

# *ZyWALL 1*

*Internet Security Gateway*

## *User's Guide*

Version 3.50  
December 2001

**ZyXEL**

TOTAL INTERNET ACCESS SOLUTION

# Copyright

Copyright © 2002 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.

# Federal Communications Commission (FCC) Interference Statement

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

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

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

## Notice 1

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

## Certifications

Refer to the product page at [www.zyxel.com](http://www.zyxel.com).

# Information for Canadian Users

The Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective operation and safety requirements. The Industry Canada label does not guarantee that the equipment will operate to a user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company's inside wiring associated with a single line individual service may be extended by means of a certified connector assembly. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

For their own protection, users should ensure that the electrical ground connections of the power utility, telephone lines, and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

## **Caution**

Users should not attempt to make such connections themselves, but should contact the appropriate electrical inspection authority, or electrician, as appropriate.

## **Note**

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the radio interference regulations of Industry Canada.

# 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
<b>LOCATION</b>				
<b>WORLDWIDE</b>	<a href="mailto:support@zyxel.com.tw">support@zyxel.com.tw</a> <a href="mailto:support@europe.zyxel.com">support@europe.zyxel.com</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, Taiwan 300, R.O.C.
<b>NORTH AMERICA</b>	<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.
<b>SCANDINAVIA</b>	<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.
<b>AUSTRIA</b>	<a href="mailto:support@zyxel.at">support@zyxel.at</a>  <a href="mailto:sales@zyxel.at">sales@zyxel.at</a>	+43-1-4948677-0  +43-1-4948678	<a href="http://www.zyxel.at">www.zyxel.at</a>  <a href="ftp://ftp.zyxel.at">ftp.zyxel.at</a>	ZyXEL Communications Services GmbH. Thaliastrasse 125a/2/2/4 A-1160 Vienna, Austria
<b>GERMANY</b>	<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/A4 D-52146 Wuerselen, Germany
<b>MALAYSIA</b>	<a href="mailto:support@zyxel.com.my">support@zyxel.com.my</a>  <a href="mailto:sales@zyxel.com.my">sales@zyxel.com.my</a>	+603-795-44-688  +603-795-34-407	<a href="http://www.zyxel.com.my">www.zyxel.com.my</a>	Lot B2-06, PJ Industrial Park, Section 13, Jalan Kemajuan, 46200 Petaling Jaya Selangor Darul Ehasn, Malaysia

# Table of Contents

Copyright.....	ii
Federal Communications Commission (FCC) Interference Statement .....	iii
Information for Canadian Users .....	iv
ZyXEL Limited Warranty .....	v
Customer Support .....	vi
List of Figures.....	xi
List of Tables .....	xii
List of Diagrams.....	xiii
Preface .....	xiv
<b>GETTING STARTED .....</b>	<b>I</b>
<b>Chapter 1 Getting to Know Your ZyWALL .....</b>	<b>1-1</b>
1.1 The ZyWALL 1 Internet Security Gateway.....	1-1
1.2 Features of the ZyWALL 1 .....	1-1
1.3 ZyWALL VPN Application .....	1-3
<b>Chapter 2 Hardware Installation .....</b>	<b>2-1</b>
2.1 ZyWALL Front and Rear Panels.....	2-1
2.1.1 Front Panel LEDs.....	2-1
2.2 ZyWALL Rear Panel and Connections.....	2-2
2.2.1 WAN 10M Port.....	2-3
2.2.2 LAN 10/100M Ports.....	2-3
2.2.3 UPLINK Button .....	2-3
2.2.4 LAN 10/100M Connections/Uplink Button Usage at a Glance .....	2-4
2.2.5 POWER 5VDC Port.....	2-4
2.2.6 RESET Button.....	2-4
2.3 Additional Installation Requirements.....	2-4
2.4 Turning on Your ZyWALL.....	2-4
2.5 Resetting the ZyWALL.....	2-5
2.5.1 Procedure To Use The RESET Button.....	2-5
2.6 ZyWALL Configuration .....	2-5
2.6.1 Using the Web Configurator .....	2-5
2.6.2 Using FTP/TFTP.....	2-5
2.6.3 Using CI Commands .....	2-5
<b>THE WEB CONFIGURATOR SCREENS .....</b>	<b>II</b>
<b>Chapter 3 Introducing the Web Configurator .....</b>	<b>3-1</b>
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
<b>Chapter 4 The Wizard Setup Screens .....</b>	<b>4-1</b>
4.1 Wizard Setup – Screen 1 .....	4-1

4.1.1	General Setup and System Name .....	4-1
4.1.2	Domain Name .....	4-1
4.2	Wizard Setup - Screen 2 .....	4-1
4.2.1	Ethernet .....	4-1
4.2.2	PPTP Encapsulation .....	4-2
4.2.3	PPPoE Encapsulation .....	4-2
4.3	Wizard Setup – Screen 3 .....	4-2
4.3.1	WAN IP Address Assignment .....	4-2
4.3.2	IP Address and Subnet Mask .....	4-3
4.3.3	DNS Server Address Assignment .....	4-4
4.3.4	WAN Setup .....	4-4
4.4	Basic Setup Complete .....	4-4
<b>Chapter 5</b>	<b>The Advanced Screens .....</b>	<b>5-1</b>
5.1	The System Screen .....	5-1
5.1.1	General Setup .....	5-1
5.1.2	Dynamic DNS .....	5-1
5.1.3	Password .....	5-1
5.1.4	Time Zone .....	5-2
5.2	The LAN Screen .....	5-2
5.2.1	DHCP Setup .....	5-2
5.2.2	LAN TCP/IP .....	5-2
5.3	The WAN Screen .....	5-3
5.4	The SUA/NAT Screen .....	5-4
5.4.1	Introduction .....	5-4
5.4.2	The SUA Server Screen .....	5-4
5.4.3	Services and Port Numbers .....	5-4
5.4.4	Configuring Servers Behind SUA (Example) .....	5-5
5.5	The Static Route Screen .....	5-7
5.5.1	General Information About Static Routes .....	5-7
5.5.2	IP Static Route Setup .....	5-8
5.6	The Firewall Screen .....	5-8
5.6.1	Introduction .....	5-8
5.6.2	Tabs in the Firewall Screen .....	5-11
5.7	About VPN/IPSec .....	5-11
5.7.1	VPN .....	5-11
5.7.2	IPSec .....	5-12
5.7.3	Security Association .....	5-12
5.7.4	Other Terminology .....	5-12
5.8	IPSec Architecture .....	5-13
5.8.1	IPSec Algorithms .....	5-13
5.9	IPSec and NAT .....	5-14



5.10	The VPN/IPSec Screen - Fields in the VPN/IPSec Setup Tab .....	5-14
5.10.1	Active Field .....	5-14
5.10.2	IPSec Keying Mode Field .....	5-15
5.10.3	Negotiation Mode Field .....	5-15
5.10.4	Source Address Field .....	5-16
5.10.5	Destination Address Start Field .....	5-16
5.10.6	Destination Address End Field .....	5-16
5.10.7	My IP Address Field .....	5-16
5.10.8	Secure Gateway IP Address Field .....	5-16
5.10.9	Encapsulation Mode Field .....	5-17
5.10.10	IPSec Protocol Field .....	5-18
5.10.11	Pre-Shared Key Field .....	5-19
5.10.12	Encryption Algorithm Field .....	5-19
5.10.13	Authentication Algorithm Field .....	5-20
5.11	The VPN/IPSec Screen - Fields in the SA Monitor Tab .....	5-20
5.12	The VPN/IPSec Screen - Fields in the View IPSec Log Tab .....	5-21
5.12.1	Example Logs .....	5-21
5.12.2	Example Log Messages .....	5-23
<b>Chapter 6 The Maintenance Screens .....</b>		<b>6-1</b>
6.1	Introduction .....	6-1
6.2	The System Status Screen .....	6-1
6.2.1	System Status .....	6-1
6.3	The DHCP Table Screen .....	6-1
6.4	The F/W (Firmware) Upgrade Screen .....	6-1
6.5	The Configuration Screen .....	6-1
6.5.1	Backup .....	6-2
6.5.2	Restore .....	6-2
6.5.3	Default .....	6-2
<b>ADVANCED MANAGEMENT USING FTP/TFTP .....</b>		<b>III</b>
<b>Chapter 7 Firmware and Configuration File Maintenance .....</b>		<b>7-1</b>
7.1	Filename Conventions .....	7-1
7.2	Backup Configuration .....	7-2
7.2.1	Using the FTP Command from the Command Line .....	7-2
7.2.2	Example of FTP Commands from the Command Line .....	7-3
7.2.3	GUI-based FTP Clients .....	7-3
7.2.4	Backup Configuration Using TFTP .....	7-3
7.2.5	TFTP Command Example .....	7-4
7.2.6	GUI-based TFTP Clients .....	7-4
7.3	Restore or Upload a Configuration File .....	7-5
7.3.1	Restore Using FTP .....	7-5
7.3.2	Restore Using FTP Session Example .....	7-6

7.4	Uploading a Firmware File .....	7-6
7.4.1	Firmware File Upload .....	7-6
7.4.2	FTP File Upload Command from the DOS Prompt Example .....	7-6
7.4.3	FTP Session Example of Firmware File Upload .....	7-7
7.4.4	TFTP File Upload .....	7-7
7.4.5	TFTP Upload Command Example .....	7-7
<b>TROUBLESHOOTING AND ADDITIONAL INFORMATION .....</b>		<b>IV</b>
<b>Chapter 8 Troubleshooting .....</b>		<b>8-1</b>
8.1	Problems Starting Up the ZyWALL .....	8-1
8.2	Problems with the Password .....	8-1
8.3	Problems with the LAN Interface .....	8-2
8.4	Problems with the WAN Interface .....	8-2
8.5	Problems with Internet Access .....	8-3
8.6	Problems with the Firewall .....	8-3
<b>Appendix A PPPoE .....</b>		<b>A</b>
<b>Appendix B PPTP .....</b>		<b>C</b>
<b>Appendix C Power Adapter Specifications .....</b>		<b>F</b>
<b>Glossary .....</b>		<b>G</b>
<b>Index .....</b>		<b>Q</b>

# List of Figures

Figure 1-1 Internet Access Application .....	1-4
Figure 2-1 Front Panel .....	2-1
Figure 2-2 ZyWALL 1 Rear Panel Connections.....	2-2
Figure 3-1 The MAIN MENU Screen of the Web Configurator .....	3-2
Figure 3-2 Overview of the ZyWALL Web Configurator .....	3-3
Figure 5-1 Multiple Servers Behind NAT Example.....	5-6
Figure 5-2 SUA/NAT Web Configurator Screen.....	5-7
Figure 5-3 Example of Static Routing Topology .....	5-8
Figure 5-4 Encryption and Decryption.....	5-12
Figure 5-5 IPSec Architecture.....	5-13
Figure 5-6 Two Phases to set up the IPSec SA .....	5-15
Figure 5-7 Telecommuter's ZyWALL Configuration.....	5-17
Figure 5-8 Transport and Tunnel Mode IPSec Encapsulation .....	5-17
Figure 5-9 Example VPN Initiator IPSec Log .....	5-22
Figure 5-10 Example VPN Responder IPSec Log .....	5-23
Figure 7-1 FTP Session Example.....	7-3
Figure 7-2 Restore Using FTP Session Example .....	7-6
Figure 7-3 FTP Session Example of Firmware File Upload .....	7-7

## List of Tables

Table 2-1 LED Descriptions .....	2-1
Table 2-2 Ethernet Cable Requirements for LAN 10/100M Port Connections .....	2-4
Table 4-1 Private IP Address Ranges .....	4-3
Table 4-2 Example of Network Properties for LAN Servers with Fixed IP Addresses .....	4-4
Table 5-1 Services and Port Numbers.....	5-5
Table 5-2 VPN and NAT .....	5-14
Table 5-3 Telecommuter and Headquarters Configuration Example .....	5-16
Table 5-4 AH and ESP.....	5-19
Table 5-5 SA Monitor Tab Fields .....	5-20
Table 5-6 View IPSec Log Tab Fields.....	5-21
Table 5-7 Sample IKE Key Exchange Logs .....	5-24
Table 5-8 Sample IPSec Logs During Packet Transmission.....	5-25
Table 5-9 RFC-2408 ISAKMP Payload Types.....	5-26
Table 7-1 Filename Conventions .....	7-2
Table 7-2 General Commands for GUI-based FTP Clients .....	7-3
Table 7-3 General Commands for GUI-based TFTP Clients.....	7-4
Table 8-1 Troubleshooting the Start-Up of your ZyWALL.....	8-1
Table 8-2 Troubleshooting the Password.....	8-1
Table 8-3 Troubleshooting the LAN Interface.....	8-2
Table 8-4 Troubleshooting the WAN Interface .....	8-2
Table 8-5 Troubleshooting Internet Access .....	8-3
Table 8-6 Troubleshooting the Firewall.....	8-3

# 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

# Preface

## About Your Gateway

Congratulations on your purchase of the ZyWALL 1 Internet Security Gateway.

The ZyWALL 1 is a dual Ethernet broadband Internet security gateway integrated with an ICSA certified firewall and network management features designed for telecommuters or home offices and small businesses to access the Internet via cable/xDSL modem.

Your ZyWALL 1 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 the ZyWALL's management settings. Use the web configurator for actual configuration of your ZyWALL.

## About This User's Guide

This user's guide helps you connect your ZyWALL hardware, explains how to access the web configurator, gives you more detail about the features of your ZyWALL and provides some instruction on how to use FTP/TFTP for a limited number of functions. 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 ZyWALL configuration.**

## Related Documentation

### ➤ Supporting Disk

More detailed information and examples can be found in our included disk (as well as on the [zyxel.com](http://zyxel.com) web site). This disk contains information on configuring your ZyWALL for Internet Access, general and advanced FAQs, Application Notes, Troubleshooting, a reference for CI Commands and bundled software.

### ➤ Quick Start Guide

Our Quick Start Guide is designed to help you get up and running right away. It contains a detailed easy-to-follow connection diagram, default settings, handy checklists and information on setting up your network and configuring for Internet access.

### ➤ ZyXEL Web Page and FTP Server Site

You can access product certifications, release notes and firmware upgrade information at ZyXEL web and FTP sites. Refer to the *Customer Support* page for more information.

### ➤ ZyXEL Web Site

The ZyXEL download library at [www.zyxel.com](http://www.zyxel.com) contains additional support documentation.

## **Syntax Conventions**

- The ZyWALL 1 may be referred to as the ZyWALL in this guide.





---

## Part I:

---

## Getting Started

---

This section helps you connect and install your ZyWALL.



# Chapter 1

## Getting to Know Your ZyWALL

*This chapter introduces the main features and applications of the ZyWALL as well as a checklist for fast Internet access.*

### 1.1 The ZyWALL 1 Internet Security Gateway

The ZyWALL 1 is a dual Ethernet Internet Security Gateway with an integrated 4-port switch and robust network management features for Internet access via external cable/xDSL modem. Equipped with a 10Mbps Ethernet WAN port, four auto-negotiating 10/100Mbps Ethernet LAN ports and the Network Address Translation (NAT) feature, the ZyWALL is uniquely suited as a broadband Internet access sharing gateway for telecommuters and home offices.

### 1.2 Features of the ZyWALL 1

The following are the main features of the ZyWALL 1.

#### **IPSec VPN Capability**

Establish a Virtual Private Network (VPN) to connect to your (home) office using data encryption and the Internet to provide secure communications without the expense of leased site-to-site lines. The ZyWALL 1 VPN is based on the IPSec standard and is fully interoperable with other IPSec-based VPN products. The ZyWALL 1 supports 1 SA (Security Association).

#### **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 prevention, real time alerts, reports 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 transfer 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.

### **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 actual 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 client.

### **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.

### **RoadRunner Support**

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

### **Time and Date**

The ZyWALL gets the current time and date from an external server when you turn it on. The real time is then displayed in the web configurator and logs.

### **Logging and Tracing**

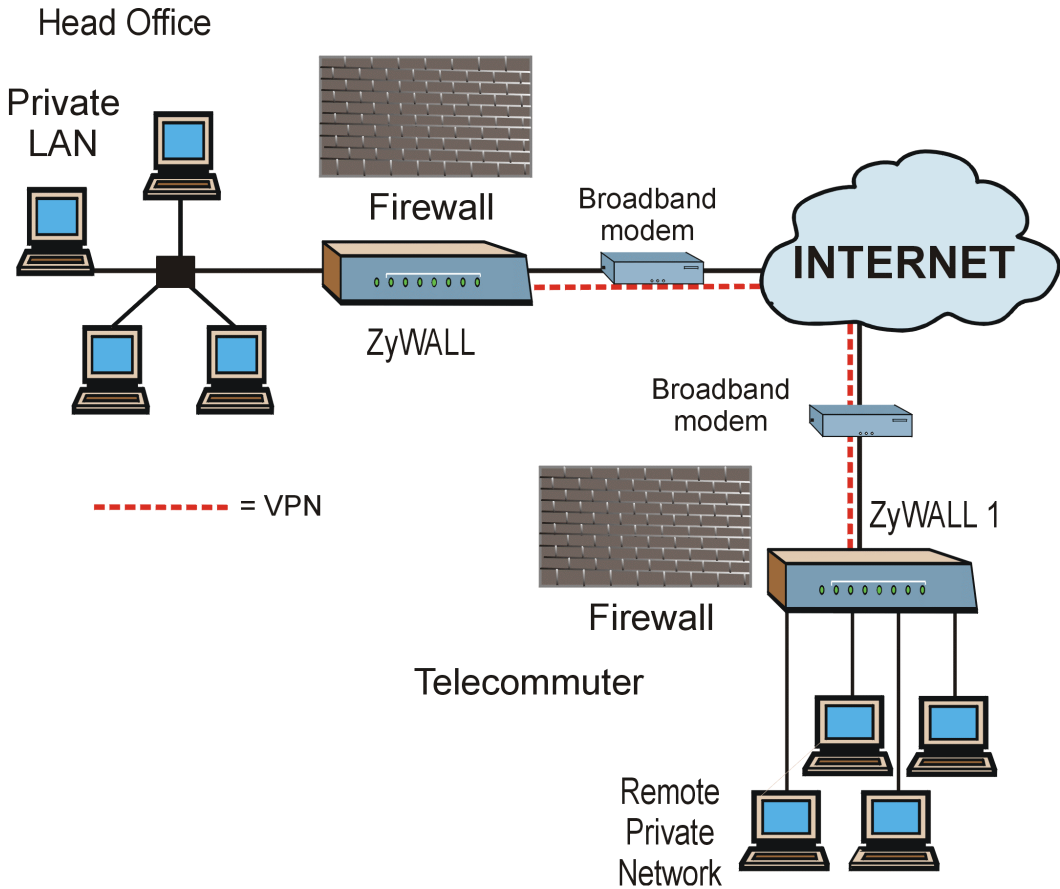
Built-in message logging and packet tracing.

### **Embedded FTP and TFTP Servers**

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

## **1.3 ZyWALL VPN Application**

A cable or DSL modem can connect to the ZyWALL for broadband Internet access via Ethernet port on the modem. It provides not only high speed Internet access, but also management features and protection for your internal network. A typical Internet access application is shown next.



**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 and Rear Panels

#### 2.1.1 Front Panel LEDs

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.

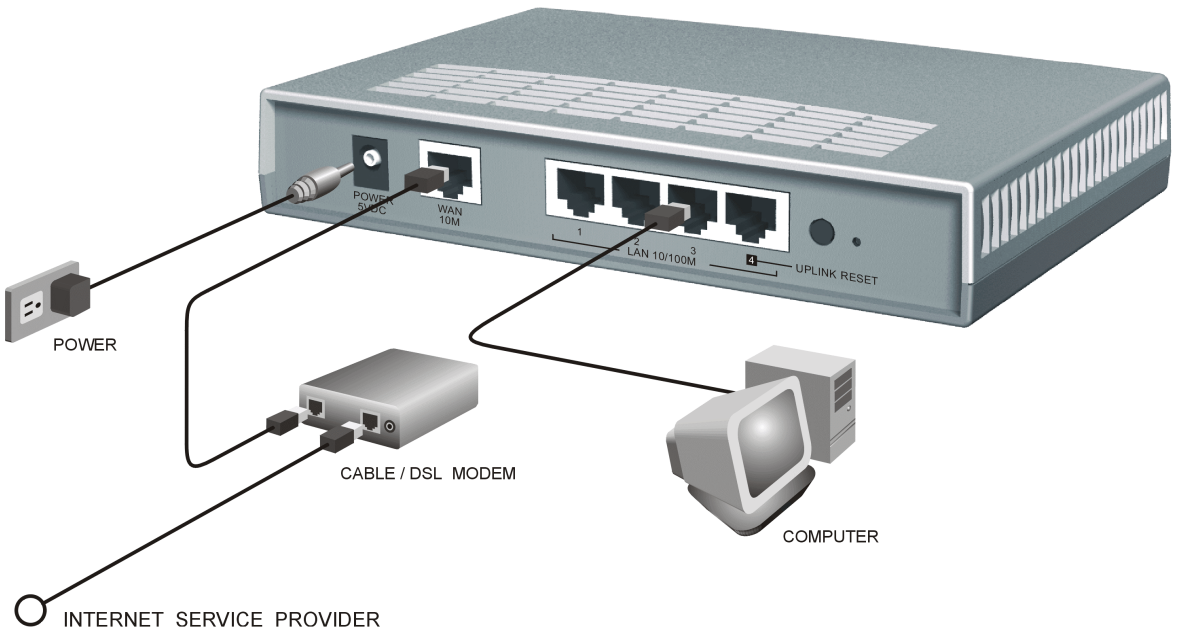
**Table 2-1 LED Descriptions**

LED	COLOR	STATUS	DESCRIPTION
SYS	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.

LED	COLOR	STATUS	DESCRIPTION
		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 1 and related connections.



**Figure 2-2 ZyWALL 1 Rear Panel Connections**



## 2.2.1 WAN 10M Port

### Connecting the ZyWALL to a Cable Modem

1. 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 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 four 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 UPLINK Button

Pushing the **UPLINK** button in ("on") lets you connect **LAN 10/100M** port 4 on the ZyWALL directly to a computer using a straight-through Ethernet cable. If the **UPLINK** button is off ("not on"), you must use a crossover Ethernet cable for this connection.

When connecting the ZyWALL **LAN 10/100M port 4** to a hub, press the **UPLINK** button in ("on") order to use a crossover Ethernet cable instead of a straight-through cable.

## 2.2.4 LAN 10/100M Connections/Uplink Button Usage at a Glance

Table 2-2 Ethernet Cable Requirements for LAN 10/100M Port Connections

LAN 10/100M PORT NUMBER	TYPE OF ETHERNET CABLE FOR CONNECTING THE ZYWALL TO A ...	
	COMPUTER	HUB
1	straight-through	crossover
2	straight-through	crossover
3	straight-through	crossover
4 UPLINK button "on"	straight-through	crossover
4 UPLINK button "off"	crossover	straight-through

## 2.2.5 POWER 5VDC Port

Connect the female 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.**

## 2.2.6 RESET Button

Refer to section 2.5 for information on the **RESET** button.

## 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 **SYS** 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 Resetting the ZyWALL

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 ZyWALL factory defaults.

- IP address: 192.168.1.1
- Password: 1234

### 2.5.1 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.

## 2.6 ZyWALL Configuration

### 2.6.1 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. Find out how to access the web configurator by reading *Chapter 3* or referring to the *Quick Start Guide*.

### 2.6.2 Using FTP/TFTP

Refer to *Chapter 7* to learn how to upload firmware and configuration files using FTP/TFTP.

### 2.6.3 Using CI Commands

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



---

## Part II:

---

### The Web Configurator Screens

---

This section introduces and describes the ZyWALL web configurator screens including MAIN MENU, WIZARD SETUP, ADVANCED and MAINTENANCE.



# Chapter 3

## Introducing the Web Configurator

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

### 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 Internet (refer to the *Preparing Your Network* portion of 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**. You should see a screen asking you to change your password (highly recommended).
- Step 6.** Type a new password (and retype it to confirm) and click **Apply** or click **Ignore**.
- Step 7.** You should now see the **MAIN MENU** screen.

Congratulations, you have successfully accessed the web configurator. Refer to the next section for a summary of how to navigate the web configurator.

**The ZyWALL gives priority of use on a "first come, first serve" basis. That is, if you have already connected to your ZyWALL via the web configurator, you will not be logged out if another user logs in and vice versa.**

**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.

Click **WIZARD SETUP** for initial configuration including general setup, ISP parameters for Internet Access and WAN IP/DNS Server/MAC address assignment.

Click **ADVANCED** to configure advanced features such as **SYSTEM** (General Setup, Dynamic DNS, Password, Time Zone), **LAN** (DHCP Setup, TCP/IP Setup), **WAN** (ISP, IP, MAC), **SUA/NAT**, **STATIC ROUTE** (Route Entry), **FIREWALL** (Log Settings, Content Filtering, Show Logs) and **VPN/IPSec** (Setup, Monitor, Logs).



Click **LOGOUT** at any time to exit the web configurator.

Click **MAINTENANCE** to view information about your ZyWALL or upgrade configuration/firmware files. Maintenance includes **SYSTEM STATUS** (Statistics), **DHCP TABLE**, **F/W** (firmware) **UPGRADE** and **CONFIGURATION** (Backup, Restore Default).

Welcome to the ZyXEL embedded web configurator.

- Click Wizard Setup to configure your system for Internet access using the factory default settings.
- Click Advanced to access a range of advanced submenus.
- Click Maintenance to access a range of Maintenance submenus.
- Click Logout to exit the web configurator.
- When in a submenu, click Main Menu (not shown here) to return to this screen.

**Figure 3-1 The MAIN MENU Screen of the Web Configurator**

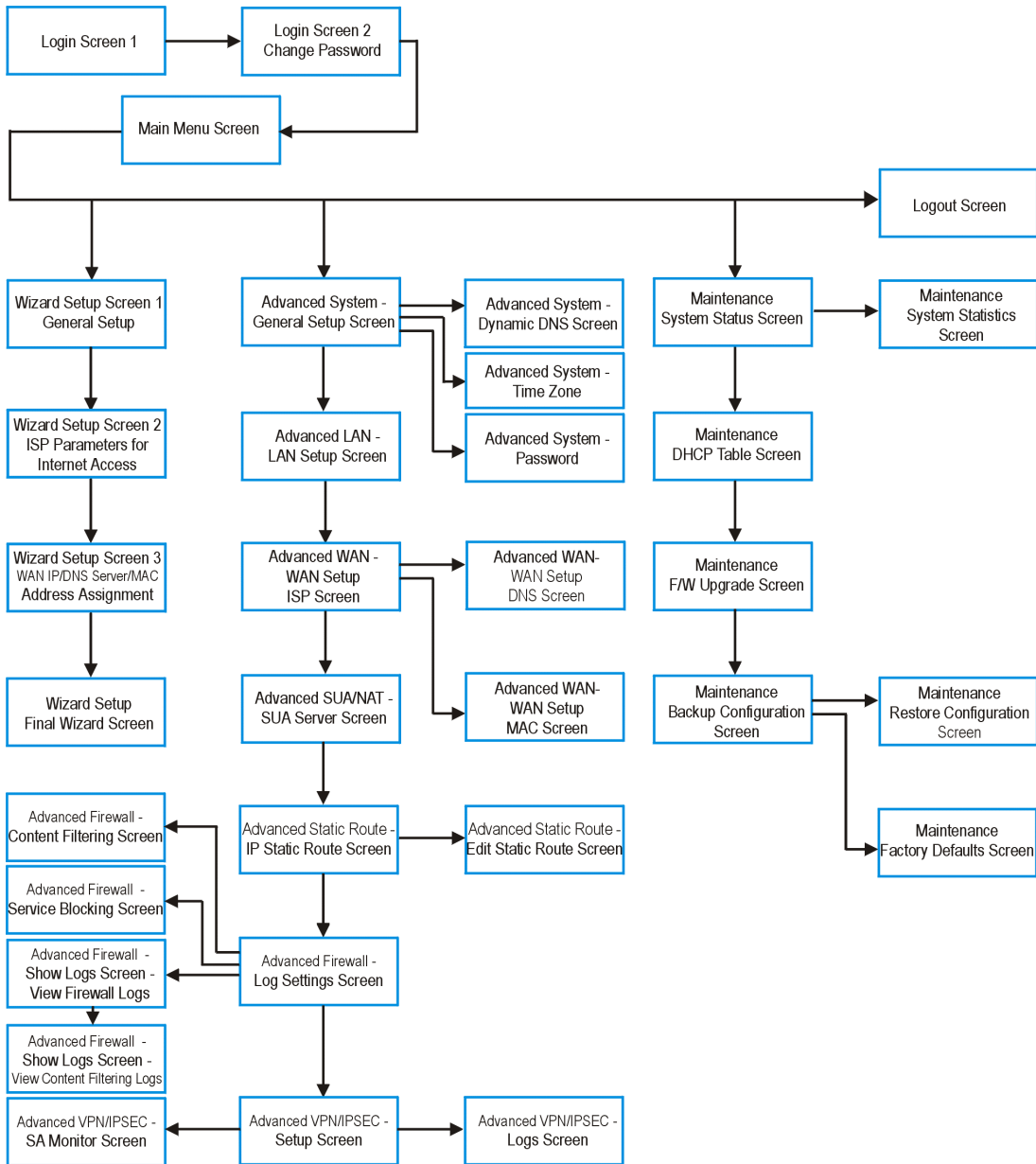
Follow the instructions you see in the MAIN MENU screen or click the  icon (located in the top right corner of most screens) to view embedded help. The  icon does not appear in the MAIN MENU screen.

If you forget your password, refer to section 2.5 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 3-2 Overview of the ZyWALL Web Configurator**



# Chapter 4

## The Wizard Setup Screens

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

### 4.1 Wizard Setup – Screen 1

#### 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 **Prestige 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.

### 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.

## 4.2.2 PPTP Encapsulation

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables 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.

For more information on PPTP, please refer to the *PPTP Appendix*.

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

## 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 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 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 access.

For more information on PPPoE, please refer to the *PPPoE Appendix*.

## 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 4-1 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 workstation 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.

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.

**Table 4-2 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)

### 4.3.4 WAN Setup

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.

## 4.4 Basic Setup Complete

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

# Chapter 5

## The Advanced Screens

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

### 5.1 The System Screen

This section briefly describes the **General**, **DDNS**, **Password** and **Time Zone** tabs in the System screen.

#### 5.1.1 General Setup

Refer to section 4.1.1.

#### 5.1.2 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) which 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.

#### **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](http://www.yourhost.dyndns.org) and still reach your hostname.

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

#### 5.1.3 Password

This screen allows you to change the ZyWALL password (recommended).

## 5.1.4 Time Zone

Use this screen to configure ZyWALL time based on your local time zone.

## 5.2 The LAN Screen

This section details DHCP setup and LAN TCP/IP in the **LAN** screen.

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

#### 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.

#### Primary and Secondary DNS Server

Refer to section 4.3.2.

### 5.2.2 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.

#### Factory LAN Defaults

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

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

#### IP Address and Subnet Mask

Refer to section 4.3.2 for this information.



## RIP Setup

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

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

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

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

## Multicast

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

IGMP (Internet Group 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. 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 (**ADVANCED->LAN**; **ADVANCED->WAN**). Select **None** to disable IP Multicasting on these interfaces.

## 5.3 The WAN Screen

This screen allows you to configure the WAN parameters of your ZyWALL. Refer to section 4.3. Read about Network Address Translation in the next section.

## 5.4 The SUA/NAT Screen

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

### 5.4.1 Introduction

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

### 5.4.2 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.**

### 5.4.3 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 5-1 Services and Port Numbers**

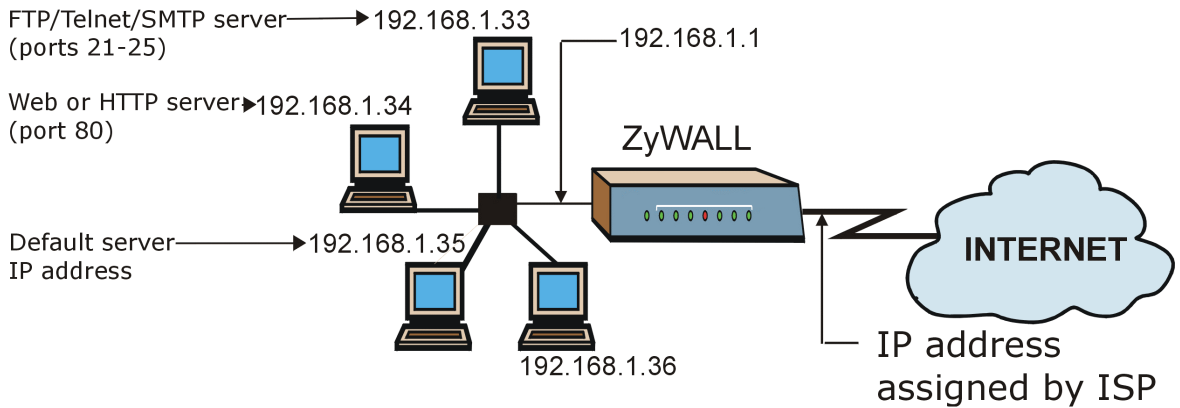
SERVICES	PORT NUMBER
ECHO	7
FTP (File Transfer Protocol)	21
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)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

#### 5.4.4 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

The NAT network appears as a single host on the Internet



**Figure 5-1 Multiple Servers Behind NAT Example**

- Step 1.** In the web configurator, click **ADVANCED**->**SUA/NAT**.
- Step 2.** Configure the SUA/NAT screen as follows.

**ZyXEL**  
TOTAL INTERNET ACCESS SOLUTION

**SUA/NAT**

MAIN MENU  
ADVANCED SYSTEM  
LAN  
WAN  
SUA/NAT  
STATIC ROUTE  
FIREWALL  
VPN/IPSEC  
LOGOUT

**SUA Server**

Default Server: 192.168.35

#	Start Port	End Port	Server IP Address
1	21	25	192.168.1.33
2	80	80	192.168.1.34
3	0	0	0.0.0.0
4	0	0	0.0.0.0
5	0	0	0.0.0.0
6	0	0	0.0.0.0
7	0	0	0.0.0.0
8	0	0	0.0.0.0
9	0	0	0.0.0.0
10	0	0	0.0.0.0

Respond to Ping on Internet WAN Port

Apply Reset

Status: Ready

Figure 5-2 SUA/NAT Web Configurator 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.**

## 5.5 The Static Route Screen

Static routes tell the ZyWALL routing information that it cannot learn automatically through other means. This can arise in cases where RIP is disabled on the LAN.

### 5.5.1 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.

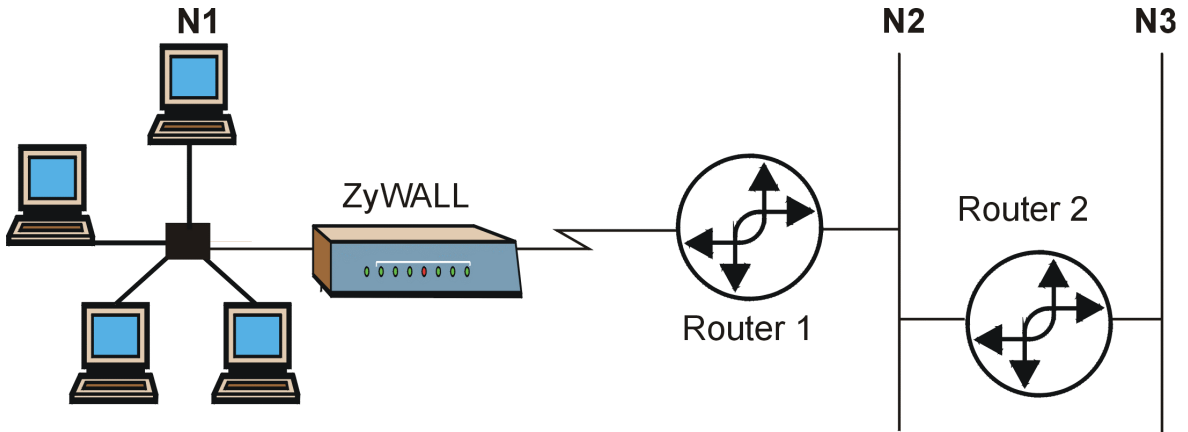


Figure 5-3 Example of Static Routing Topology

## 5.5.2 IP Static Route Setup

In the web configurator, click **ADVANCED** ->**STATIC ROUTE**. Click a static route index number, then click **Edit**. Use the embedded help to assist you in filling out the required information for each static route.

## 5.6 The Firewall Screen

This section provides a brief overview of the firewall portion of your ZyWALL using the web configurator. You can filter content, restrict services and track/maintain the functions of your firewall in this screen.

### 5.6.1 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 **ADVANCED** ->**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 be allowed (by default) unless the remote host is authorized to use a specific service.

### Guidelines For Enhancing Security With Your Firewall

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

7. Keep the firewall in a secured (locked) room.

### **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.

1. 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!
2. 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.
3. Never give out a password or any sensitive information to an unsolicited telephone call or e-mail.
4. Never e-mail sensitive information such as passwords, credit card information, etc., without encrypting the information first.
5. 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.
6. 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.
7. 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 #.
8. 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.
9. If you use “chat rooms” or IRC sessions, be careful with any information you reveal to strangers.



10. 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.
11. 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.

## 5.6.2 Tabs in the Firewall Screen

To access the tabs described next, click **ADVANCED** and then **FIREWALL**.

### Log Settings

Use this screen to activate the firewall, enter your email/mail server address information, activate Send Alert/Log features and to assign a trusted computer IP address.

### Filter (or Content Filtering)

Use this screen to enable URL keyword blocking, enter/delete/modify keywords you want to block and the date/time you want to block them.

### Services (or Service Blocking)

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.

### Logs (or Show Logs)

Use this screen to view your firewall and content filtering logs.

## 5.7 About VPN/IPSec

This section provides information about VPN/IPSec.

### 5.7.1 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.

## 5.7.2 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.

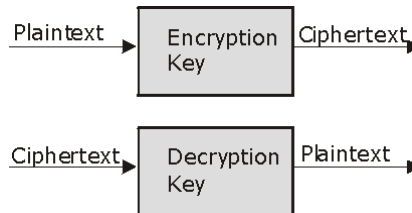
## 5.7.3 Security Association

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

## 5.7.4 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 5-4 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.

## 5.8 IPsec Architecture

The overall IPsec architecture is shown as follows.

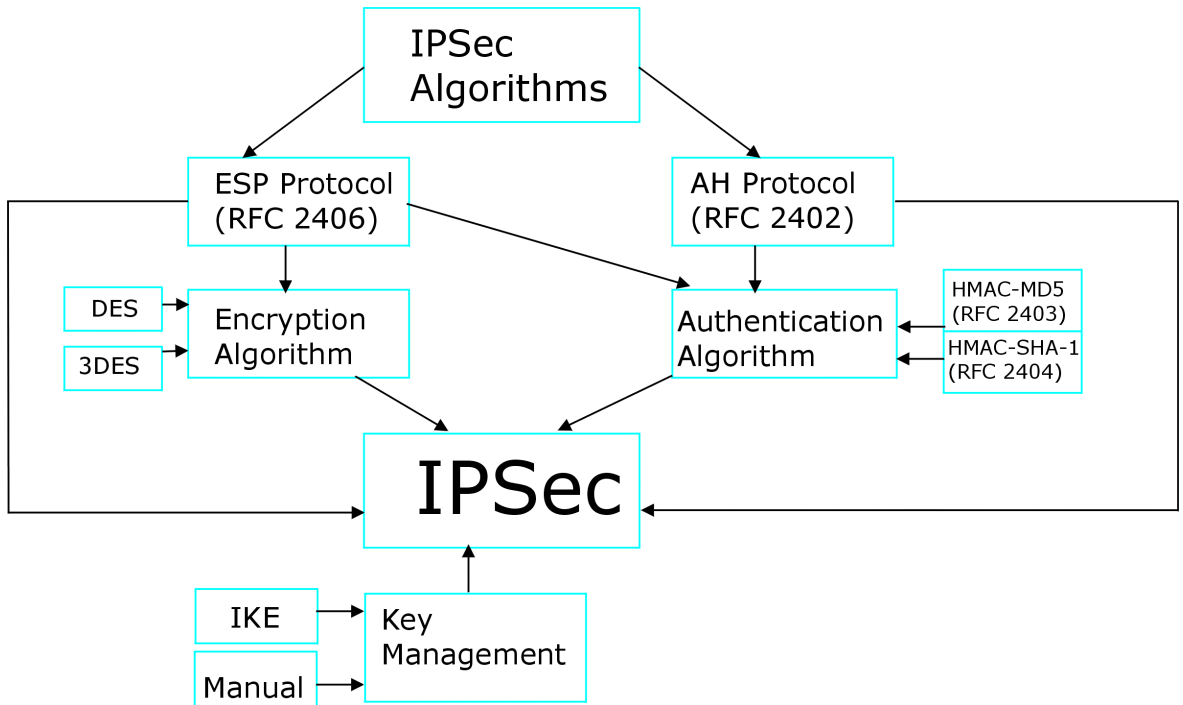


Figure 5-5 IPsec Architecture

### 5.8.1 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.

## 5.9 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.

**Table 5-2 VPN and NAT**

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

## 5.10 The VPN/IPSec Screen - Fields in the VPN/IPSec Setup Tab

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

### 5.10.1 Active Field

Select this check box to activate this VPN policy.

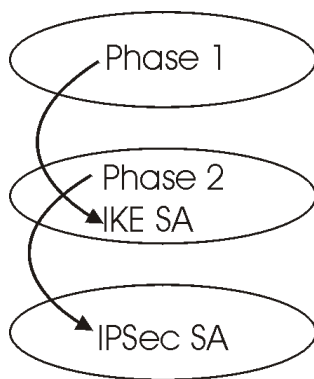
## 5.10.2 IPSec Keying Mode Field

Select **IKE** or **Manual** from the scroll down menu. **Manual** is useful for troubleshooting; **IKE** is more user friendly.

**Make sure the remote gateway has the same configuration in this field.**

### 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 (Security Association) and the second one uses that SA to negotiate SAs for IPSec.



**Figure 5-6 Two Phases to set up the IPSec SA**

## 5.10.3 Negotiation Mode Field

Select **Main** or **Aggressive** from the scroll down menu.

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 has the same configuration in this field.**

### 5.10.4 Source Address Field

Enter the IP address of the computer using the VPN IPSec feature of your ZyWALL.

### 5.10.5 Destination Address Start Field

Enter the beginning IP address (in a range) of computers on the remote network behind the remote IPSec gateway.

### 5.10.6 Destination Address End Field

Enter the end IP address (in a range) of computers on the remote network behind the remote IPSec gateway.

### 5.10.7 My IP Address Field

**My IP Addr** is the (initiator) ZyWALL 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 **My IP Addr** changes after setup, then the VPN tunnel will have to be rebuilt again.

### 5.10.8 Secure Gateway IP Address Field

**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 do 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 5-3 Telecommuter and Headquarters Configuration Example**

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

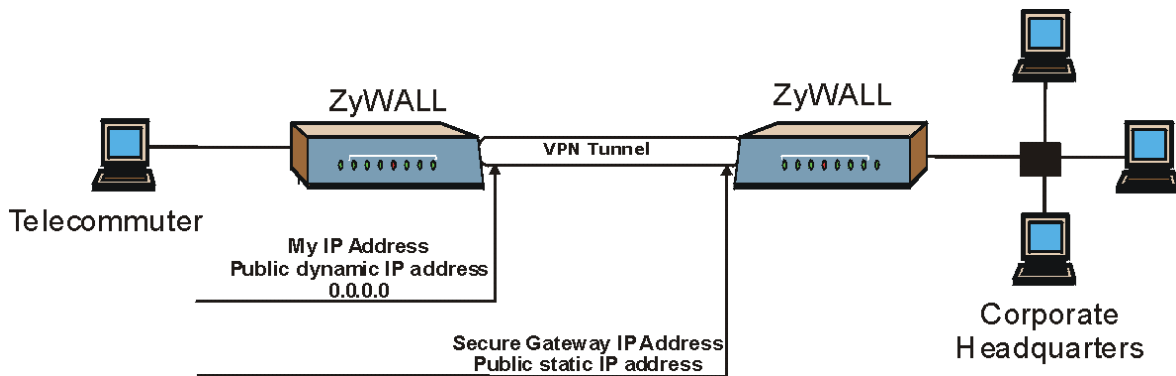


Figure 5-7 Telecommuter's ZyWALL Configuration

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

A ZyWALL with Secure Gateway IP Address set to 0.0.0.0 may receive multiple VPN connection requests using the same VPN rule at the same time.

### 5.10.9 Encapsulation Mode Field

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

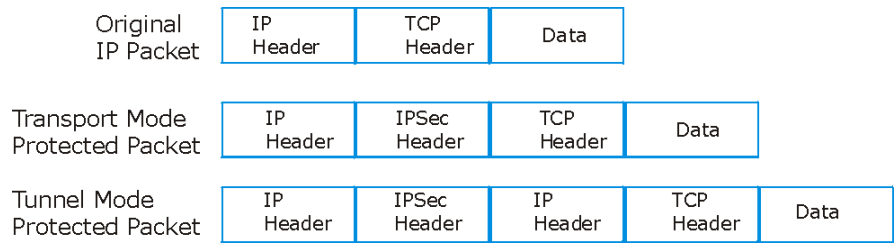


Figure 5-8 Transport and Tunnel Mode IPSec Encapsulation

### 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.

## 5.10.10 IPsec Protocol Field

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 5-4 AH and ESP**

ESP	AH
Select DES for minimal security and 3DES for maximum.	Select MD5 for minimal security and SHA-1 for maximum security.
<b>DES</b> (default) Data Encryption Standard (DES) 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.	<b>MD5</b> (default) MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.
<b>3DES</b> 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.	<b>SHA1</b> SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.

**You may configure one IPSec rule in the ZyWALL 1.**

### 5.10.11 Pre-Shared Key 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.

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.

### 5.10.12 Encryption Algorithm Field

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].

### 5.10.13 Authentication Algorithm Field

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).

Encapsulation Mode, IPSec Protocol, Pre-Shared Key, Encryption Algorithm and Authentication Algorithm **fields must contain the same parameters as your remote gateway.**

## 5.11 The VPN/IPSec Screen - Fields in the 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 the **Refresh** function to display active VPN connections. This screen is read-only. The following table describes the fields in this tab.

**An SA times out automatically after one minute if there is no traffic.**

**Table 5-5 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.	<b>Taiwan</b>
Encapsulation	This field displays <b>Tunnel</b> mode or <b>Transport</b> mode. See previous for discussion.	<b>Tunnel</b>
IPSec Algorithm	This field displays the security protocols used for an SA. <b>ESP</b> provides confidentiality and integrity of data by encrypting the data and encapsulating it into IP packets. Encryption methods include 56-bit <b>DES</b> and 168-bit <b>3DES</b> . An incoming SA may have an <b>AH</b> in addition to <b>ESP</b> . 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.	<b>ESP DES MD5</b>

FIELD	DESCRIPTION	EXAMPLE
	This provides an additional level of security. <b>AH</b> choices are <b>MD5</b> (default - 128 bits) and <b>SHA1</b> (160 bits).	

## 5.12 The VPN/IPSec Screen - Fields in the View IPSec Log Tab

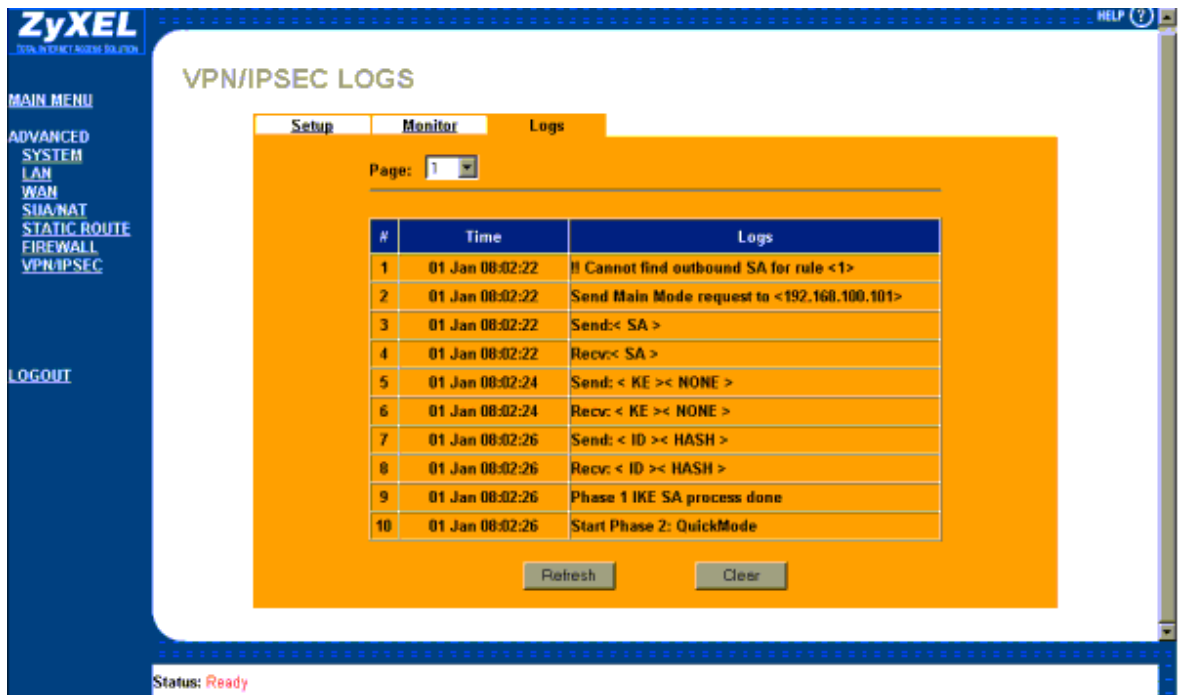
View IPSec and IKE connection logs in this screen. This screen is useful for troubleshooting. The following table describes the fields in this tab.

**Table 5-6 View IPSec Log Tab Fields**

FIELD	DESCRIPTION	EXAMPLE
Page	Select a number from the drop down list and select a number to view the corresponding page.	1
#	This is the index number of the IKE/IPSec log. 128 entries are available and are numbered from 0 to 127. Once they are all used, the log will wrap around and the old logs will be lost.	001
Time	This is the time the log was recorded in this format.	01 Jan 00:01:11
Logs	This field shows the IKE process by displaying packet exchange information. When the IKE process is successful, the VPN (IKE) tunnel will be listed in the <b>SA Monitor</b> screen.  MM means Main Mode, QM means Quick Mode and AG means Aggressive mode.	MM Receiving IKE Packet = 2
		Sending IKE Packet = 3

### 5.12.1 Example Logs

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



The screenshot displays the ZyXEL VPN/IPSEC LOGS interface. The interface has a blue header with the ZyXEL logo and a navigation menu on the left. The main content area is orange and contains a table of logs. The table has three columns: #, Time, and Logs. The logs show the process of a VPN connection, including sending and receiving SA, KE, and ID hashes, and the completion of Phase 1 and Phase 2.

**ZyXEL**  
VPN/SECURITY SOLUTION

MAIN MENU  
ADVANCED SYSTEM  
LAN  
WAN  
SNA/NAT  
STATIC ROUTE  
FIREWALL  
VPN/IPSEC  
LOGOUT

VPN/IPSEC LOGS

Setup Monitor Logs

Page: 1

#	Time	Logs
1	01 Jan 08:02:22	!! Cannot find outbound SA for rule <1>
2	01 Jan 08:02:22	Send Main Mode request to <192.168.100.101>
3	01 Jan 08:02:22	Send:< SA >
4	01 Jan 08:02:22	Recv:< SA >
5	01 Jan 08:02:24	Send: < KE >< NONE >
6	01 Jan 08:02:24	Recv: < KE >< NONE >
7	01 Jan 08:02:26	Send: < ID >< HASH >
8	01 Jan 08:02:26	Recv: < ID >< HASH >
9	01 Jan 08:02:26	Phase 1 IKE SA process done
10	01 Jan 08:02:26	Start Phase 2: QuickMode

Refresh Clear

Status: Ready

**Figure 5-9 Example VPN Initiator IPsec Log**

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

The screenshot displays the ZyWALL 1 Internet Security Gateway interface. On the left is a blue sidebar with a 'MAIN MENU' containing options like ADVANCED SYSTEM, LAN, WAN, SUA/NAT, STATIC ROUTE, FIREWALL, and VPN/IPSEC. The main content area is titled 'VPN/IPSEC LOGS' and has three tabs: 'Setup', 'Monitor', and 'Logs'. The 'Logs' tab is active, showing a table of log entries. Below the table are 'Refresh' and 'Clear' buttons. At the bottom left, the status is 'Ready'.

#	Time	Logs
1	01 Jan 08:08:07	Recv Main Mode request from <192.168.100.100>
2	01 Jan 08:08:07	Recv: < SA >
3	01 Jan 08:08:08	Send: < SA >
4	01 Jan 08:08:08	Recv: < KE >< NONE >
5	01 Jan 08:08:10	Send: < KE >< NONE >
6	01 Jan 08:08:10	Recv: < ID >< HASH >
7	01 Jan 08:08:10	Send: < ID >< HASH >
8	01 Jan 08:08:10	Phase 1 IKE SA process done
9	01 Jan 08:08:10	Recv: < HASH >< SA >< NONE >< ID >< ID >
10	01 Jan 08:08:10	Start Phase 2: QuickMode

Figure 5-10 Example VPN Responder IPsec Log

### 5.12.2 Example Log Messages

Log messages are useful for troubleshooting. The following tables help explain the logs in *Figure 5-9* and *Figure 5-10*.

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

The following tables show example log messages during IKE key exchange.

**Table 5-7 Sample IKE Key Exchange Logs**

LOG MESSAGE	DESCRIPTION
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.
Send Main Mode request to <IP> Send Aggressive Mode request to <IP>	The ZyWALL has started negotiation with the peer.
Recv Main Mode request from <IP> Recv Aggressive Mode request from <IP>	The ZyWALL has received an IKE negotiation request from the peer.
Send:<Symbol><Symbol> Recv:<Symbol><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 <i>Table 5-9</i> .
Phase 1 IKE SA process done	Phase 1 negotiation is finished.
Start Phase 2: Quick Mode	Phase 2 negotiation is beginning using Quick Mode.
!! 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

**Table 5-7 Sample IKE Key Exchange Logs**

LOG MESSAGE	DESCRIPTION
	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.

The following table shows sample log messages during packet transmission.

**Table 5-8 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 ZyWALL will use the current ZyWALL WAN IP address (static or dynamic) to set up the VPN tunnel.
!! Cannot find Phase 2 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.
!! 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	The decryption configuration settings are incorrect. Please check

**Table 5-8 Sample IPSec Logs During Packet Transmission**

LOG MESSAGE	DESCRIPTION
failed	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.

**Table 5-9 RFC-2408 ISAKMP Payload Types**

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



# Chapter 6

## The Maintenance Screens

*This chapter briefly describes the Maintenance screens in the web configurator.*

### 6.1 Introduction

The web configurator allows easy maintenance of your ZyWALL and is recommended for all users. If you prefer to maintain your ZyWALL via FTP/TFTP, refer to *Chapter 7*. Advanced users may use the CI commands included in the support notes.

The following are Maintenance screens located in the web configurator. From the **MAIN MENU**, click **MAINTENANCE** and the appropriate link to access each of the following screens.

### 6.2 The System Status Screen

Read-only information here includes system name, ZyNOS firmware version and routing protocols. Also provided are the IP address, DHCP status and IP subnet mask of both the LAN and WAN.

#### 6.2.1 System Status

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.

### 6.3 The DHCP Table Screen

Read-only information here relates to your DHCP status. The DHCP table shows current DHCP Client information (including IP Address, Host name and MAC Address) of all network clients using the DHCP server.

### 6.4 The F/W (Firmware) Upgrade Screen

Follow the instructions in this screen to upload firmware to your ZyWALL.

### 6.5 The Configuration Screen

**Backup**, **Restore** and **Default** tabs are located in the **CONFIGURATION** screen. Follow the instructions in each screen to perform the action described next.

### 6.5.1 Backup

This screen backs up your current ZyWALL configuration to your computer.

### 6.5.2 Restore

This screen restores a previously saved configuration file from your computer to your ZyWALL.

### 6.5.3 Default

This screen clears all user-entered configuration information and returns the ZyWALL to its factory defaults. You can also press the **RESET** button on the rear panel to reset the factory defaults of your ZyWALL. Refer to *section 2.5* for more information on the **RESET** button.

---

## Part III:

---

### Advanced Management Using FTP/TFTP

---

This section provides information on Firmware and Configuration File Maintenance using FTP/TFTP.



# Chapter 7

## Firmware and Configuration File Maintenance

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

It is strongly recommended that you use the web configurator to perform functions mentioned in this chapter (refer to *Chapter 6*). The web configurator is less technical and more intuitive than using FTP/TFTP. Refer to *Chapter 3* to connect to the web configurator. If you wish use FTP/TFTP, then follow the instructions in this chapter.

### 7.1 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 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 7-1 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.

## 7.2 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.

### 7.2.1 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.

## 7.2.2 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 7-1 FTP Session Example**

## 7.2.3 GUI-based FTP Clients

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

**Table 7-2 General Commands for GUI-based FTP Clients**

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	<p>Anonymous.</p> <p>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.</p> <p>Normal.</p> <p>The server requires a unique User ID and Password to login.</p>
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).

## 7.2.4 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.**

## 7.2.5 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 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.

## 7.2.6 GUI-based TFTP Clients

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

**Table 7-3 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.



## 7.3 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.**

### 7.3.1 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.

## 7.3.2 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 7-2 Restore Using FTP Session Example**

## 7.4 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 7.3.

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

### 7.4.1 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.

### 7.4.2 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").
- Step 5.** Enter "bin" to set transfer mode to binary.
- Step 6.** Use "put" to transfer files from the computer to the ZyWALL, for example, "put firmware.bin ras" transfers the firmware on your computer (firmware.bin) to the ZyWALL and renames it "ras". See earlier in this chapter for more information on filename conventions.
- Step 7.** Enter "quit" to exit the ftp prompt.

### 7.4.3 FTP Session Example of Firmware File Upload

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 type I OK
ftp> put firmware.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 1103936 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

**Figure 7-3 FTP Session Example of Firmware File Upload**

More commands (found in GUI-based FTP clients) are listed earlier in this chapter.

### 7.4.4 TFTP File Upload

The ZyWALL also supports the uploading of firmware files using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To transfer the firmware and 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 example below) to transfer files between the ZyWALL and the computer. The file name for the firmware is "ras".

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.

### 7.4.5 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.



---

## PART IV:

---

### Troubleshooting and Additional Information

---

This section provides information about solving common problems, some Appendices, as well as a Glossary and Index.



# Chapter 8

## 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.*

### 8.1 Problems Starting Up the ZyWALL

**Table 8-1 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>

### 8.2 Problems with the Password

**Table 8-2 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 section 2.5.1.
	If the error persists, you may have a hardware problem. In this case, you should contact your vendor.

## 8.3 Problems with the LAN Interface

**Table 8-3 Troubleshooting the LAN Interface**

PROBLEM	CORRECTIVE ACTION
I cannot access the ZyWALL from the LAN.	Check your Ethernet cable type and connections. Refer to section 2.2 for LAN connection instructions.  Make sure your NIC (Network Interface Card) is installed and functioning properly.
I cannot ping any computer on the LAN.	If all of the 10/100M LAN LEDs are off, check the cables between the ZyWALL and your computer or hub.  Verify that the IP addresses and subnet masks of the ZyWALL and the computers on the LAN are on the same subnet.

## 8.4 Problems with the WAN Interface

**Table 8-4 Troubleshooting the WAN Interface**

PROBLEM	CORRECTIVE ACTION
I cannot get a WAN IP address from the ISP.	The WAN IP is provided after the ISP verifies the MAC address, host name or user ID.  Find out the verification method used by your ISP.  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.  If the ISP does not allow you to use a new MAC, click <b>ADVANCED, 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.  If the ISP checks the host name, enter your computer's name (refer to Chapter 4 in the User's Guide) in the <b>System Name</b> field in the first screen of the <b>WIZARD SETUP</b> .  If the ISP checks the user ID, click <b>ADVANCED, WAN</b> and the <b>ISP</b> tab. Check your service type, user name, and password.



## 8.5 Problems with Internet Access

**Table 8-5 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 <b>ADVANCED</b> and then <b>WAN</b> and verify your settings.</p>

## 8.6 Problems with the Firewall

**Table 8-6 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>ADVANCED</b>-&gt; <b>FIREWALL</b>-&gt; <b>SERVICES</b> to review what services are currently blocked.</p>



# 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) which connects to a 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:

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

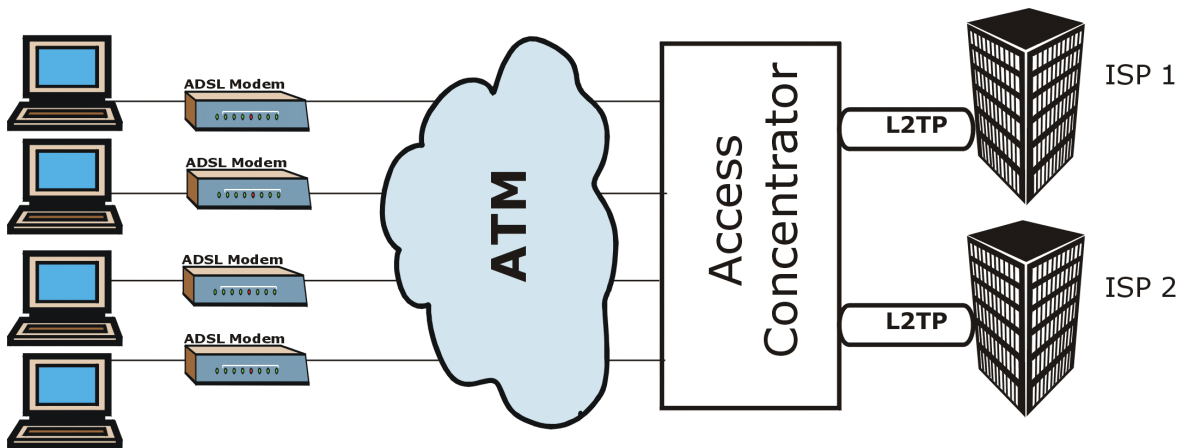


Diagram 1 Single-PC per Modem Hardware Configuration

### 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.

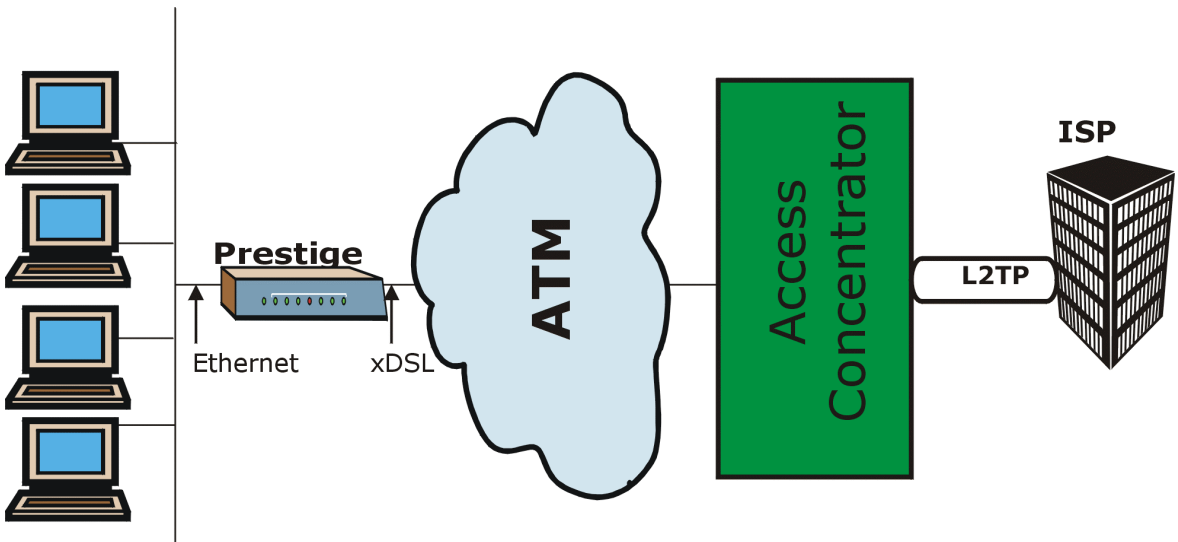


Diagram 2 ZyWALL as a PPPoE Client

# Appendix B

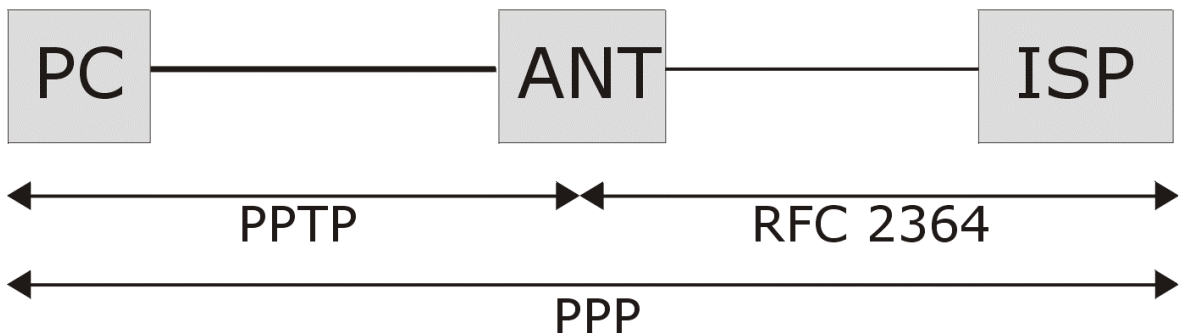
## PPTP

### 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**

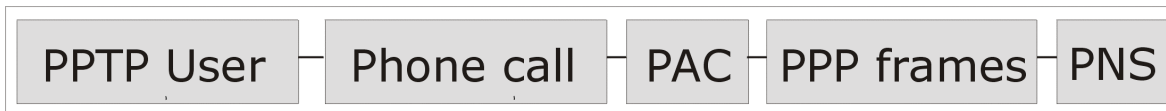
### PPTP and the ZyWALL

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.

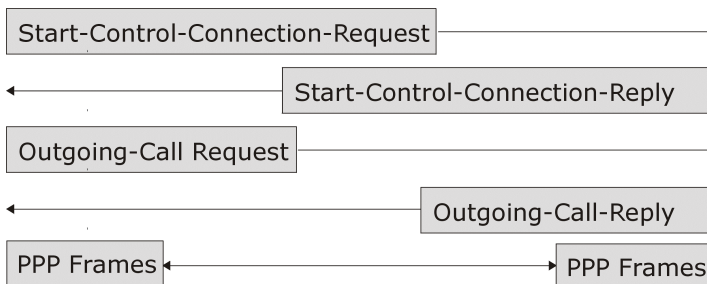
## Control and PPP Connections

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

## 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	12w
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



# Glossary

<b>100Base-T</b>	The 100-Mbps baseband Ethernet specification uses two pairs of twisted-pair wire with a maximum distance of 100 meters between the hub and the workstation.
<b>10Base-S Mode</b>	This is a VDSL mode. Each mode operates in a specific frequency band allocation with associated upstream and downstream speeds.
<b>10Base-T</b>	Twisted-pair cable with maximum segment lengths of 100 meters.
<b>A</b>	
<b>ADSL</b>	Asymmetrical Digital Subscriber Line is an asymmetrical technology which means that the downstream data rate of the line is much higher than the upstream data rate. ADSL operates in a frequency range that is above the frequency range of voice services, so the two systems can operate over the same cable.
<b>AH</b>	Authentication Header (RFC 2402) is a protocol that IPSec uses to verify integrity of a data packet (including the header) and the identity of it's sender.
<b>ARP</b>	Address Resolution Protocol is a protocol for mapping an Internet Protocol address (IP address) to a physical computer address that is recognized in the local network.
<b>ATM</b>	Asynchronous Transfer Mode. ATM is a LAN and WAN networking technology that provides high-speed data transfer. ATM uses fixed-size packets of information called cells. With ATM, a high QoS (Quality of Service) can be guaranteed.
<b>Authentication Algorithm</b>	This is an established, step-by-step procedure for verifying the identity of a packet's sender.
<b>B</b>	
<b>Bandwidth</b>	This is the capacity on a link usually measured in bits-per-second (bps).
<b>Bit</b>	A Binary Digit (either a one or a zero); a single digit number in base-2. A bit is the smallest unit of computerized data.
<b>Boot Module Commands</b>	Boot Module Commands, available in the debug mode via SMT (some devices may not have SMTs), help you initialize the configuration of the basic functions and features of your device(s) such as uploading firmware, changing the console port speed and viewing product-related information.
<b>Brute Force Hacking</b>	A technique used to find passwords or encryption keys. Force Hacking involves trying every possible combination of letters, numbers, etc., until the code is broken.

<b>Byte</b>	A set of bits that represent a single character. There are eight bits in a byte.
<b>C</b>	
<b>Command Line Interface</b>	A command line interface is a computer environment in which you enter predefined commands on the command line to modify, configure and display information about a device or devices. A command line is the line on the display screen where a command is expected. Generally, the command line is the line that contains the most recently displayed command prompt. An interface is a set of commands (for example, a ZyXEL Command Line Interface) or menus (for example, a ZyXEL web configurator) used to communicate with a program. A command-driven interface is an interface in which you enter commands.
<b>Crossover Ethernet Cable</b>	A cable that wires a pin to its opposite pin, for example, RX+ is wired to TX+. This cable connects two similar devices, for example, two data terminal equipment (DTE) or data communications equipment (DCE) devices.
<b>DES</b>	Data Encryption Standard is a widely-used method of data encryption that uses a private (secret) key. DES applies a 56-bit key to each 64-bit block of data.
<b>DHCP</b>	Dynamic Host Configuration Protocol automatically assigns IP addresses to clients when they log on. DHCP centralizes IP address management on central computers that run the DHCP server program. DHCP leases addresses, for a period of time, which means that past addresses are "recycled" and made available for future reassignment to other systems.
<b>Diffie-Hellman (DH)</b>	Diffie-Hellman 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.
<b>DNS</b>	Domain Name System links names to IP addresses. When you access Web sites on the Internet you can type the IP address of the site or the DNS name. When you type a domain name in a Web browser a query is sent to the primary DNS server defined in your Web browser's configuration dialog box. The DNS server converts the name you specified to an IP address and returns this address to your system. Thereafter, the IP address is used in all subsequent communications.
<b>Domain Name</b>	The unique name that identifies an Internet site. Domain Names always have two or more parts that are separated by dots. The part on the left is the most specific and the part on the right is the most general.
<b>E</b>	
<b>Encryption</b>	An Encryption Algorithm describes the use of encryption techniques such as DES

<b>Algorithm</b>	(Data Encryption Standard) and Triple DES algorithms.
<b>Encryption Algorithm</b>	An Encryption Algorithm describes the use of encryption techniques such as DES (Data Encryption Standard) and Triple DES algorithms.
<b>ESP</b>	Encapsulating Security Payload (RFC 2406) is a protocol that IPSec uses to encrypt data to ensure confidentiality.
<b>ESP</b>	Encapsulating Security Payload (RFC 2406) is a protocol that IPSec uses to encrypt data to ensure confidentiality.
<b>Ethernet</b>	A very common method of networking computers in a LAN. There are a number of adaptations to the IEEE 802.3 Ethernet standard, including adaptations with data rates of 10 Mbits/sec and 100 Mbits/sec over coaxial cable, twisted-pair cable and fiber-optic cable. The latest version of Ethernet, Gigabit Ethernet, has a data rate of 1 Gbit/sec.
<b>F</b>	
<b>Firewall</b>	A hardware or software "wall" that restricts access in and out of a network. Firewalls are most often used to separate an internal LAN or WAN from the Internet.
<b>FTP</b>	File Transfer Protocol is an Internet file transfer service that operates on the Internet and over TCP/IP networks. FTP is basically a client/server protocol in which a system running the FTP server accepts commands from a system running an FTP client. The service allows users to send commands to the server for uploading and downloading files. FTP is popular on the Internet because it allows for speedy transfer of large files between two systems.
<b>G</b>	
<b>Gateway</b>	A gateway is a computer system or other device that acts as a translator between two systems that do not use the same communication protocols, data formatting structures, languages, and/or architecture.
<b>GSTN</b>	A GSTN (General Switched Telephone Network) denotes an analog network (PSTN) or digital network (ISDN).
<b>H</b>	
<b>Hash</b>	This is a type of encryption that transforms plain text input into encrypted output of a fixed length called the message digest.
<b>Host</b>	Any computer on a network that is a repository for services available to other computers on the network. It is quite common to have one host machine provide

	several services, such as WWW and USENET.
<b>HTTP</b>	Hyper Text Transfer Protocol. The most common protocol used on the Internet. HTTP is the primary protocol used for web sites and web browsers. It is also prone to certain kinds of attacks.
<b>I</b>	
<b>IANA</b>	Internet Assigned Number Authority acts as the clearing house to assign and coordinate the use of numerous Internet protocol parameters such as Internet addresses, domain names, protocol numbers, and more. Use a search engine to find the current IANA web site.
<b>ICMP</b>	Internet Control Message Protocol is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and are not directly apparent to the application user.
<b>IKE</b>	Internet Key Exchange is a two-phase security negotiation and key management service – 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.
<b>Internet</b>	(Upper case "I"). The vast collection of inter-connected networks that use TCP/IP protocols evolved from the ARPANET (Advanced Research Projects Agency Network) of the late 1960's and early 1970's.
<b>internet</b>	(Lower case "i"). Any time you connect two or more networks together, you have an internet.
<b>Intranet</b>	A private network inside a company or organization that uses the same kinds of software that you would find on the public Internet, but that is only for internal use.
<b>IP</b>	Internet Protocol. (Currently IP version 4 or IPv4). The underlying protocol for routing packets on the Internet and other TCP/IP-based networks.
<b>IP Pool</b>	Internet Protocol Pool refers to the collective group of IP addresses located in any particular place (for example, LAN, WAN, Ethernet, etc.).
<b>IPSec</b>	Internet Protocol Security is a standards-based VPN (Virtual Private Network) 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.
<b>IPSec</b>	Internet Protocol Security is a standards-based VPN (Virtual Private Network) 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.
<b>ISP</b>	Internet Service Providers provide connections into the Internet for home users and businesses. There are local, regional, national, and global ISPs. You can think of local ISPs as the gatekeepers into the Internet.
<b>J</b>	
<b>K</b>	
<b>Keys</b>	Keys are used like passwords to lock and unlock messages with encryption and authentication functions. While encryption algorithms are often well known and published, the key must be kept secret.
<b>L</b>	
<b>LAN</b>	Local Area Network is a shared communication system to which many computers are attached. A LAN, as its name implies, is limited to a local area. This has to do more with the electrical characteristics of the medium than the fact that many early LANs were designed for departments, although the latter accurately describes a LAN as well. LANs have different topologies, the most common being the linear bus and the star configuration.
<b>LED</b>	Light Emitting Diode. LEDs are visual indicators that relay information about the status of specific device functions to the user by lighting up, turning off or blinking. LEDs are usually found on the front panel of the physical device. Examples include Status, Power and System LEDs.
<b>M</b>	
<b>MAC</b>	On a local area network (LAN) or other network, the MAC (Media Access Control) address is a computer's unique hardware number. (On an Ethernet LAN, it's the same as your Ethernet address). The MAC layer frames data for transmission over the network, then passes the frame to the physical layer interface where it is transmitted as a stream of bits.
<b>MD5</b>	Message Digest 5, HMAC-MD5 (RFC 2403) is a hash algorithm used to verify the identity of a data packet's source.
<b>N</b>	
<b>Name Resolution</b>	The allocation of an IP address to a host name. See also DNS.
<b>NAT</b>	Network Address Translation is the translation of an Internet Protocol address used

	within one network to a different IP address known within another network - see also SUA.
<b>NetBIOS</b>	Network Basic Input/Output System. NetBIOS is an extension of the DOS BIOS that enables a computer to connect to and communicate with a LAN.
<b>Network</b>	Any time you connect two or more computers together, allowing them to share resources, you have a computer network. Connect two or more networks together and you have an internet.
<b>NIC</b>	Network Interface Card. A board that provides network communication capabilities to and from a computer system. Also called an adapter.
<b>O</b>	
<b>P</b>	
<b>PAC</b>	The PPTP Access Concentrator (PAC) is the box that calls/answers the phone call and relays the PPP frames to the PNS (PPTP Network Server). A PAC must have IP and dial-up capability.
<b>Perfect Forward Secrecy</b>	Perfect Forward Secrecy (PFS) is an IPSec keying method that uses a brand new key for each new IPSec SA setup. The keys are created by new key exchanges, see Diffie-Hellman.
<b>POP</b>	Post Office Protocol. This is a common protocol used for sending, receiving, and delivering mail messages.
<b>Port</b>	An Internet port refers to a number that is part of a URL, appearing after a colon (:), directly following the domain name. Every service on an Internet server listens on a particular port number on that server. Most services have standard port numbers, for instance Web servers normally listen on port 80.
<b>Port (H/W)</b>	An interface on a computer for connecting peripherals or devices to the computer. A printer port, for example, is an interface that is designed to have a printer connected to it. Ports can be defined by specific hardware (such as a keyboard port) or through software.
<b>POTS</b>	Plain Old Telephone Service is the analog telephone service that runs over copper twisted-pair wires and is based on the original Bell telephone system. Twisted-pair wires connect homes and businesses to a neighborhood central office. This is called the local loop. The central office is connected to other central offices and long-distance facilities.
<b>PPP</b>	Point to Point Protocol. PPP encapsulates and transmits IP (Internet Protocol)

	datagrams over serial point-to-point links. PPP works with other protocols such as IPX (Internetwork Packet Exchange). The protocol is defined in IETF (Internet Engineering Task Force) RFC 1661 through 1663. PPP provides router-to-router, host-to-router, and host-to-host connections.
<b>PPPoE</b>	PPPoE (Point-to-Point Protocol over Ethernet) relies on two widely accepted standards: PPP and Ethernet. PPPoE is a specification for connecting the users on an Ethernet to the Internet through a common broadband medium, such as a single DSL line, wireless device or cable modem. All the users over the Ethernet share a common connection, so the Ethernet principles supporting multiple users in a LAN combine with the principles of PPP, which apply to serial connections. From authentication, accounting and secure access to configuration management, PPPoE supports a broad range of existing applications and services.
<b>PPTP</b>	Point-to-Point Tunneling Protocol.
<b>Protocol</b>	A "language" for communicating on a network. Protocols are sets of standards or rules used to define, format and transmit data across a network. There are many different protocols used on networks. For example, most web pages are transmitted using the HTTP protocol.
<b>PSTN</b>	Public Switched Telephone Network was put into place many years ago as a voice telephone call-switching system. The system transmits voice calls as analog signals across copper twisted cables from homes and businesses to neighborhood COs (central offices); this is often called the local loop. The PSTN is a circuit-switched system, meaning that an end-to-end private circuit is established between caller and the person called.
<b>Q</b>	
<b>QoS</b>	Quality of Service refers to both a network's ability to deliver data with minimum delay, and the networking methods used to provide bandwidth for real-time multimedia applications.
<b>R</b>	
<b>ras</b>	This is the name of the firmware on the ZyXEL device. Renaming may be necessary when uploading new firmware to the device.
<b>RFC</b>	An RFC (Request for Comments) is an Internet formal document or standard that is the result of committee drafting and subsequent review by interested parties. Some RFCs are informational in nature. Of those that are intended to become Internet standards, the final version of the RFC becomes the standard and no further comments or changes are permitted. Change can occur, however, through subsequent RFCs.

<b>RIP</b>	Routing Information Protocol is an interior or intra-domain routing protocol that uses distance-vector routing algorithms. RIP is used on the Internet and is common in the NetWare environment as a method for exchanging routing information between routers.
<b>Rom-0</b>	This is the name of the configuration file on your ZyXEL device. Renaming may be necessary when uploading a new configuration file to your ZyXEL device.
<b>Router</b>	A device that connects two networks together. Routers monitor, direct and filter information that passes between these networks. Because of their location, routers are a good place to install traffic or mail filters. Routers are also prone to attacks because they contain a great deal of information about a network.
<b>S</b>	
<b>SA</b>	A Security Association (SA) is a contract between two parties indicating what security parameters, such as keys and algorithms they will use.
<b>SHA1</b>	Secure Hash Algorithm HMAC-SHA-1 (RFC 2404), is a hash algorithm used to verify the identity of a data packet's source.
<b>SNMP</b>	Simple Network Management Protocol is a popular management protocol defined by the Internet community for TCP/IP networks. It is a communication protocol for collecting information from devices on the network.
<b>Static Routing</b>	Static routes tell routing information that a networking device cannot learn automatically through other means. The need for static routing can arise in cases where RIP is disabled on the LAN or a remote network is beyond the one that is directly connected to a remote node.
<b>STP</b>	Shielded Twisted-Pair cable consists of copper-core wires surrounded by an insulator. Two wires are twisted together to form a pair; the pair form a balanced circuit. The twisting prevents interference problems, STP provides protection against external crosstalk.
<b>Straight-through Ethernet cable</b>	A cable that wires a pin to its equivalent pin. This cable connects two dissimilar devices, for example, a data terminal equipment (DTE) device and a data communications equipment (DCE) device. A straight through Ethernet cable is the most commonly used Ethernet cable.
<b>SUA</b>	Single User Account. Your system's SUA feature allows multiple user Internet access for the cost of a single ISP account. See also NAT.
<b>Subnet Mask</b>	The subnet mask specifies the network number portion of an IP address. Your device



	will compute the subnet mask automatically based on the IP Address that you entered. You do not need to change the computer subnet mask unless you are instructed to do so.
<b>T</b>	
<b>TCP</b>	Transmission Control Protocol is a connection-oriented transport service that ensures the reliability of message delivery. It verifies that messages and data were received.
<b>Terminal</b>	A device that allows you to send commands to a computer somewhere else. At a minimum, this usually means a keyboard, display screen and some simple circuitry.
<b>Terminal Software</b>	Software that pretends to be (emulates) a physical terminal and allows you to type commands to a computer somewhere else.
<b>TFTP</b>	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP (File Transfer Protocol), but it is scaled back in functionality so that it requires fewer resources to run. TFTP uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
<b>Transport</b>	IPSec uses transport mode to protect upper layer protocols and affects only the data in the IP packet. 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).
<b>Triple DES</b>	This is a stronger variant of DES (Data Encryption Standard). Triple DES is a widely-used method of data encryption that applies three separate private (secret) 56-bit keys to each 64-bit block of data.
<b>Tunnel</b>	IPSec uses tunnel mode to encapsulate the entire IP packet and transmit it securely. Tunnel mode is fundamentally an IP tunnel with authentication and encryption and is required for gateway services to provide access to internal systems.
<b>Twisted Pair</b>	Two insulated wires, usually copper, twisted together and often bound into a common sheath to form multi-pair cables. In ISDN, the cables are the basic path between a subscriber's terminal or telephone and the PBX or the central office.
<b>U</b>	
<b>UDP</b>	User Datagram Protocol. DP is a connectionless transport service that dispenses with the reliability services provided by TCP. UDP gives applications a direct interface with the Internet Protocol (IP) and the ability to address a particular application process running on a host via a port number without setting up a connection session.
<b>UNIX</b>	A widely-used operating system in large networks. Usually used on workstations and

	servers.
<b>V</b>	
<b>W</b>	
<b>WAN</b>	Wide Area Networks link geographically dispersed offices in other cities or around the globe. Just about any long-distance communication medium can serve as a WAN link including switched and permanent telephone circuits, terrestrial radio systems and satellite systems.
<b>Web Configurator</b>	This is a HTML-based configurator that allows easy setup and management..
<b>WWW</b>	World Wide Web. Frequently used (incorrectly) when referring to "The Internet". WWW has two major definitions. One, the whole constellation of resources that can be accessed using Gopher, FTP, HTTP, USENET, WAIS and other tools. Two, the universe of hypertext servers (HTTP servers).
<b>X</b>	
<b>xDSL</b>	Digital Subscriber Line(s) where x, when specified, denotes a particular flavor of DSL, eg., ADSL, G.SHDSL, SDSL, VDSL, RDSL, etc.
<b>Y</b>	
<b>Z</b>	
<b>ZyNOS</b>	ZyXEL Network Operating System is the firmware used in many ZyXEL products.

# Index

!	
!!	5-23
4	
4-Port Switch	1-1
A	
About This User's Guide	xiv
About Your Gateway	xiv
Additional Installation Requirements	2-4
Advanced Users Only	2-5
Applications	1-3
Auto-negotiating LAN 10/100M Ethernet/Fast LAN Interface	1-1
B	
Backup Configuration	7-2
Backup Configuration Using TFTP	7-3
Benefits of PPPoE	A
C	
Cable Modem	5-9
Call Connection	D
Canadian Users	iv
Caution	iv
CI Commands	xiv, 2-5
Configuration	2-5
Configuration Options	2-5
Configuration Recommendations	2-5
Configure	2-5
Configuring Servers Behind SUA (Example)	5-5
Connect and Install	I
Connecting to a Cable Modem	2-3
Connecting to a DSL Modem	2-3
Control and PPP Connections	D
Copyright	ii
Crossover Ethernet Cable	2-3
Customer Support	vi
D	
Default Server IP Address	5-4
What happens if I don't Assign One?	5-4
Denial of Service	5-9
DHCP Setup	5-2
DHCP Support	1-2
DHCP Table	6-1
Disclaimer	ii
DNS (Domain Name System)	4-4
DNS Server Address Assignment	4-4
Domain Name	4-1
DSL Modem	1-3
Dynamic DNS	5-1
Limitations	5-1
Dynamic DNS Support	1-2
Dynamic Service Selection	4-2
DYNDNS Wildcard	5-1
E	
Embedded FTP and TFTP Servers	1-3
Embedded Help (web configurator)	3-2
Encapsulation Choices	4-1
Ethernet	4-1
Example of FTP Commands from the Command Line	7-3
External Hub	2-3
F	
Factory Defaults	2-5, 6-2
Password	3-1
Factory LAN Defaults	5-2
FCC	iii
Features	1-1

Federal Communications Commission (FCC)	
Interference Statement .....	iii
File Transfer Process	
Warning .....	7-5
Filename Conventions .....	7-1
Firewall	
Guidelines For Enhancing Security .....	5-9
Firmware and Configuration File Maintenance	7-1
Firmware File Upload.....	7-6
Front and Rear Panels .....	2-1
Front Panel.....	2-1
Front Panel Figure .....	2-1
Front Panel LEDs .....	2-1
FTP File Upload Command from the DOS	
Prompt Example .....	7-6
FTP Session Example of Firmware File Upload ...	
.....	7-7
FTP/TFTP.....	xiv
Full duplex Mode.....	4-4
Full Network Management.....	1-3
<b>G</b>	
General Commands for GUI-based FTP Clients ...	
.....	7-3
General Commands for GUI-based TFTP Clients	
.....	7-4
General Setup.....	5-1
General Setup and System Name.....	4-1
Getting Started .....	I
Getting to Know Your ZyWALL .....	1-1
GUI-based FTP Clients.....	7-3
GUI-based TFTP Clients .....	7-4
<b>H</b>	
Half-duplex Mode.....	4-4
Hardware Installation.....	2-1
Help .....	xiv
Help Icon in the web configurator .....	3-2
How PPPoE Works.....	B

<b>I</b>	
IANA.....	4-3
IGMP (Internet Group Multicast Protocol) .....	5-3
IKE Key Exchange Logs Examples .....	5-24
Industry Canada.....	iv
Information for Canadian Users .....	iv
Internet Access Application.....	1-4
Internet Assigned Numbers Authority (IANA)	4-3
IP Address Allocation.....	4-3
IP Address and Subnet Mask.....	4-3, 5-2
IP Multicast .....	1-2
IP Pool.....	5-2
IP Pool Setup.....	5-2
IP Static Route.....	5-7, 5-8
IPSec Logs During Packet Transmission	
Examples .....	5-25
<b>L</b>	
LAN 10/100M Ports .....	2-3
LAN TCP/IP .....	5-2
Limited Warranty .....	v
List of Diagrams .....	xiii
List of Figures .....	xi
List of Tables.....	xii
Log Examples.....	5-21
Log Message Examples .....	5-23
Logging and Tracing .....	1-3
<b>M</b>	
MAC Address.....	4-4
Cloning Recommendation .....	4-4
Cloning .....	4-4
Multicast.....	5-3
<b>N</b>	
NAT (Network Address Translation)/SUA	
(Single User Account) .....	1-2
Network Adapter .....	2-3
NIC (Network Interface Card).....	2-4

O		RFC 1597.....	4-3
Online Registration .....	v	RFC 1700.....	5-4
Overview of the ZyWALL Web Configurator.....	3-3	RFC 2408 ISAKMP Payload Types .....	5-26
P		RIP (Routing Information Protocol).....	5-3
Password .....	3-1, 5-1	RIP Direction .....	5-3
Changing Your .....	3-1	RIP Setup .....	5-3
Port Numbers .....	5-4	RIP Version .....	5-3
Power 5VDC Port .....	2-4	RoadRunner Support .....	1-3
Power Adapter Specifications .....	F	S	
PPP Data Connection .....	E	SA Monitor .....	5-20
PPPoE .....	A	Screen Specific Help.....	xiv
PPPoE Encapsulation.....	4-2	Security Association .....	5-20
PPPoE in Action.....	A	Security In General.....	5-10
PPPoE Support.....	1-3	Services and Port Numbers.....	5-4
PPTP .....	C	Single User Account .....	4-3
PPTP Encapsulation.....	4-2	Single-PC per Modem Hardware Configuration.....	A
PPTP Protocol Overview .....	D	Stateful Inspection .....	5-9
PPTP Support.....	1-3	Static Routes .....	5-7
Preface .....	xiv	Straight-through Ethernet Cable .....	2-3
Preparing Your Network.....	3-1	SUA Server.....	5-4
Primary and Secondary DNS Server.....	5-2	SUA/NAT .....	5-4
Priority of Use.....	3-1	SUA/NAT Web Configurator Screen .....	5-7
Private IP Address Ranges.....	4-3	Subnet Mask .....	4-4
Procedure To Use The RESET Button.....	2-5	Supporting Disk.....	xiv
R		Syntax Conventions .....	xv
Read Me First.....	xiv	System Status.....	6-1
Rear Panel and Connections.....	2-2	T	
Register your product.....	v	Table of Contents.....	vii
Related Documentation.....	xiv	TFTP Command Example .....	7-4
Remote Node .....	5-7	TFTP File Upload.....	7-7
Repair or Replacement.....	v	TFTP Upload Command Example.....	7-7
RESET Button .....	2-4, 6-2	The ZyWALL as a PPPoE Client .....	B
Resetting .....	2-5	Time and Date.....	1-3
Restore or Upload a Configuration File .....	7-5	Time Out.....	3-1
Restore Using FTP or TFTP .....	7-5	To avoid damage to the ZyWALL.....	2-4
Restore Using FTP Session Example.....	7-6	Trademarks .....	ii
RFC 1058.....	5-3	Traditional Dial-up Scenario .....	A
RFC 1389.....	5-3	Troubleshooting.....	8-1
RFC 1466.....	4-3	Troubleshooting and Additional Information .....	V

Troubleshooting Internet Access .....	8-3	Web Configurator ..xiv, 1-2, 1-3, 2-5, III, 3-1, 5-3,	
Troubleshooting Start-Up .....	8-1	.....5-6, 5-8, 6-1, 7-1, 8-3	
Troubleshooting the Firewall .....	8-3	Accessing .....	3-1
Troubleshooting the LAN Interface .....	8-2	Advanced Screens .....	5-1
Troubleshooting the Password .....	8-1	Backup .....	6-2
Troubleshooting the WAN Interface .....	8-2	Default .....	6-2
Trusted Network .....	5-8	F/W Upgrade .....	6-1
Turning On Your ZyWALL .....	2-4	Features Overview .....	3-2
U		Help .....	xiv
Uplink Button .....	2-3	Introducing .....	3-1
Upload a Configuration File .....	7-5	Introduction and Description .....	III
Uploading a Firmware File .....	7-6	Maintenance Screens .....	6-1
Using CI Commands .....	2-5	Navigating .....	3-1
Using FTP/TFTP .....	2-5	Navigation .....	3-1
Using the FTP Command from the Command		Navigation Summation .....	3-1
Line .....	7-2	Overview .....	3-2
Using the Web Configurator .....	2-5	Restore .....	6-2
W		The Configuration Screen .....	6-1
WAN 10M Port .....	2-3	The Wizard Setup Screens .....	4-1
WAN IP Address Assignment .....	4-2	What is a Firewall? .....	5-8
WAN Parameters .....	5-3	What is PPTP? .....	C
WAN Setup .....	4-4	Z	
Warranty .....	v	ZyXEL Limited Warranty .....	v
		ZyXEL's Firewall	
		Introduction .....	5-9