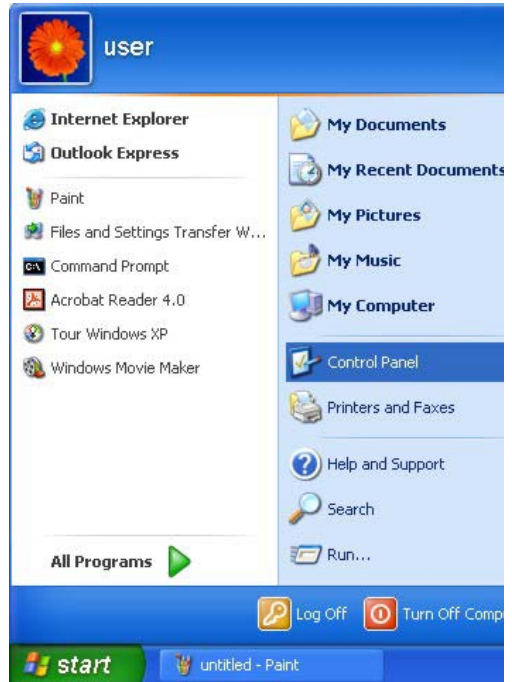
4. Click **OK** to save and close the **TCP/IP Properties** window.
5. Click **OK** to close the **Network** window. Insert the Windows CD if prompted.
6. Turn on your ZyWALL and restart your computer when prompted.

### Verifying Your Computer's IP Address

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

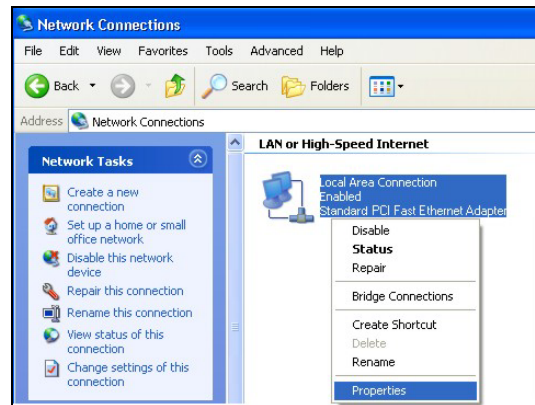
1. For Windows XP, click **start, Control Panel**. In Windows 2000/NT, click **Start, Settings, Control Panel**.



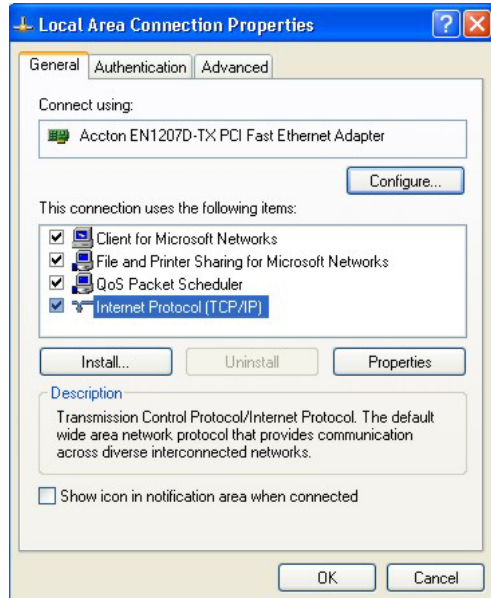
2. For Windows XP, click **Network Connections**. For Windows 2000/NT, click **Network and Dial-up Connections**.



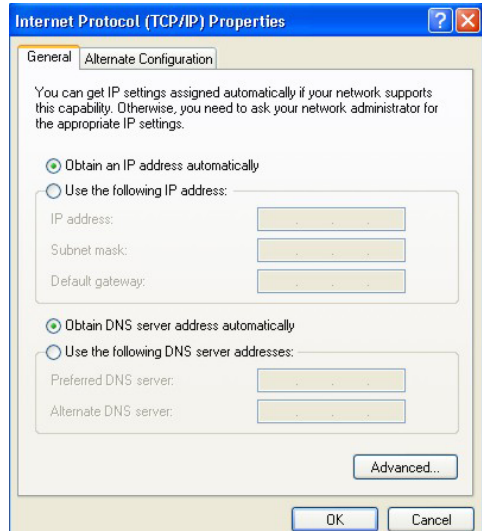
3. Right-click **Local Area Connection** and then click **Properties**.



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



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

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

-In the **IP Settings** tab, in IP addresses, click **Add**.

-In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.

-Repeat the above two steps for each IP address you want to add.

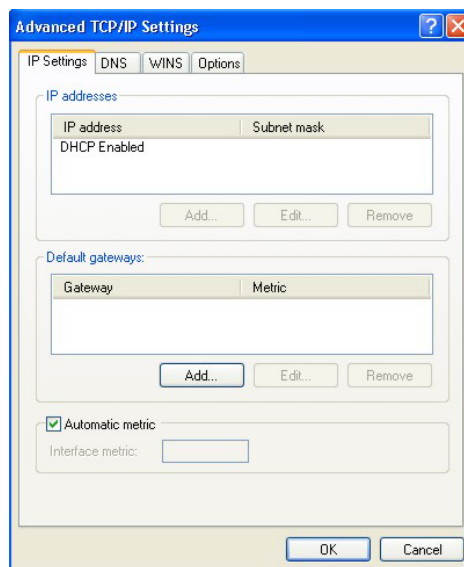
-Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.

-In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.

-Click **Add**.

-Repeat the previous three steps for each default gateway you want to add.

-Click **OK** when finished.

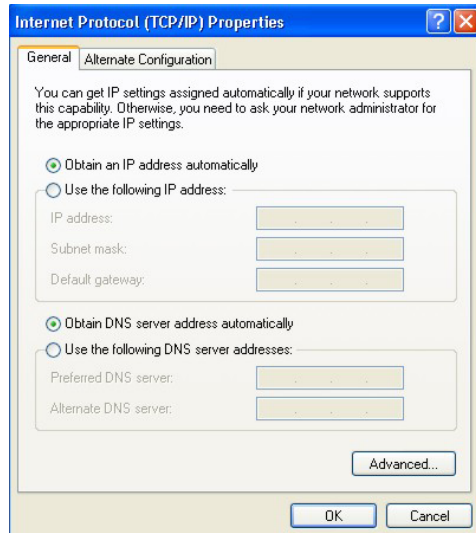


7. In the **Internet Protocol TCP/IP Properties** window (the **General tab** in Windows XP):

-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.



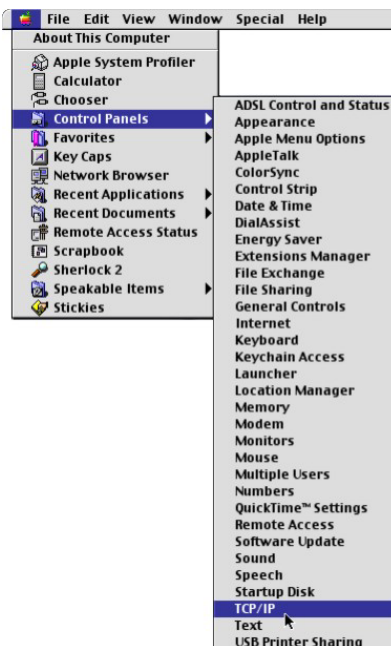
8. Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
9. Click **OK** to close the **Local Area Connection Properties** window.
10. Turn on your ZyWALL and restart your computer (if prompted).

### Verifying Your Computer's IP Address

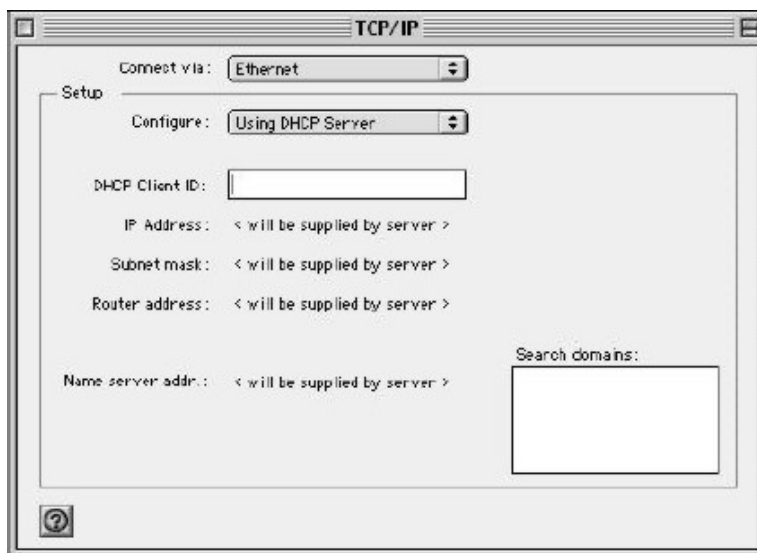
1. Click **Start, All Programs, Accessories** and then **Command Prompt**.
2. In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

## Macintosh OS 8/9

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



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



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

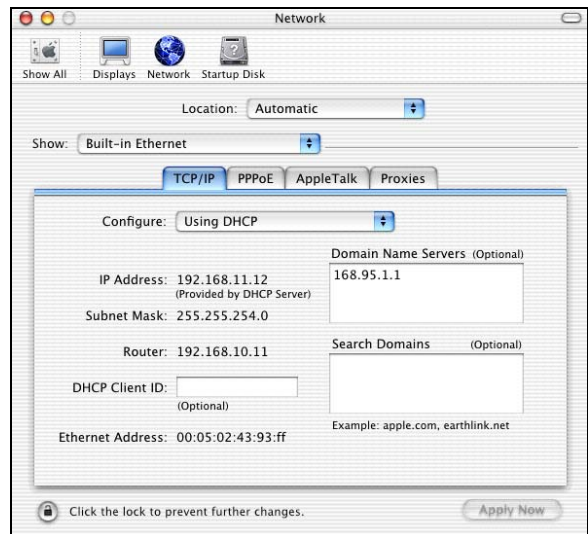
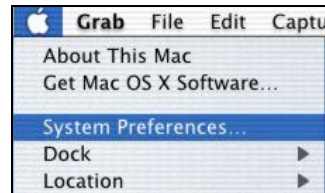
4. For statically assigned settings, do the following:
  - From the **Configure** box, select **Manually**.
  - Type your IP address in the **IP Address** box.
  - Type your subnet mask in the **Subnet mask** box.
  - Type the IP address of your ZyWALL in the **Router address** box.
5. Close the **TCP/IP 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 Your Computer's IP Address

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.
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.
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 Your Computer's IP Address

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



# Appendix F

## Log Descriptions

### Chart 14 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.

### Chart 15 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.
DHCP client gets %s	A DHCP client got a new ip from the DHCP server.
DHCP client IP expired	A DHCP client's IP address has expired.
DHCP server assigns %s	The DHCP server assigns an IP address to a client.
SMT Login Successfully	Someone has logged on to the router's SMT interface.
SMT Login Fail	Someone has failed to log on to the router's SMT interface.
WEB Login Successfully	Someone has logged on to the router's web configurator interface.
WEB Login Fail	Someone has failed to log on to the router's web configurator interface.
TELNET Login Successfully	Someone has logged on to the router via telnet.

**Chart 15 System Maintenance Logs**

TELNET Login Fail	Someone has failed to log on to the router via telnet.
FTP Login Successfully	Someone has logged on to the router via ftp.
FTP Login Fail	Someone has failed to log on to the router via ftp.
NAT Session Table is Full!	The maximum number of session table entries has been exceeded and the table is full.
!! Phase 1 ID type mismatch	The ID type of an incoming packet does not match the local's peer ID type.
!! Phase 1 ID content mismatch	The ID content of an incoming packet does not match the local's peer ID content.
!! No known phase 1 ID type found	The ID type of an incoming packet does not match any known ID type.

**Chart 16 UPnP Logs**

LOG MESSAGE	DESCRIPTION
UPnP pass through Firewall	UPnP packets can pass through the firewall.

**Chart 17 Content Filtering Logs**

CATEGORY	LOG MESSAGE	DESCRIPTION
URLFOR	IP/Domain Name	This IP/Domain can be forwarded.
URLBLK	IP/Domain Name	This IP/Domain name has been blocked due to a forbidden keyword. All web traffic is disabled except for trusted domains, untrusted domains, or the cybernot list.
	IP/Domain Name	
	IP/Domain Name	
	IP/Domain Name	

**Chart 17 Content Filtering Logs**

JAVBLK	IP/Domain Name	This IP/Domain name has been blocked because of a forbidden service such as: activex, java applet, cookie, or proxy.
	IP/Domain Name	
	IP/Domain Name	
	IP/Domain Name	

**Chart 18 Attack Logs**

<b>LOG MESSAGE</b>	<b>DESCRIPTION</b>
attack TCP	The firewall detected a TCP attack.
attack UDP	The firewall detected an UDP attack.
attack IGMP	The firewall detected an IGMP attack.
attack ESP	The firewall detected an ESP attack.
attack GRE	The firewall detected a GRE attack.
attack OSPF	The firewall detected an OSPF attack.
attack ICMP (type:%d, code:%d)	The firewall detected an ICMP attack, see the section on ICMP messages for type and code details.
land TCP	The firewall detected a TCP land attack.
land UDP	The firewall detected an UDP land attack.
land IGMP	The firewall detected an IGMP land attack.
land ESP	The firewall detected an ESP land attack.
land GRE	The firewall detected a GRE land attack.
land OSPF	The firewall detected an OSPF land attack.
land ICMP (type:%d, code:%d)	The firewall detected an ICMP land attack, see the section on ICMP messages for type and code details..
ip spoofing - WAN TCP	The firewall detected a TCP IP spoofing attack from WAN port.
ip spoofing - WAN UDP	The firewall detected an UDP IP spoofing attack from the WAN port.

Chart 18 Attack Logs

LOG MESSAGE	DESCRIPTION
ip spoofing - WAN IGMP	The firewall detected an IGMP IP spoofing attack from the WAN port.
ip spoofing - WAN ESP	The firewall detected an ESP IP spoofing attack from the WAN port.
ip spoofing - WAN GRE	The firewall detected a GRE IP spoofing attack from the WAN port.
ip spoofing - WAN OSPF	The firewall detected an OSPF IP spoofing attack from the WAN port.
ip spoofing - WAN ICMP (type:%d, code:%d)	The firewall detected an ICMP IP spoofing attack from the WAN port. See the section on ICMP messages for type and code details.
icmp echo ICMP (type:%d, code:%d)	The firewall detected an ICMP attack of icmp echo, ICMP. See the section on ICMP messages for type and code details.
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 an 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, see the section on ICMP messages for type and code details.
illegal command TCP	The firewall detected a TCP illegal command attack.
NetBIOS TCP	The firewall detected an TCP NetBIOS attack.
ip spoofing - no routing entry TCP	The firewall detected an ip spoofing attack for no routing entry of TCP.
ip spoofing - no routing entry UDP	The firewall detected an IP spoofing attack for no routing entry of UDP.
ip spoofing - no routing entry IGMP	The firewall detected an IP spoofing attack for no routing entry of IGMP.
ip spoofing - no routing entry ESP	The firewall detected an IP spoofing attack for no routing entry of ESP.

**Chart 18 Attack Logs**

<b>LOG MESSAGE</b>	<b>DESCRIPTION</b>
ip spoofing - no routing entry GRE	The firewall detected an IP spoofing attack for no routing entry of GRE.
ip spoofing - no routing entry OSPF	The firewall detected an IP spoofing attack for no routing entry of OSPF.
ip spoofing - no routing entry ICMP (type:%d, code:%d)	The firewall detected an IP spoofing attack for no routing entry of ICMP, see the section on ICMP messages for type and code details.
vulnerability ICMP (type:%d, code:%d)	The firewall detected an ICMP vulnerability attack; see the section on ICMP messages for type and code details.
traceroute ICMP (type:%d, code:%d)	The firewall detected an ICMP traceroute attack; see the section on ICMP messages for type and code details.

**Chart 19 Access Logs**

<b>LOG MESSAGE</b>	<b>DESCRIPTION</b>
Firewall default policy: TCP (set:%d)	TCP access matched the default policy and was blocked or forwarded according to the user's settings. The ACL set denotes the packet's direction.
Firewall default policy: UDP (set:%d)	UDP access matched the default policy and was blocked or forwarded according to the user's settings. The ACL set denotes the packet's direction.
Firewall default policy: ICMP (set:%d, type:%d, code:%d)	ICMP access matched the default policy and was blocked or forwarded according to the user's settings. The ACL set denotes the packet's direction. See the section on ICMP messages for type and code details.
Firewall default policy: IGMP (set:%d)	IGMP access matched the default policy and was blocked or forwarded according to the user's settings. The ACL set denotes the packet's direction.
Firewall default policy: ESP (set:%d)	ESP access matched the default policy and was blocked or forwarded according to the user's settings. The ACL set denotes the packet's direction.
Firewall default policy: GRE (set:%d)	GRE access matched the default policy and was blocked or forwarded according to the user's settings. The ACL set denotes the packet's direction.
Firewall default policy: OSPF (set:%d)	OSPF access matched the default policy and was blocked or forwarded according to the user's settings. The ACL set denotes the packet's direction.
Firewall default policy: (set:%d)	Access matched the default policy and was blocked or forwarded according to the user's settings. The ACL set denotes the packet's direction.
Firewall rule match: TCP (set:%d, rule:%d)	TCP access matched one of the user's configured firewall rules and was blocked or forwarded according to the user's rule. Set and rule denote the packet direction and the number of the firewall rule.
Firewall rule match: UDP (set:%d, rule:%d)	UDP access matched one of the user's configured firewall rules and was blocked or forwarded according to the user's rule. Set and rule denote the packet direction and the number of the firewall rule.



**Chart 19 Access Logs**

Firewall rule match: ICMP (set:%d, rule:%d, type:%d, code:%d)	ICMP access matched one of the user's configured firewall rules and was blocked or forwarded according to the user's rule. Set and rule denote the packet direction and the number of the firewall rule. See the section on ICMP messages for type and code details.
Firewall rule match: IGMP (set:%d, rule:%d)	IGMP access matched one of the user's configured firewall rules and was blocked or forwarded according to the user's rule. Set and rule denote the packet direction and the number of the firewall rule.
Firewall rule match: ESP (set:%d, rule:%d)	ESP access matched with firewall user setting, 'Block' or 'Forward' by user setting. Set and rule denote the packet direction and the number of setting rule.
Firewall rule match: GRE (set:%d, rule:%d)	GRE access matched one of the user's configured firewall rules and was blocked or forwarded according to the user's rule. Set and rule denote the packet direction and the number of the firewall rule.
Firewall rule match: OSPF (set:%d, rule:%d)	OSPF access matched one of the user's configured firewall rules and was blocked or forwarded according to the user's rule. Set and rule denote the packet direction and the number of the firewall rule.
Firewall rule match: (set:%d, rule:%d)	Access matched one of the user's configured firewall rules and was blocked or forwarded according to the user's rule. Set and rule denote the packet direction and the number of the firewall rule.
Firewall rule NOT match: TCP (set:%d, rule:%d)	TCP access did not match one of the user's configured firewall rules and was logged. Set and rule denote the packet direction and the number of the firewall rule that the packet did not match.
Firewall rule NOT match: UDP (set:%d, rule:%d)	UDP access did not match one of the user's configured firewall rules and was logged. Set and rule denote the packet direction and the number of the firewall rule that the packet did not match. □
Firewall rule NOT match: ICMP (set:%d, rule:%d, type:%d, code:%d)	ICMP access did not match one of the user's configured firewall rules and was logged. Set and rule denote the packet direction and the number of the firewall rule that the packet did not match.
Firewall rule NOT match: IGMP (set:%d, rule:%d)	IGMP access did not match one of the user's configured firewall rules and was logged. Set and rule denote the packet direction and the number of the firewall rule that the packet did not match.

Chart 19 Access Logs

Firewall rule NOT match: ESP (set:%d, rule:%d)	ESP access did not match one of the user's configured firewall rules and was logged. Set and rule denote the packet direction and the number of the firewall rule that the packet did not match.□
Firewall rule NOT match: GRE (set:%d, rule:%d)	GRE access did not match one of the user's configured firewall rules and was logged. Set and rule denote the packet direction and the number of the firewall rule that the packet did not match.□
Firewall rule NOT match: OSPF (set:%d, rule:%d)	OSPF access did not match one of the user's configured firewall rules and was logged. Set and rule denote the packet direction and the number of the firewall rule that the packet did not match.
Firewall rule NOT match: (set:%d, rule:%d)	Access did not match one of the user's configured firewall rules and was logged. Set and rule denote the packet direction and the number of the firewall rule that the packet did not match.
Filter default policy DROP!	TCP access matched a default filter policy, access was blocked by dropping the packet.
Filter default policy DROP!	UDP access matched a default filter policy; access was blocked by dropping the packet.
Filter default policy DROP!	ICMP access matched a default filter policy; access was blocked by dropping the packet.
Filter default policy DROP!	Access matched a default filter policy; access was blocked by dropping the packet.
Filter default policy DROP!	Access matched a default filter policy (denied LAN IP); access was blocked by dropping the packet.
Filter default policy FORWARD!	TCP access matched a default filter policy, access was allowed and the router forwarded the packet.
Filter default policy FORWARD!	UDP access matched a default filter policy, access was allowed and the router forwarded the packet.
Filter default policy FORWARD!	ICMP access matched a default filter policy, access was allowed and the router forwarded the packet.
Filter default policy FORWARD!	Access matched a default filter policy, access was allowed and the router forwarded the packet.
Filter default policy FORWARD!	Access matched a default filter policy (denied LAN IP), access was allowed and the router forwarded the packet.

**Chart 19 Access Logs**

Filter match DROP <set %d/rule %d>	TCP access matched a user configured filter rule; access was blocked by dropping the packet.
Filter match DROP <set %d/rule %d>	UDP access matched a user configured filter rule; access was blocked by dropping the packet.
Filter match DROP <set %d/rule %d>	ICMP access matched a user configured filter rule; access was blocked by dropping the packet.
Filter match DROP <set %d/rule %d>	Access matched a user configured filter rule; access was blocked by dropping the packet.
Filter match DROP <set %d/rule %d>	Access matched a user configured filter rule (denied LAN IP); access was blocked by dropping the packet.
Filter match FORWARD <set %d/rule %d>	TCP access matched a user configured filter rule, access was allowed and the router forwarded the packet.
Filter match FORWARD <set %d/rule %d>	UDP access matched a user configured filter rule, access was allowed and the router forwarded the packet.
Filter match FORWARD <set %d/rule %d>	ICMP access matched a user configured filter rule, access was allowed and the router forwarded the packet.
Filter match FORWARD <set %d/rule %d>	Access matched a user configured filter rule, access was allowed and the router forwarded the packet.
Filter match FORWARD <set %d/rule %d>	Access matched a user configured filter rule (denied LAN IP), access was allowed and the router forwarded the packet.

**Chart 20 ACL Setting Notes**

ACL SET NUMBER	DIRECTION	DESCRIPTION
L to W	LAN to WAN	Rule for packets traveling from the LAN to the WAN.
W to L	WAN to LAN	Rule for packets traveling from the WAN to the LAN.
L to L	LAN to LAN/ZyWALL	Rule for packets traveling from the LAN to the LAN or the ZyWALL.
W to W	WAN to WAN/ZyWALL	Rule for packets traveling from the WAN to the WAN or the ZyWALL.

**Chart 21 ICMP Notes**

<b>TYPE</b>	<b>CODE</b>	<b>DESCRIPTION</b>
0		Echo Reply
	0	Echo reply message
3		Destination Unreachable
	0	Net unreachable
	1	Host unreachable
	2	Protocol unreachable
	3	Port unreachable
	4	A packet that needed fragmentation was dropped because it was set to Don't Fragment (DF)
	5	Source route failed
4		Source Quench
	0	A gateway may discard internet datagrams if it does not have the buffer space needed to queue the datagrams for output to the next network on the route to the destination network.
5		Redirect
	0	Redirect datagrams for the Network
	1	Redirect datagrams for the Host
	2	Redirect datagrams for the Type of Service and Network
	3	Redirect datagrams for the Type of Service and Host
8		Echo
	0	Echo message
11		Time Exceeded
	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded
12		Parameter Problem

Chart 21 ICMP Notes

TYPE	CODE	DESCRIPTION
	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

## VPN/IPSec logs

The following figure shows a typical log from the initiator of a VPN connection.

```

Index:      Date/Time:      Log:
-----
001  01 Jan 08:02:22  Send Main Mode request to <192.168.100.101>
002  01 Jan 08:02:22  Send:<SA>
003  01 Jan 08:02:22  Recv:<SA>
004  01 Jan 08:02:24  Send:<KE><NONCE>
005  01 Jan 08:02:24  Recv:<KE><NONCE>
006  01 Jan 08:02:26  Send:<ID><HASH>
007  01 Jan 08:02:26  Recv:<ID><HASH>
008  01 Jan 08:02:26  Phase 1 IKE SA process done
009  01 Jan 08:02:26  Start Phase 2: Quick Mode
010  01 Jan 08:02:26  Send:<HASH><SA><NONCE><ID><ID>
011  01 Jan 08:02:26  Recv:<HASH><SA><NONCE><ID><ID>
012  01 Jan 08:02:26  Send:<HASH>
Clear IPSec Log (y/n):

```

Diagram 6 Example VPN Initiator IPSec Log

## VPN Responder IPSec Log

The following figure shows a typical log from the VPN connection peer.

```

Index:      Date/Time:      Log:
-----
001  01 Jan 08:08:07  Recv Main Mode request from <192.168.100.100>
002  01 Jan 08:08:07  Recv:<SA>
003  01 Jan 08:08:08  Send:<SA>
004  01 Jan 08:08:08  Recv:<KE><NONCE>
005  01 Jan 08:08:10  Send:<KE><NONCE>
006  01 Jan 08:08:10  Recv:<ID><HASH>
007  01 Jan 08:08:10  Send:<ID><HASH>
008  01 Jan 08:08:10  Phase 1 IKE SA process done
009  01 Jan 08:08:10  Recv:<HASH><SA><NONCE><ID><ID>
010  01 Jan 08:08:10  Start Phase 2: Quick Mode
011  01 Jan 08:08:10  Send:<HASH><SA><NONCE><ID><ID>
012  01 Jan 08:08:10  Recv:<HASH>
Clear IPSec Log (y/n):
    
```

**Diagram 7 Example VPN Responder IPSec Log**

This menu is useful for troubleshooting. A log index number, the date and time the log was created and a log message are displayed.

**Double exclamation marks (!!)** denote an error or warning message.

The following table shows sample log messages during IKE key exchange.

**Chart 22 Sample IKE Key Exchange Logs**

LOG MESSAGE	DESCRIPTION
Send <Symbol> Mode request to <IP> Send <Symbol> Mode request to <IP>	The ZyWALL has started negotiation with the peer.
Recv <Symbol> Mode request from <IP> Recv <Symbol> Mode request from <IP>	The ZyWALL has received an IKE negotiation request from the peer.
Recv:<Symbol>	IKE uses the ISAKMP protocol (refer to RFC2408 – ISAKMP) to transmit data. Each ISAKMP packet contains payloads of different types that show in the log - see Chart 24.
Phase 1 IKE SA process done	Phase 1 negotiation is finished.
Start Phase 2: Quick Mode	Phase 2 negotiation is beginning using Quick Mode.

Chart 22 Sample IKE Key Exchange Logs

LOG MESSAGE	DESCRIPTION
!! IKE Negotiation is in process	The ZyWALL has begun negotiation with the peer for the connection already, but the IKE key exchange has not finished yet.
!! Duplicate requests with the same cookie	The ZyWALL has received multiple requests from the same peer but it is still processing the first IKE packet from that peer.
!! No proposal chosen	The parameters configured for Phase 1 or Phase 2 negotiations don't match. Please check all protocols and settings for these phases. For example, one party may be using 3DES encryption, but the other party is using DES encryption, so the connection will fail.
!! Verifying Local ID failed !! Verifying Remote ID failed	During IKE Phase 2 negotiation, both parties exchange policy details, including local and remote IP address ranges. If these ranges differ, then the connection fails.
!! Local / remote IPs of incoming request conflict with rule <#d>	If the security gateway is "0.0.0.0", the ZyWALL will use the peer's "Local Addr" as its "Remote Addr". If this IP (range) conflicts with a previously configured rule then the connection is not allowed.
!! Invalid IP <IP start>/<IP end>	The peer's "Local IP Addr" range is invalid.
!! Remote IP <IP start> / <IP end> conflicts	If the security gateway is "0.0.0.0", the ZyWALL will use the peer's "Local Addr" as its "Remote Addr". If a peer's "Local Addr" range conflicts with other connections, then the ZyWALL will not accept VPN connection requests from this peer.
!! Active connection allowed exceeded	The ZyWALL limits the number of simultaneous Phase 2 SA negotiations. The IKE key exchange process fails if this limit is exceeded.
!! IKE Packet Retransmit	The ZyWALL did not receive a response from the peer and so retransmits the last packet sent.
!! Failed to send IKE Packet	The ZyWALL cannot send IKE packets due to a network error.
!! Too many errors! Deleting SA	The ZyWALL deletes an SA when too many errors occur.

**Chart 22 Sample IKE Key Exchange Logs**

LOG MESSAGE	DESCRIPTION
!! Phase 1 ID type mismatch	The ID type of an incoming packet does not match the local's peer ID type.
!! Phase 1 ID content mismatch	The ID content of an incoming packet does not match the local's peer ID content.
!! No known phase 1 ID type found	The ID type of an incoming packet does not match any known ID type.
Peer ID: IP address type <IP address>	The IP address type or IP address of an incoming packet does not match the peer IP address type or IP address configured on the local router. The log displays the IP address type and IP address of the incoming packet.
vs. My Remote <IP address>	The IP address type or IP address of an incoming packet does not match the peer IP address type or IP address configured on the local router. The log displays this router's configured remote IP address type or IP address that the incoming packet did not match.
vs. My Local <IP address>	The IP address type or IP address of an incoming packet does not match the peer IP address type or IP address configured on the local router. The log displays this router's configured local IP address type or IP address that the incoming packet did not match.
-> <symbol>	The router sent a payload type of IKE packet.
Error ID Info	The parameters configured for Phase 1 ID content do not match or the parameters configured for the Phase 2 ID (IP address of single, range or subnet) do not match. Please check all protocols and settings for these phases.

The following table shows sample log messages during packet transmission.

**Chart 23 Sample IPsec Logs During Packet Transmission**

LOG MESSAGE	DESCRIPTION
!! WAN IP changed to <IP>	If the ZyWALL's WAN IP changes, all configured "My IP Addr" are changed to b "0.0.0.0". If this field is configured as 0.0.0.0, then the



**Chart 23 Sample IPsec Logs During Packet Transmission**

LOG MESSAGE	DESCRIPTION
	ZyWALL will use the current ZyWALL WAN IP address (static or dynamic) to set up the VPN tunnel.
!! Cannot find IPsec SA	The ZyWALL cannot find a phase 2 SA that corresponds with the SPI of an inbound packet (from the peer); the packet is dropped.
!! Cannot find outbound SA for rule <%d>	The packet matches the rule index number (#d), but Phase 1 or Phase 2 negotiation for outbound (from the VPN initiator) traffic is not finished yet.
!! Discard REPLAY packet	If the ZyWALL receives a packet with the wrong sequence number it will discard it.
!! Inbound packet authentication failed	The authentication configuration settings are incorrect. Please check them.
!! Inbound packet decryption failed	The decryption configuration settings are incorrect. Please check them.
Rule <#d> idle time out, disconnect	If an SA has no packets transmitted for a period of time (configurable via CI command), the ZyWALL drops the connection.

The following table shows RFC-2408 ISAKMP payload types that the log displays. Please refer to the RFC for detailed information on each type.

**Chart 24 RFC-2408 ISAKMP Payload Types**

LOG DISPLAY	PAYLOAD TYPE
SA	Security Association
PROP	Proposal
TRANS	Transform
KE	Key Exchange
ID	Identification
CER	Certificate
CER_REQ	Certificate Request
HASH	Hash
SIG	Signature
NONCE	Nonce

**Chart 24 RFC-2408 ISAKMP Payload Types**

<b>LOG DISPLAY</b>	<b>PAYLOAD TYPE</b>
NOTFY	Notification
DEL	Delete
VID	Vendor ID

# Appendix G

## 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.

### Chart 25 Brute-Force Password Guessing Protection Commands

COMMAND	DESCRIPTION
<code>sys pwderrtm</code>	This command displays the brute-force guessing password protection settings.
<code>sys pwderrtm 0</code>	This command turns off the password's protection from brute-force guessing. The brute-force password guessing protection is turned off by default.
<code>sys pwderrtm N</code>	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.
<b>Example</b>	
<code>sys pwderrtm 5</code>	This command sets the password protection to block all access attempts for five minutes after the third time an incorrect password is entered.



# Index

- A
- About This User's Guide ..... xv
  - Address Assignment ..... 4-8, 4-9
  - Application..... 1-3, 1-4
  - Auto-negotiating LAN 10/100M Ethernet/Fast LAN Interface ..... 1-1
- B
- Backup ..... 14-9, 15-2, 15-3
- C
- Cable Modem..... 2-2
  - CI ..... xv, 1-3, 2-4
  - Computer's IP Address ..... Q
  - Configuration ... A, 1-2, 2-4, 6-1, 12-8, 14-4, 15-1, 15-2, 15-3, 15-4
  - Content Filtering ..... 1-2
  - Customer Support ..... iii
- D
- Default ..... 14-9
  - DHCP. 1-2, 4-1, 4-9, 5-2, 6-1, 6-3, 14-4, 15-1, 16-2
  - Dial-up ..... A
  - DNS
    - Primary Server ..... 6-3
    - Secondary Server ..... 6-3
  - Domain Name ..... 4-1, 4-9, 7-2
  - DSL Modem..... 2-2
  - Dynamic DNS ..... 1-2, 5-2
  - DYNDNS Wildcard ..... 5-2
- E
- ECHO..... 7-2
  - Embedded FTP and TFTP Services..... 1-3
  - Enter ..... See Syntax Conventions
  - Ethernet. A, B, C, 1-1, 2-2, 2-3, 4-2, 4-6, 11-1, 16-2
- F
- Factory LAN Defaults ..... 6-1
  - Features of the ZyWALL..... 1-1
  - Finger..... 7-2
  - Firewall..... 1-1, 11-1, 11-2, 16-3
  - Firmware File Upload..... 15-5
  - Firmware Version ..... 15-1
  - FTPiii, 1-3, 2-4, 5-2, 6-1, 7-1, 7-2, 11-2, 15-1, 15-2, 15-3, 15-4, 15-5, 15-6
  - FTP/TFTP ..... 1-3, 2-4, 15-1
- G
- General Setup ..... 4-1, 5-1
  - Getting to Know Your ZyWALL ..... 1-1
- H
- Host..... 5-5
  - HTTP ..... 7-2, 12-17, 12-18
- I
- IGMP ..... 1-3, 6-2
  - Installation ..... 2-1, 2-3
  - Internet Access..... 16-3
  - IP Address..... 4-8, 4-9, 6-1, 6-4, 7-1, 7-3, 14-4
  - IP Multicast..... 1-3
  - IP Pool ..... 6-3
  - IP Pool Setup ..... 6-1
  - IP Ports ..... 12-17, 12-18

IPSec VPN Capability .....	1-1		
		L	
LAN 10/100M .....	1-1, 2-3		
LAN Setup .....	6-1		
LAN TCP/IP .....	6-1		
LED Descriptions .....	2-1		
Logging .....	1-3		
		M	
Management Information Base (MIB) .....	10-2		
Metric .....	8-3		
Multicast .....	1-3, 6-2, 6-4		
		N	
NAT.C, xv, 1-1, 1-2, 4-6, 4-9, 7-1, 7-2, 7-3, 11-2, 12-4			
NAT Transversal .....	9-1, 9-3		
Network Management .....	1-2, 1-3, 7-2		
NNTP .....	7-2		
		O	
Online Registration .....	ii		
		P	
Password .....	2-3, 5-4, 15-2, 15-3, 16-1		
Point-to-Point Tunneling Protocol C, 1-3, 4-4, 7-2			
POP3 .....	7-2		
Port Numbers .....	7-1		
Power Adapter .....	O		
PPPoE .....	A, B, 1-3, 4-2, 4-6		
PPTP .....	C, D, 1-3, 4-2, 4-4, 4-5, 4-7, 7-2		
PPTP Encapsulation .....	4-4		
Preface .....	xv		
Private .....	8-4		
Private IP Address .....	4-8		
		Q	
Quick Start Guide .....	3-1		
			R
Rear Panel .....	2-2		
RESET Button .....	2-3		
Restore .....	14-9		
RIP .....	6-2		
		S	
Security .....	11-2		
Select .....	See Syntax Conventions		
Server .....	5-6		
Services .....	7-1, 7-2, 11-8		
Single User Account .....	1-2, 7-1		
SMTP .....	7-2		
SNMP .....	1-2, 7-2, 11-2		
Community .....	10-3		
Configuration .....	10-2		
Get .....	10-2		
Manager .....	10-2		
MIBs .....	10-2		
Trap .....	10-2		
Trusted Host .....	10-3		
Stateful Inspection .....	11-1		
Static Route .....	8-1		
SUA .....	1-2, 7-1, 7-2, 7-3		
Subnet Mask .....	4-9, 6-1, 6-4		
System Maintenance .....	13-2		
System Name .....	5-1		
		T	
TCP/IP .....	6-3		
Time Zone .....	5-5		
Tracing .....	1-3		
Troubleshooting .....	16-1		
Turning on .....	2-4		

U		WAN Setup.....	4-10
Universal Plug and Play (UPnP).....	9-1, 9-3	Warranty .....	ii, iii
Uploading a Firmware File .....	15-5	web configurator .....	16-3
UPnP Examples .....	9-3	Web Configurator .....	1-2, 2-4, 3-1, 3-2
User Name .....	5-3	Wizard Setup .....	4-1, 4-2, 4-8
V		Z	
VPN/IPSec .....	12-1	ZyNOS.....	15-1
W			
WAN 10M Port.....	2-2		