

# *ZyWALL 10*

*Internet Security Gateway*

## *User's Guide*

Version 3.24

April 2001

**ZyXEL**

TOTAL INTERNET ACCESS SOLUTION

# Copyright

## **Copyright © 2001 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**

Trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

# Federal Communications Commission (FCC) Interference Statement

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:  
This device may not cause harmful interference.

This device must accept any interference received, including interference that may cause undesired operations.

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

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

Reorient or relocate the receiving antenna.

Increase the separation between the equipment and the receiver.

Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.

Notice 1

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

Notice 2

Use of Shielded RS-232 cables is required to ensure compliance with FCC Part 15, and it is the responsibility of the user to provide and use shielded RS-232 cables.

## 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 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 the 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.

# Declaration of Conformity

We, the Manufacturer/Importer,

**ZyXEL Communications Corp.**  
**No. 6, Innovation Rd. II,**  
**Science-Based Industrial Park,**  
**Hsinchu, Taiwan, 300 R.O.C**

declare that the product

**ZyWALL 10**

is in conformity with

(reference to the specification under which conformity is declared)

<b>Standard</b>	<b>Standard Item</b>	<b>Version</b>
• EN 55022	Radio disturbance characteristics — Limits and method of measurement.	1994
• EN 61000-3-2	Disturbance in supply system caused by household appliances and similar electrical equipment “Harmonics”.	1995
• EN 61000-3-3	Disturbance in supply system caused by household appliances and similar electrical equipment “Voltage fluctuations”.	1995
• EN 61000-4-2	Electrostatic discharge immunity test — Basic EMC Publication	1995
• EN 61000-4-3	Radiated, radio-frequency, electromagnetic field immunity test	1996
• EN 61000-4-4	Electrical fast transient / burst immunity test - Basic EMC Publication	1995
• EN 61000-4-5	Surge immunity test	1995
• EN 61000-4-6	Immunity to conducted disturbances, induced by radio-frequency fields	1996
• EN 61000-4-8		1993
• EN 61000-4-11	Voltage dips, short interruptions and voltage variations immunity tests	1994



## Declaration of Conformity

The following products is herewith confirmed to comply with the requirements set out in the Council Directive on the Approximation of the laws of the Member States relating to Electromagnetic Compatibility Directive (89/336/EEC). The listed standard as below were applied:

The following Equipment:

Product : LAN / Gateway Router  
Model Number : PRESTIGE 310 / 310-S, ZyWALL 10

RFI Emission: Generic emission standard according to EN 50081-1/1992  
Limit class B according to EN 55022/1998  
Limit class A for harmonic current emission according to EN 61000-3-2/1995  
Limitation of voltage fluctuation and flicker in low-voltage supply system according to EN 61000-3-3/1995  
Immunity : Generic immunity standard according to EN 50082-1/1997/ EN 55024: 1998  
Electrostatic Discharge according to EN 61000-4-2:1995  
Contact Discharge: 4 kV, Air Discharge : 8 kV  
Radio-frequency electromagnetic field according to EN 61000-4-3:1996  
80 - 1000MHz with 1kHz AM 80% Modulation: 3V/m  
Electromagnetic field from digital telephones according to ENV 50204:1995  
900 ±5MHz with 200Hz rep. Frequency ,Duty Cycle 50%  
Electrical fast transient/burst according to EN 61000-4-4:1995  
AC/DC power supply: 1kV, Data/Signal lines : 0.5kV  
Surge immunity test according to EN 61000-4-5:1995  
AC/DC Line to Line: 1kV, AC/DC Line to Earth : 2kV  
Immunity to conducted disturbances, Induced by radio-frequency fields: EN 61000-4-6:1996  
0.15 - 80MHz with 1kHz AM 80% Modulation: 3V/m  
Power frequency magnetic field immunity test according to EN 61000-4-8:1993  
3A/m at frequency 50Hz  
Voltage dips, short interruptions and voltage variations immunity test according to EN 61000-4-11:1994  
30% Reduction @ 10ms/ 500ms, 60% Reduction @100ms, >95%Reduction @10ms/ 5000ms

The following importer/manufacture is responsible for this declaration:

Company Name **ZyXEL Communications Services GmbH.**  
Company Address : Thaliastrasse 125a/2/2/4  
A-1160 Wien • AUSTRIA  
Telephone : Tel.: 01 / 494 86 77-0 Facsimile :  
Fax: 01 / 494 86 78

Person is responsible for marking this declaration:

Hianfred RECLA  
Name (Full Name)  
October 23, 2000  
Date

ZyXEL Techn Support  
Position/ Title  
Hianfred Recla  
Legal Signature  
**ZyXEL Communications Services GmbH.**  
Thaliastrasse 125a/2/2/4  
A-1160 Wien • AUSTRIA  
Tel.: 01 / 494 86 77-0  
Fax: 01 / 494 86 78

# ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

## **NOTE**

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind of character to the purchaser.

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



## **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

**When you contact your customer support representative please have the following information ready:**

- ◆ ZyWALL Model and serial number.
- ◆ Information in **Menu 24.2.1 —System Information**.
- ◆ Warranty Information.
- ◆ Date you received your ZyWALL.
- ◆ Brief description of the problem and the steps you took to solve it.

Method	EMAIL — Support	Telephone	Web Site	Regular Mail
Region	EMAIL — Sales	Fax	FTP Site	
Worldwide	<a href="mailto:support@zyxel.com.tw">support@zyxel.com.tw</a> <a href="mailto:support@europe.zyxel.com">support@europe.zyxel.com</a>	+886-3-578-3942	<a href="http://www.zyxel.com">www.zyxel.com</a> <a href="http://www.europe.zyxel.com">www.europe.zyxel.com</a>	ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, HsinChu, Taiwan.
	<a href="mailto:sales@zyxel.com.tw">sales@zyxel.com.tw</a>	+886-3-578-2439	<a href="http://ftp.europe.zyxel.com">ftp.europe.zyxel.com</a>	
North America	<a href="mailto:support@zyxel.com">support@zyxel.com</a>	+1-714-632-0882 800-255-4101	<a href="http://www.zyxel.com">www.zyxel.com</a>	ZyXEL Communications Inc., 1650 Miraloma Avenue, Placentia, CA 92870, U.S.A.
	<a href="mailto:sales@zyxel.com">sales@zyxel.com</a>	+1-714-632-0858	<a href="http://ftp.zyxel.com">ftp.zyxel.com</a>	
Scandinavia	<a href="mailto:support@zyxel.dk">support@zyxel.dk</a>	+45-3955-0700	<a href="http://www.zyxel.dk">www.zyxel.dk</a>	ZyXEL Communications A/S, Columbusvej 5, 2860 Soeborg, Denmark.
	<a href="mailto:sales@zyxel.dk">sales@zyxel.dk</a>	+45-3955-0707	<a href="http://ftp.zyxel.dk">ftp.zyxel.dk</a>	
Austria	<a href="mailto:support@zyxel.at">support@zyxel.at</a>	+43-1-4948677-0 0810-1-ZyXEL 0810-1-99935	<a href="http://www.zyxel.at">www.zyxel.at</a>	ZyXEL Communications Services GmbH., Thaliastrasse 125a/2/2/4, A-1160 Vienna, Austria
	<a href="mailto:sales@zyxel.at">sales@zyxel.at</a>	+43-1-4948678	<a href="http://ftp.zyxel.at">ftp.zyxel.at</a> Note: for Austrian users with *.at domain only!	
Germany	<a href="mailto:support@zyxel.de">support@zyxel.de</a>	+49-2405-6909-0 0180-5213247 Tech Support hotline 0180-5099935	<a href="http://www.zyxel.de">www.zyxel.de</a>	ZyXEL Deutschland GmbH., Adenauerstr. 20/A4, D-52146 Wuersele, Germany.
	<a href="mailto:sales@zyxel.de">sales@zyxel.de</a>	RMA/Repair hotline +49-2405-6909-99	<a href="http://ftp.europe.zyxel.com">ftp.europe.zyxel.com</a>	



# Table of Contents

<b>Copyright</b> .....	<b>ii</b>
<b>Federal Communications Commission (FCC) Interference Statement</b> .....	<b>iii</b>
<b>Information for Canadian Users</b> .....	<b>iv</b>
<b>ZyXEL Limited Warranty</b> .....	<b>vii</b>
<b>Customer Support</b> .....	<b>viii</b>
<b>Table of Contents</b> .....	<b>ix</b>
<b>List of Figures</b> .....	<b>xvii</b>
<b>List of Tables</b> .....	<b>xxiii</b>
<b>Preface</b> .....	<b>xxvii</b>
Getting Started.....	I
<b>Chapter 1 Getting to Know Your ZyWALL</b> .....	<b>1-1</b>
1.1 The ZyWALL 10 Internet Security Gateway .....	1-1
1.2 Features of The ZyWALL 10 .....	1-1
1.3 Applications for ZyWALL 10 .....	1-3
1.3.1 Broadband Internet Access via Cable or xDSL Modem.....	1-3
<b>Chapter 2 Hardware Installation &amp; Initial Setup</b> .....	<b>2-1</b>
2.1 Front Panel LEDs and Back Panel Ports .....	2-1
2.1.1 Front Panel LEDs .....	2-1
2.2 ZyWALL 10 Rear Panel and Connections .....	2-2
2.3 Additional Installation Requirements .....	2-3
2.4 Turn On Your ZyWALL .....	2-4
2.5 Navigating the SMT Interface .....	2-4
2.5.1 Main Menu .....	2-6
2.5.2 System Management Terminal Interface Summary .....	2-7
2.5.3 SMT Menus at a Glance .....	2-8
2.6 Changing the System Password.....	2-9
2.6.1 Resetting the ZyWALL .....	2-9

2.7	General Setup.....	2-9
2.7.1	Dynamic DNS .....	2-10
2.7.2	Procedure For Configuring Menu 1 .....	2-10
2.7.3	Configuring Dynamic DNS.....	2-11
2.8	WAN Setup.....	2-12
2.9	LAN Setup .....	2-13
2.9.1	LAN Port Filter Setup .....	2-14
<b>Chapter 3 Internet Access.....</b>		<b>3-1</b>
3.1	TCP/IP and DHCP for LAN .....	3-1
3.1.1	Factory LAN Defaults.....	3-1
3.1.2	DHCP Configuration.....	3-1
3.1.3	IP Address and Subnet Mask .....	3-2
3.1.4	Private IP Addresses .....	3-2
3.1.5	RIP Setup .....	3-3
3.1.6	IP Multicast .....	3-3
3.1.7	IP Alias.....	3-4
3.2	TCP/IP and DHCP Ethernet Setup.....	3-4
3.2.1	IP Alias Setup.....	3-7
3.3	Internet Access Setup.....	3-8
3.3.1	Ethernet Encapsulation.....	3-8
3.3.2	PPTP Encapsulation .....	3-10
3.3.3	Configuring the PPTP Client.....	3-10
3.3.4	PPPoE Encapsulation .....	3-11
3.4	Basic Setup Complete .....	3-13
Advanced Applications.....		II
<b>Chapter 4 Remote Node Setup .....</b>		<b>4-1</b>
4.1	Remote Node Profile.....	4-1
4.1.1	Ethernet Encapsulation.....	4-1
4.1.2	PPPoE Encapsulation.....	4-3
4.1.3	PPTP Encapsulation .....	4-4
4.2	Editing TCP/IP Options (with Ethernet Encapsulation).....	4-6
4.2.1	Editing TCP/IP Options (with PPTP Encapsulation) .....	4-7
4.2.2	Editing TCP/IP Options (with PPPoE Encapsulation) .....	4-9
4.3	Remote Node Filter .....	4-9
<b>Chapter 5 IP Static Route Setup .....</b>		<b>5-1</b>

---

5.1	IP Static Route Setup.....	5-2
<b>Chapter 6 Network Address Translation (NAT) .....</b>		<b>6-1</b>
6.1	Introduction .....	6-1
6.1.1	NAT Definitions .....	6-1
6.1.2	What NAT Does .....	6-1
6.1.3	How NAT works .....	6-2
6.1.4	NAT Mapping Types.....	6-3
6.1.5	SUA (Single User Account) Versus NAT .....	6-4
6.1.6	NAT Application.....	6-4
6.2	SMT Menus.....	6-5
6.2.1	Applying NAT in the SMT Menus .....	6-5
6.2.2	Configuring NAT .....	6-7
6.2.3	Address Mapping Sets and NAT Server Sets: .....	6-7
6.3	NAT Server Sets.....	6-12
6.3.1	Multiple Servers behind NAT .....	6-13
6.3.2	Configuring a Server behind NAT .....	6-13
6.4	Examples .....	6-15
6.4.1	Internet Access Only .....	6-15
6.4.2	Example 2: Internet Access with an Inside Server .....	6-16
6.4.3	Example 3: General Case .....	6-17
6.4.4	Example 4: NAT Unfriendly Application Programs .....	6-20
Advanced Management.....		III
<b>Chapter 7 Filter Configuration.....</b>		<b>7-1</b>
7.1	About Filtering .....	7-1
7.1.1	The Filter Structure of the ZyWALL.....	7-2
7.2	Configuring a Filter Set.....	7-4
7.2.1	Filter Rules Summary Menu.....	7-6
7.2.2	Configuring a Filter Rule.....	7-7
7.2.3	TCP/IP Filter Rule.....	7-7
7.2.4	Generic Filter Rule .....	7-11
7.3	Example Filter .....	7-13
7.4	Filter Types and NAT.....	7-15
7.5	Firewall.....	7-16
7.6	Applying a Filter and Factory Defaults .....	7-16
7.6.1	LAN traffic .....	7-16

7.6.2	Remote Node Filters.....	7-17
<b>Chapter 8 SNMP Configuration.....</b>		<b>8-1</b>
8.1	About SNMP.....	8-1
8.2	Configuring SNMP.....	8-1
<b>Chapter 9 System Information &amp; Diagnosis.....</b>		<b>9-1</b>
9.1	System Status.....	9-1
9.2	System Information and Console Port Speed.....	9-3
9.2.1	System Information.....	9-4
9.2.2	Console Port Speed.....	9-5
9.3	Log and Trace.....	9-5
9.3.1	Viewing Error Log.....	9-5
9.3.2	UNIX Syslog.....	9-6
9.3.3	Call-Triggering Packet.....	9-10
9.4	Diagnostic.....	9-10
9.4.1	WAN DHCP.....	9-11
<b>Chapter 10 Firmware and Configuration File Maintenance.....</b>		<b>10-1</b>
10.1	Filename conventions.....	10-1
10.1.1	Firmware Development.....	10-2
10.2	Backup Configuration.....	10-2
10.2.1	Example: Backup Configuration Using HyperTerminal.....	10-3
10.2.2	Backup Configuration Using Telnet.....	10-3
10.3	Restore Configuration.....	10-4
10.3.1	Example: Restore Configuration Using HyperTerminal.....	10-4
10.4	Upload Firmware.....	10-5
10.4.1	Uploading the Router Firmware.....	10-5
10.4.2	Example: Xmodem Upload Using HyperTerminal.....	10-6
10.4.3	Uploading Router Configuration File.....	10-6
10.5	TFTP File Transfer.....	10-7
10.5.1	Example: TFTP Command.....	10-8
10.6	FTP File Transfer.....	10-9
10.6.1	Using the FTP command from the DOS Prompt.....	10-11
<b>Chapter 11 System Maintenance &amp; Information.....</b>		<b>11-1</b>
11.1	Command Interpreter Mode.....	11-1

---

11.2	Call Control Support .....	11-2
11.2.1	Budget Management.....	11-2
11.2.2	Call History .....	11-3
11.3	Time and Date Setting.....	11-4
	How often does the ZyWALL update the time?.....	11-6
11.4	Remote Management Setup.....	11-7
11.5	Boot Commands .....	11-8
<b>Chapter 12</b>	<b>Telnet Configuration and Capabilities .....</b>	<b>12-1</b>
12.1	About Telnet Configuration.....	12-1
12.2	Telnet Under NAT.....	12-1
12.3	Telnet Capabilities.....	12-1
12.3.1	Single Administrator .....	12-1
12.3.2	System Timeout.....	12-2
12.4	Telnet Behind the Firewall .....	12-2
Firewall and Content Filters .....		13-1
<b>Chapter 13</b>	<b>What is a Firewall? .....</b>	<b>13-1</b>
13.1	Types of Firewalls .....	13-1
13.1.1	Packet Filtering Firewalls .....	13-1
13.1.2	Application-level Firewalls .....	13-1
13.1.3	Stateful Inspection Firewalls .....	13-2
13.2	Introduction to ZyXEL's Firewall.....	13-2
13.3	Denial of Service .....	13-3
13.3.1	Basics.....	13-3
13.3.2	Types of DoS attacks.....	13-4
13.4	Stateful Inspection .....	13-6
13.4.1	Stateful Inspection Process.....	13-7
13.4.2	Stateful Inspection & the ZyWALL .....	13-8
13.4.3	TCP Security .....	13-8
13.4.4	UDP/ICMP Security.....	13-9
13.4.5	Upper Layer Protocols.....	13-9
13.5	Guidelines For Enhancing Security With Your Firewall.....	13-9
13.5.1	Security In General.....	13-10
<b>Chapter 14</b>	<b>Introducing the ZyWALL Firewall .....</b>	<b>14-1</b>

14.1	SMT Menus.....	14-1
14.1.1	View Firewall Log .....	14-2
14.1.2	Attack Types .....	14-2
14.2	The Big Picture - Filtering, Firewall and NAT .....	14-5
14.3	Packet Filtering Vs Firewall.....	14-6
14.3.1	Packet Filtering: .....	14-6
14.3.2	Firewall .....	14-7
<b>Chapter 15 Introducing the ZyWALL Web Configurator .....</b>		<b>15-1</b>
15.1	Web Configurator Login and Welcome Screens.....	15-1
15.2	Enabling the Firewall .....	15-3
15.3	E-mail.....	15-3
15.3.1	What are Alerts?.....	15-3
15.3.2	What are Logs? .....	15-4
15.3.3	SMTP Error Messages .....	15-6
15.3.4	Example E-mail Log .....	15-6
15.4	Attack Alert.....	15-7
15.4.1	Threshold Values: .....	15-7
15.4.2	Half-Open Sessions .....	15-8
<b>Chapter 16 Creating Custom Rules .....</b>		<b>16-1</b>
16.1	Rules Overview.....	16-1
16.2	Rule Logic Overview .....	16-1
16.2.1	Rule Checklist .....	16-1
16.2.2	Security Ramifications .....	16-2
16.2.3	Key Fields For Configuring Rules .....	16-2
16.3	Connection Direction .....	16-3
16.3.1	LAN to WAN Rules .....	16-3
16.3.2	WAN to LAN Rules.....	16-3
16.4	Rule Summary.....	16-4
16.5	Predefined Services .....	16-7
16.5.1	Creating/Editing Firewall Rules.....	16-10
16.5.2	Source and Destination Addresses .....	16-12
16.6	Timeout .....	16-14
16.6.1	Factors Influencing Choices for Timeout Values.....	16-14
<b>Chapter 17 Custom Ports.....</b>		<b>17-1</b>

---

17.1	Introduction .....	17-1
17.2	Creating/Editing A Custom Port .....	17-3
<b>Chapter 18</b>	<b>Logs .....</b>	<b>18-1</b>
18.1	Log Screen.....	18-1
<b>Chapter 19</b>	<b>Example Firewall Rules.....</b>	<b>19-1</b>
19.1	Examples .....	19-1
19.1.1	Example 1: Firewall Rule To Allow Web Service From The Internet .....	19-1
19.1.2	Example 2: Small Office With Mail, FTP and Web Servers .....	19-6
19.1.3	Example 3: DHCP Negotiation and Syslog Connection from the Internet.....	19-12
<b>Chapter 20</b>	<b>Content Filtering.....</b>	<b>20-1</b>
20.1	Categories.....	20-1
20.1.1	Restrict Web Features.....	20-1
20.1.2	Filter List .....	20-1
20.1.3	Days and Times .....	20-1
20.2	Update List .....	20-3
20.3	Exempting Computers .....	20-4
20.4	Customizing.....	20-5
20.5	Keywords .....	20-6
20.6	Log Records .....	20-7
Troubleshooting, Appendices, Glossary and Index.....		V
<b>Chapter 21</b>	<b>Troubleshooting.....</b>	<b>21-1</b>
21.1	Problems Starting Up the ZyWALL.....	21-1
21.2	Problems with the LAN Interface.....	21-2
21.3	Problems with the WAN interface.....	21-2
21.4	Problems with Internet Access .....	21-3
21.5	Problems with the Firewall.....	21-3
<b>Appendix A</b>	<b>PPPoE.....</b>	<b>A</b>
<b>Appendix B</b>	<b>PPTP .....</b>	<b>C</b>
<b>Appendix C</b>	<b>Hardware Specifications .....</b>	<b>E</b>
<b>Appendix D</b>	<b>Important Safety Instructions .....</b>	<b>F</b>

<b>Appendix E Firewall CLI Commands .....</b>	<b>G</b>
<b>Appendix F Power Adapter Specifications.....</b>	<b>L</b>
<b>Glossary of Terms .....</b>	<b>N</b>
<b>Index .....</b>	<b>Y</b>



# List of Figures

Figure 1-1 Secure Internet Access via Cable .....	1-4
Figure 1-2 Secure Internet Access via DSL .....	1-4
Figure 2-1 Front Panel .....	2-1
Figure 2-2 ZyWALL 10 Rear Panel and Connections.....	2-2
Figure 2-3 Initial Screen.....	2-4
Figure 2-4 Password Screen.....	2-4
Figure 2-5 ZyWALL 10 Main Menu.....	2-6
Figure 2-6 SMT Menus at a Glance .....	2-8
Figure 2-7 Menu 23 — System Password.....	2-9
Figure 2-8 Menu 1 — General Setup .....	2-10
Figure 2-9 Configure Dynamic DNS .....	2-11
Figure 2-10 Menu 2 — WAN Setup.....	2-13
Figure 2-11 Menu 3 — LAN Setup.....	2-14
Figure 2-12 Menu 3.1 — LAN Port Filter Setup .....	2-14
Figure 3-1 Physical Network.....	3-4
Figure 3-2 Partitioned Logical Networks.....	3-4
Figure 3-3 Menu 3 — LAN Setup .....	3-5
Figure 3-4 Menu 3.2 — TCP/IP and DHCP Ethernet Setup.....	3-5
Figure 3-5 Menu 3.2.1 — IP Alias Setup.....	3-7
Figure 3-6 Menu 4 — Internet Access Setup (Ethernet).....	3-9
Figure 3-7 Internet Access Setup (PPTP) .....	3-11
Figure 3-8 Internet Access Setup (PPPoE) .....	3-12
Figure 4-1 Menu 11.1 — Remote Node Profile for Ethernet Encapsulation.....	4-1
Figure 4-2 Menu 11.1 — Remote Node Profile for PPPoE Encapsulation.....	4-3
Figure 4-3 Menu 11.1 — Remote Node Profile for PPTP Encapsulation.....	4-5

Figure 4-4 Menu 11.3 — Remote Node Network Layer Options.....	4-6
Figure 4-5 Menu 11.3 — Remote Node Network Layer Options.....	4-8
Figure 4-6 Menu 11.5 — Remote Node Filter (Ethernet Encapsulation) .....	4-10
Figure 4-7 Menu 11.5 — Remote Node Filter (PPPoE or PPTP Encapsulation) .....	4-10
Figure 5-1 Example of Static Routing Topology .....	5-1
Figure 5-2 Menu 12 — IP Static Route Setup .....	5-2
Figure 5-3 Menu 12. 1 — Edit IP Static Route.....	5-2
Figure 6-1 How NAT Works.....	6-2
Figure 6-2 NAT Application .....	6-5
Figure 6-3 Menu 4 — Applying NAT for Internet Access .....	6-6
Figure 6-4 Menu 11.3 — Applying NAT to the Remote Node.....	6-6
Figure 6-5 Menu 15 — NAT Setup.....	6-7
Figure 6-6 Menu 15.1 — Address Mapping Sets .....	6-8
Figure 6-7 Menu 15.1.255 — SUA Address Mapping Rules .....	6-8
Figure 6-8 Menu 15.1.1 — First Set.....	6-10
Figure 6-9 Menu 15.1.1.1 — Editing an Individual Rule in a Set .....	6-11
Figure 6-10 Multiple Servers Behind NAT.....	6-13
Figure 6-11 Menu 15.2 — NAT Server Setup .....	6-14
Figure 6-12 NAT Example 1.....	6-15
Figure 6-13 Menu 4 — Internet Access & NAT Example.....	6-15
Figure 6-14 NAT Example 2.....	6-16
Figure 6-15 Menu 15.2 — Specifying an Inside Server .....	6-16
Figure 6-16 NAT Example 3.....	6-17
Figure 6-17 Example 3: Menu 11.3 .....	6-18
Figure 6-18 Example 3: Menu 15.1.1.1 .....	6-18
Figure 6-19 Example 3: Final Menu 15.1.1 .....	6-19
Figure 6-20 Example 3: Menu 15.2 .....	6-19

---

Figure 6-21 NAT Example 4.....	6-20
Figure 6-22 Example 4: Menu 15.1.1.1 — Address Mapping Rule.....	6-21
Figure 6-23 Example 4: Menu 15.1.1 — Address Mapping Rules .....	6-21
Figure 7-1 Outgoing Packet Filtering Process .....	7-1
Figure 7-2 Filter Rule Process.....	7-3
Figure 7-4 Menu 21 — Filter and Firewall Setup .....	7-4
Figure 7-5 Menu 21.1 — Filter Set Configuration.....	7-4
Figure 7-6 NetBIOS_WAN Filter Rules Summary .....	7-5
Figure 7-7 NetBIOS_LAN Filter Rules Summary.....	7-5
Figure 7-8 TEL_FTP_WEB_WAN Filter Rules Summary .....	7-5
Figure 7-9 Menu 21.1.1.1 — TCP/IP Filter Rule.....	7-7
Figure 7-10 Executing an IP Filter.....	7-10
Figure 7-11 Menu 21.4.1.1 — Generic Filter Rule .....	7-11
Figure 7-12 Telnet Filter Example .....	7-13
Figure 7-13 Example Filter — Menu 21.1.1.1 .....	7-14
Figure 7-14 Example Filter Rules Summary — Menu 21.1.3 .....	7-15
Figure 7-15 Protocol and Device Filter Sets .....	7-16
Figure 7-16 Filtering LAN Traffic .....	7-17
Figure 7-17 Filtering Remote Node Traffic .....	7-17
Figure 8-1 Menu 22 — SNMP Configuration.....	8-1
Figure 9-1 Menu 24 — System Maintenance .....	9-1
Figure 9-2 Menu 24.1 — System Maintenance — Status.....	9-2
Figure 9-3 Menu 24.2 — System Information and Console Port Speed.....	9-3
Figure 9-4 Menu 24.2.1 — System Maintenance — Information.....	9-4
Figure 9-5 Menu 24.2.2 — System Maintenance — Change Console Port Speed.....	9-5
Figure 9-6 Menu 24.3 — System Maintenance — Log and Trace .....	9-6
Figure 9-7 Examples of Error and Information Messages .....	9-6

Figure 9-8 Menu 24.3.2 — System Maintenance — UNIX Syslog.....	9-6
Figure 9-9 Call-Triggering Packet Example.....	9-10
Figure 9-10 Menu 24.4 — System Maintenance — Diagnostic.....	9-11
Figure 9-11 WAN & LAN DHCP.....	9-12
Figure 10-1 System Maintenance — Backup Configuration.....	10-2
Figure 10-2 Example: Backup Configuration.....	10-3
Figure 10-4 Telnet into Menu 24.5 — Backup Configuration.....	10-3
Figure 10-5 System Maintenance — Restore Configuration.....	10-4
Figure 10-6 Example: Restore Configuration.....	10-4
Figure 10-8 Telnet into Menu 24.6 Restore Configuration.....	10-5
Figure 10-9 Menu 24.7 — System Maintenance — Upload Firmware.....	10-5
Figure 10-10 Menu 24.7.1 — System Maintenance — Upload Router Firmware.....	10-6
Figure 10-11 Example: Xmodem Upload.....	10-6
Figure 10-12 Menu 24.7.2 — System Maintenance — Upload Router Configuration File.....	10-7
Figure 10-13 Telnet into Menu 24.7.1.....	10-10
Figure 10-14 Telnet into Menu 24.7.2 — System Maintenance.....	10-10
Figure 10-15 FTP Session Example.....	10-11
Figure 11-1 Command Mode in Menu 24.....	11-1
Figure 11-2 Valid Commands.....	11-1
Figure 11-3 Call Control.....	11-2
Figure 11-4 Budget Management.....	11-2
Figure 11-5 Call History.....	11-4
Figure 11-6 Menu 24 — System Maintenance.....	11-5
Figure 11-7 Menu 24.10 System Maintenance — Time and Date Setting.....	11-5
Figure 11-8 Menu 24.11 — Remote Management Control.....	11-7
Figure 11-9 Option to Enter Debug Mode.....	11-8
Figure 11-10 Boot Module Commands.....	11-9

---

Figure 12-1 Telnet Configuration on a TCP/IP Network .....	12-1
Figure 13-1 ZyWALL Firewall Application .....	13-3
Figure 13-2 Three-Way Handshake .....	13-5
Figure 13-3 SYN Flood.....	13-5
Figure 13-4 Smurf Attack .....	13-6
Figure 13-5 Stateful Inspection .....	13-7
Figure 14-1 SMT Main Menu .....	14-1
Figure 14-2 Menu 21 — Filter and Firewall Setup.....	14-1
Figure 14-3 Menu 21.2 — Firewall Setup .....	14-2
Figure 14-4 View Firewall Log.....	14-4
Figure 14-5 Big Picture — Filtering, Firewall and NAT.....	14-6
Figure 15-1 Login screen as seen in Netscape .....	15-1
Figure 15-2 ZyWALL Web Configurator Welcome Screen.....	15-2
Figure 15-3 Enabling the Firewall .....	15-3
Figure 15-4 E-mail Screen .....	15-4
Figure 15-5 E-mail Log.....	15-7
Figure 15-6 Attack Alert.....	15-9
Figure 16-1 LAN to WAN Traffic.....	16-3
Figure 16-2 WAN to LAN Traffic.....	16-4
Figure 16-3 Firewall Rules Summary — First Screen .....	16-5
Figure 16-4 Creating/Editing A Firewall Rule.....	16-10
Figure 16-5 Adding/Editing Source and Destination Addresses.....	16-12
Figure 16-6 Timeout Screen.....	16-14
Figure 17-1 Custom Ports .....	17-1
Figure 17-2 Creating/Editing A Custom Port .....	17-3
Figure 18-1 Log Screen.....	18-1
Figure 19-1 Activate The Firewall.....	19-2

Figure 19-2 Example 1: E-mail Screen.....	19-3
Figure 19-3 Example 1: Configuring a Rule.....	19-4
Figure 19-4 Example 1: Destination Address for Traffic Originating from the Internet .....	19-5
Figure 19-5 Example 1: Rule Summary Screen.....	19-6
Figure 19-6 Send Alerts When Attacked .....	19-7
Figure 19-7 Configuring A POP Custom Port.....	19-8
Figure 19-8 Example 2: Local Network Rule 1 Configuration.....	19-9
Figure 19-9 Example 2: Local Network Rule Summary.....	19-10
Figure 19-10 Example: Internet to Local Network Rule Summary .....	19-11
Figure 19-11 Custom Port for Syslog .....	19-12
Figure 19-12 Syslog Rule Configuration .....	19-13
Figure 19-13 Example 3: Rule Summary .....	19-14
Figure 20-1 Categories Screen.....	20-2
Figure 20-2 List Update Screen .....	20-3
Figure 20-3 Exempt Zone Screen .....	20-4
Figure 20-4 Customize Screen.....	20-5
Figure 20-5 Keyword Screen .....	20-6
Figure 20-6 Logs Screen.....	20-7

# List of Tables

Table 2-1 LED functions .....	2-1
Table 2-2 Main Menu Commands .....	2-5
Table 2-3 Main Menu Summary.....	2-7
Table 2-4 General Setup Menu Field.....	2-11
Table 2-5 Configure Dynamic DNS Menu Fields .....	2-12
Table 2-6 WAN Setup Menu Fields.....	2-13
Table 3-1 DHCP Ethernet Setup Menu Fields.....	3-6
Table 3-2 LAN TCP/IP Setup Menu Fields.....	3-6
Table 3-3 IP Alias Setup Menu Fields.....	3-8
Table 3-4 Internet Access Setup Menu Fields .....	3-9
Table 3-5 New Fields in Menu 4 (PPTP) screen .....	3-11
Table 3-6 New Fields in Menu 4 (PPPoE) screen .....	3-12
Table 4-1 Fields in Menu 11.1 .....	4-2
Table 4-2 Fields in Menu 11.1 (PPPoE Encapsulation Specific).....	4-4
Table 4-3 Fields in Menu 11.1 (PPTP Encapsulation).....	4-5
Table 4-4 Remote Node Network Layer Options Menu Fields .....	4-6
Table 4-5 Remote Node Network Layer Options Menu Fields .....	4-8
Table 5-1 IP Static Route Menu Fields.....	5-3
Table 6-1 NAT Definitions .....	6-1
Table 6-2 NAT Mapping Types .....	6-3
Table 6-3 Applying NAT in Menus 4 & 11.3 .....	6-7
Table 6-4 SUA Address Mapping Rules .....	6-9
Table 6-5 Fields in Menu 15.1.1.....	6-11
Table 6-6 Menu 15.1.1.1 — Configuring an Individual Rule.....	6-12
Table 6-7 Services & Port numbers.....	6-14
Table 7-1 Abbreviations Used in the Filter Rules Summary Menu.....	7-6

Table 7-2 Rule Abbreviations Used .....	7-6
Table 7-3 TCP/IP Filter Rule Menu Fields .....	7-8
Table 7-4 Generic Filter Rule Menu Fields.....	7-12
Table 8-1 SNMP Configuration Menu Fields .....	8-2
Table 9-1 System Maintenance — Status Menu Fields.....	9-2
Table 9-2 Fields in System Maintenance — Information .....	9-4
Table 9-3 System Maintenance Menu Syslog Parameters .....	9-7
Table 9-4 System Maintenance Menu Diagnostic.....	9-12
Table 10-1 Filename Conventions .....	10-2
Table 10-2 Third Party TFTP Clients — General commands.....	10-8
Table 10-3 Third Party FTP Clients — General Fields.....	10-12
Table 11-1 Budget Management .....	11-3
Table 11-2 Call History Fields .....	11-4
Table 11-3 Time and Date Setting Fields .....	11-6
Table 11-4 Menu 24.11 — Remote Management Control .....	11-7
Table 13-1 Common IP Ports.....	13-4
Table 14-1 ICMP Commands That Trigger Alerts.....	14-3
Table 14-2 Legal NetBIOS Commands .....	14-3
Table 14-3 Legal SMTP Commands.....	14-3
Table 14-4 View Firewall Log .....	14-5
Table 15-1 E-mail.....	15-5
Table 15-2 SMTP Error Messages .....	15-6
Table 15-3 Attack Alert.....	15-10
Table 16-1 Firewall Rules Summary — First Screen.....	16-6
Table 16-2 Predefined Services.....	16-8
Table 16-3 Creating/Editing A Firewall Rule .....	16-11
Table 16-4 Adding/Editing Source and Destination Addresses .....	16-13
Table 16-5 Timeout Menu.....	16-15



Table 17-1 Custom Ports .....	17-2
Table 17-2 Creating/Editing A Custom Port .....	17-4
Table 18-1 Log Screen .....	18-2
Table 21-1 Troubleshooting the Start-Up of your ZyWALL .....	21-1
Table 21-2 Troubleshooting the LAN Interface .....	21-2
Table 21-3 Troubleshooting the WAN interface.....	21-2
Table 21-4 Troubleshooting Internet Access .....	21-3
Table 21-5 Troubleshooting the Firewall .....	21-3



# Preface

## About Your Router

Congratulations on your purchase of the ZyWALL 10 Internet Security Gateway.

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

The ZyWALL 10 is a dual Ethernet Internet Security Gateway integrated with robust firewall solutions and network management features that allows access to the Internet via Cable/ADSL modem or Internet router. It is designed for:

- ❑ Home offices and small businesses with Cable, xDSL and wireless modem via Ethernet port as Internet access media.
- ❑ Multiple office/department connections via access devices.
- ❑ E-commerce/EDI applications.

Your ZyWALL 10 is easy to install and configure.

The ZyWALL Web Configurator (Web Configurator) is a web-based utility that allows you to access the ZyWALL's management settings and configure the firewall. Most functions of the ZyWALL 10 are also software configurable via the SMT (System Management Terminal) interface. The SMT is a menu-driven interface that you can access from a terminal emulator through the console port or over a telnet connection.

---

You can configure most features of the ZyWALL 10 via SMT but we recommend you configure the firewall using the ZyWALL Web Configurator.

---

## About This User's Manual

This manual is designed to guide you through the SMT configuration of your ZyWALL 10 for its various applications.

### Structure of this Manual

This manual is structured as follows:

- Part I. Getting Started (Chapters 1 — 3) is structured as a step-by-step guide to help you connect, install and setup your ZyWALL to operate on your network and access the Internet.
- Part II. Advanced Applications (Chapters 4 — 6) describes the advanced applications of your ZyWALL, such as Remote Node Setup, IP Static routes and NAT.
- Part III. Advanced Management (Chapters 7 — 12) provides information on ZyWALL Filtering, System Information and Diagnosis, Transferring Files, System Maintenance and Telnet.
- Part IV. Firewall (Chapters 13 — 20) defines the term “firewall”, introduces the ZyWall firewall and ZyWall web configurator, describes how to create custom rules and configure customized ports, explains logs and provides example firewall rules. Chapter 20 explains content filtering and how to use the ZyWALL to restrict web features such as ActiveX controls, Java applets and cookies, disable web proxies and block specific URLs.
- Part V. Troubleshooting (Chapter 21) provides information about solving common problems as well as some Appendices, a Glossary and an Index.

Regardless of your particular application, it is important that you follow the steps outlined in Chapters 1 and 2 to connect your ZyWALL to your LAN. You can then refer to the appropriate chapters of the manual, depending on your applications.

### Related Documentation

- **Support Disk**  
More detailed information about the ZyWALL and examples of its use can be found in our included disk (as well as on the zyxel.com web site). This disk contains information on configuring your ZyWALL for Internet Access, a General FAQ, an Advanced FAQ, Applications Notes, Troubleshooting, Reference CI Commands as well as bundled software.
- **Read Me First**  
Our Read Me First is designed to help you get your ZyWALL up and running right away. It contains a detailed easy to follow connection diagram, ZyWALL default settings, handy checklists, information on setting up your PC, and information on configuring your ZyWALL for Internet access.
- **Packing List Card**  
Finally, you should have a Packing List Card, which lists all items that should have come with your ZyWALL.
- **ZyXEL Web and FTP Server Sites**  
You can access release notes for firmware upgrades and other information at ZyXEL web and FTP server sites. Refer to the *Customer Support* page in this User's Guide for more information.

### Syntax Conventions

- “Enter” means for you to type one or more characters and press the carriage return. “Select” or “Choose” means for you to select one from the predefined choices.
- The SMT menu titles and labels are in **Bold Times** font. The choices of a menu item are in **Bold Arial** font. A single keystroke is in Arial font and enclosed in square brackets, for instance, [ENTER] means the Enter, or carriage return, key; [ESC] means the escape key and [SPACE BAR] means the space bar. [UP], {DOWN} are the up, down arrow keys.
- For brevity's sake, we will use “e.g.” as a shorthand for “for instance” and “i.e.” for “that is” or “in other words” throughout this manual.

---

# Part I:

---

## Getting Started

---

Chapters 1— 3 are structured as a step-by-step guide to help you connect, install and setup your ZyWALL to operate on your network and access the Internet.



# Chapter 1

## Getting to Know Your ZyWALL

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

### 1.1 The ZyWALL 10 Internet Security Gateway

The ZyWALL 10 is a dual Ethernet Internet Security Gateway integrated with a robust firewall and network management features designed for home offices and small businesses to access the Internet via Cable/ADSL modem or Internet router.

By integrating NAT and firewall capability, ZyXEL's ZyWALL 10 provides not only ease of installation and Internet access, but also a complete security solution to protect your Intranet and efficiently manage data traffic on your network.

The ZyWALL Web Configurator is a breeze to operate and totally independent of the operating system platform you use.

### 1.2 Features of The ZyWALL 10

The following are the main features of the ZyWALL 10.

#### Firewall

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

---

You can configure most features of the ZyWALL 10 via SMT but we recommend you configure the firewall and Content Filters using the ZyWALL Web Configurator.

---

#### 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.

#### Packet Filtering

The Packet Filtering mechanism blocks unwanted traffic from entering/leaving your network.

#### PPPoE

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

### **PPTP Encapsulation**

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using a TCP/IP-based network. PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet. The ZyWALL supports one PPTP server connection at any given time.

### **Dynamic DNS Support**

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

### **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 both versions 1 and 2.

### **IP Alias**

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

### **SNMP**

SNMP (Simple Network Management Protocol) is a protocol used for exchanging management information between network devices. SNMP is a member of 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).

### **Auto-negotiating 10/100Mbps Ethernet**

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

### **Network Address Translation (NAT)**

NAT (Network Address Translation - NAT, RFC 1631) allows the translation of an Internet Protocol address used within one network to a different IP address known within another network.

### **DHCP (Dynamic Host Configuration Protocol)**

DHCP (Dynamic Host Configuration Protocol) allows the individual clients (workstations) 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 now also act as a surrogate DHCP server (DHCP Relay) where it relays IP address assignment from the actual real DHCP server to the clients.



## **Full Network Management**

This feature allows you to access the SMT (System Management Terminal) through the console port or telnet connection.

## **RoadRunner Support**

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

## **Time and Date Setting**

This new feature (Menu 24.10) allows you to get the current time and date from an external server when you power up your ZyWALL. The real time is then displayed in the ZyWALL error logs and firewall logs. If you do not choose a time service protocol that your timeserver will send when the ZyWALL powers up, you can enter the time manually but each time the system is booted, the time and date will be reset to 2000/01/0100:00:00.

## **Logging and Tracing**

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

## **Upgrade ZyWALL Firmware via LAN**

The firmware of the ZyWALL 10 can be upgraded via the LAN.

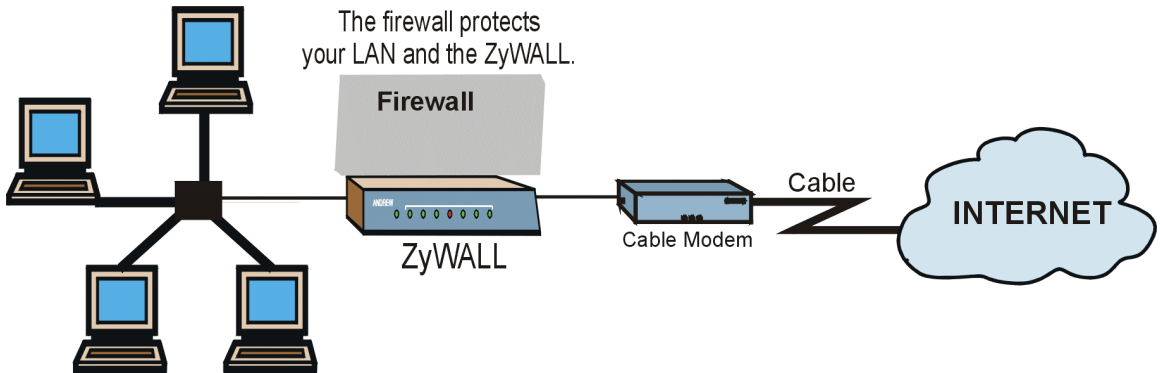
## **Embedded FTP and TFTP Servers**

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

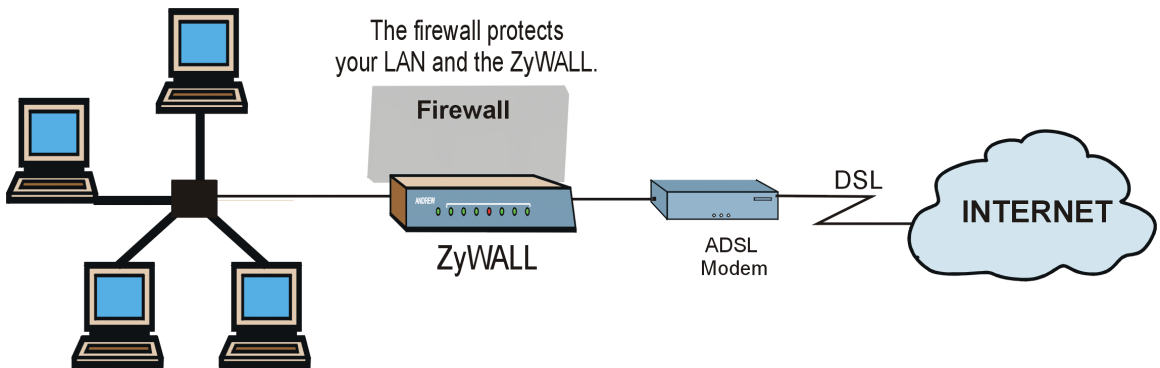
# **1.3 Applications for ZyWALL 10**

## **1.3.1 Broadband Internet Access via Cable or xDSL Modem**

A cable modem or xDSL modem can connect to the ZyWALL 10 for broadband Internet access via Ethernet port on the modem. It provides not only high speed Internet access, but secured internal network protection and management as well.



**Figure 1-1 Secure Internet Access via Cable**



**Figure 1-2 Secure Internet Access via DSL**

You can also use your xDSL modem in the bridge mode for always-on Internet access and high-speed data transfer.

# Chapter 2

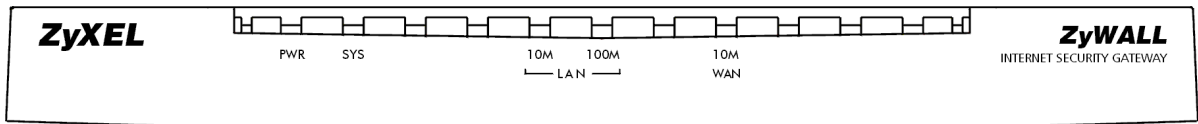
## Hardware Installation & Initial Setup

*This chapter explains the LEDs and ports as well as how to connect the hardware and perform the initial setup.*

### 2.1 Front Panel LEDs and Back Panel Ports

#### 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 the LED functions:

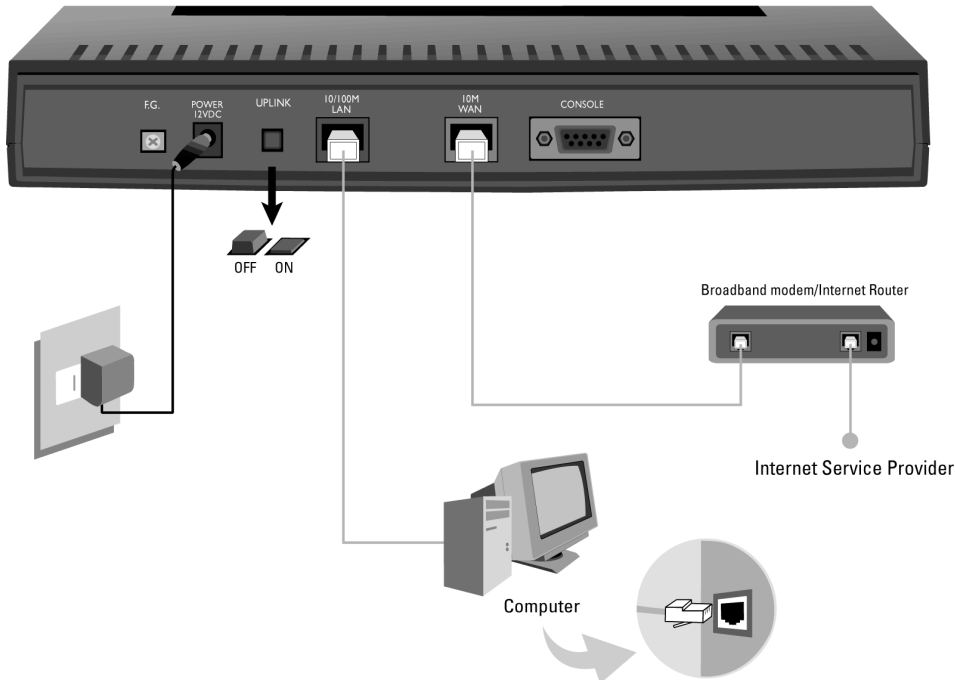
**Table 2-1 LED functions**

LEDS	FUNCTION	INDICATOR STATUS	ACTIVE	DESCRIPTION
PWR	Power	Green	On	The power adapter is connected to the ZyWALL.
SYS	System		Off	The system is not ready or failed.
			On	The system is ready and running.
			Flashing	The system is rebooting.
10M LAN	LAN	Green	Off	The 10M LAN is not connected.
			On	The ZyWALL is connected to a 10M LAN.
			Flashing	The 10M LAN is sending/receiving packets.
100M LAN	LAN	Orange	Off	The 100M LAN is not connected.
			On	The ZyWALL is connected to a 100Mbps LAN.
			Flashing	The 100M LAN is sending/receiving packets.

LEDS	FUNCTION	INDICATOR STATUS	ACTIVE	DESCRIPTION
WAN	WAN	Green	Off	The WAN Link is not ready, or has failed.
			On	The WAN Link is OK.
			Flashing	The 10M WAN link is sending/receiving packets.

## 2.2 ZyWALL 10 Rear Panel and Connections

The following figure shows the rear panel of your ZyWALL 10 and the related connections.



**Figure 2-2 ZyWALL 10 Rear Panel and Connections**

This section outlines how to connect your ZyWALL 10 to the LAN and the WAN. In the case of connecting a cable modem you must connect the coaxial cable from your cable service to the threaded coaxial cable connector on the back of the cable modem. Connect an xDSL Modem to the xDSL Wall Jack. Please also see *Appendix C* for important safety instructions on making connections to the ZyWALL.

### Step 1. Connecting the Console Port

For the initial configuration of your ZyWALL, you need to use terminal emulator software on a workstation and connect it to the ZyWALL through the console port. Connect the 9-pin end of the console cable to the

console port of the ZyWALL and the other end (choice of 9-pin or 25-pin, depending on your computer) end to a serial port (COM1, COM2 or other COM port) of your workstation. You can use an extension RS-232 cable if the enclosed one is too short. After the initial setup, you can modify the configuration remotely through telnet connections.

## Step 2. Connecting the ZyWALL to the Broadband Modem

### Step 2a. Connecting the ZyWALL to the Cable Modem:

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

**OR**

### Step 2b. Connecting the ZyWALL to the xDSL Modem:

Connect the WAN port (silver) on the ZyWALL to the Ethernet port on the xDSL modem using the cable that came with your xDSL modem.

## Step 3. Connecting the ZyWALL to the LAN

For a single computer, connect the 10/100M LAN port on the ZyWALL to the Network Adapter on the computer using the white straight-through cable and push in the Uplink button ("on"). If the Uplink button is not "on", you must use a crossover cable for this connection.

If you have more than one computer, then you must use an external hub. Connect the 10/100M LAN port (gold) on the ZyWALL to a port on the hub using a straight-through Ethernet cable and make sure the Uplink button is "off".

## Connecting the Power Adapter to your ZyWALL

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

**Caution: To prevent damage to the ZyWALL, first make sure you have the correct AC power adapter. Please see the *Appendices* for AC power adapter specifications for your region.**

## Step 4. Grounding the ZyWALL

To ground the ZyWALL, connect a grounded wire to the **F.G.** (Frame Ground) of the ZyWALL.

## 2.3 Additional Installation Requirements

In addition to the contents of your package, there are other hardware and software requirements you need before you can install and use your ZyWALL. These requirements include:

1. A computer with an Ethernet NIC (Network Interface Card) installed.
2. A computer equipped with communications software configured to the following parameters:
  - ◆ VT100 terminal emulation.
  - ◆ 9600 Baud.
  - ◆ No parity, 8 Data bits, 1 Stop bit, Flow Control set to None.

### 3. A cable/xDSL modem and an ISP account.

After the ZyWALL is properly set up, you can make future changes to the configuration through telnet connections.

## 2.4 Turn On Your ZyWALL

At this point, you should have connected the console port, the LAN port, the WAN port and the power port to the appropriate devices or lines. Plug the power adapter into a wall outlet. The Power LED should be on. The SYS LED will come on after the system tests are complete. The WAN LED and one of the LAN LEDs come on immediately after the SYS LED comes on, if connections have been made to the LAN and WAN ports.

### Initial Screen

When you turn on your ZyWALL, it performs several internal tests as well as line initialization.

After the tests, the ZyWALL asks you to press [ENTER] to continue, as shown next.

```
Copyright (c) 1994 - 2001 ZyXEL Communications Corp.
initialize ch =0, ethernet address: 00:a0:c5:41:51:61
initialize ch =1, ethernet address: 00:a0:c5:41:51:62
Press ENTER to continue...
```

**Figure 2-3 Initial Screen**

### Entering Password

The login screen appears after you press [ENTER], prompting you to enter the password, as shown below. For your first login, enter the default password 1234. As you type the password, the screen displays an (X) for each character you type.

Please note that if there is no activity for longer than five minutes after you log in, your ZyWALL will automatically log you out and will display a blank screen. If you see a blank screen, press [ENTER] to bring up the login screen again.

```
Enter Password : XXXX
```

**Figure 2-4 Password Screen**

## 2.5 Navigating the SMT Interface

The SMT (System Management Terminal) is the interface that you use to configure your ZyWALL.

Several operations that you should be familiar with before you attempt to modify the configuration are listed in the table below.

**Table 2-2 Main Menu Commands**

OPERATION	KEYSTROKES	DESCRIPTION
Move down to another menu	[ENTER]	To move forward to a submenu, type in the number of the desired submenu and press [ENTER].
Move up to a previous menu	[ESC]	Press the [ESC] key to move back to the previous menu.
Move to a "hidden" menu	Press the [SPACE BAR] to change <b>No</b> to <b>Yes</b> then press [ENTER].	Fields beginning with "Edit" lead to hidden menus and have a default setting of <b>No</b> . Press the [SPACE BAR] to change <b>No</b> to <b>Yes</b> , then press [ENTER] to go to a "hidden" menu.
Move the cursor	[ENTER] or [UP]/[DOWN] arrow keys	Within a menu, press [ENTER] to move to the next field. You can also use the [UP]/[DOWN] arrow keys to move to the previous and the next field, respectively.
Enter information	Fill in, or press the [SPACE BAR] to select from choices.	You need to fill in two types of fields. The first requires you to type in the appropriate information. The second allows you to cycle through the available choices by pressing the [SPACE BAR].
Required fields	<? >	All fields with the symbol <?> must be filled in order be able to save the new configuration.
N/A fields	<N/A>	Some of the fields in the SMT will show a <N/A>. This symbol refers to an option that is Not Applicable.
Save your configuration	[ENTER]	Save your configuration by pressing [ENTER] at the message "Press ENTER to confirm or ESC to cancel". Saving the data on the screen will take you, in most cases to the previous menu.
Exit the SMT	Type 99, then press [ENTER].	Type 99 at the main menu prompt and press [ENTER] to exit the SMT interface.

## 2.5.1 Main Menu

After you enter the password, the SMT displays the **ZyWALL 10 Main Menu**, as shown next.

```
Copyright (c) 1994 - 2001 ZyXEL Communications Corp.

ZyWALL Main Menu

Getting Started                Advanced Management

1. General Setup              21. Filter and Firewall Setup
2. WAN Setup                  22. SNMP Configuration
3. LAN Setup                  23. System Password
4. Internet Access Setup     24. System Maintenance

Advanced Applications          26. Schedule Setup
11. Remote Node Setup
12. Static Routing Setup
15. NAT Setup

99. Exit

Enter Menu Selection Number:
```

**Figure 2-5 ZyWALL 10 Main Menu**



## 2.5.2 System Management Terminal Interface Summary

**Table 2-3 Main Menu Summary**

<b>NO.</b>	<b>MENU TITLE</b>	<b>FUNCTION</b>
1	General Setup	Use this menu to set up routing/bridging and general information.
2	WAN Setup	Use this menu to clone a MAC address from a computer on your LAN.
3	Ethernet Setup	Use this menu to configure LAN DHCP and TCP/IP settings as well as apply LAN filters.
4	Internet Access Setup	Configure your Internet Access setup (Internet address, gateway, login, etc.) with this menu.
11	Remote Node Setup	Use this menu to configure detailed remote node settings (your ISP is also a remote node) as well as apply WAN filters.
12	Static Routing Setup	Configure static routes for bridging and IP in this menu.
15	NAT Setup	Use this menu to configure Network Address Translation.
21	Filter and Firewall Setup	Configure filters, activate/deactivate the firewall and view the firewall log.
22	SNMP Configuration	Use this menu to configure SNMP-related parameters.
23	System Password	Change your password in this menu (recommended).
24	System Maintenance	From displaying system status to uploading firmware, this menu provides comprehensive system maintenance.
26	Schedule Setup	Use this menu to schedule outgoing calls.
99	Exit	Use this menu to exit (necessary for remote configuration).

### 2.5.3 SMT Menus at a Glance

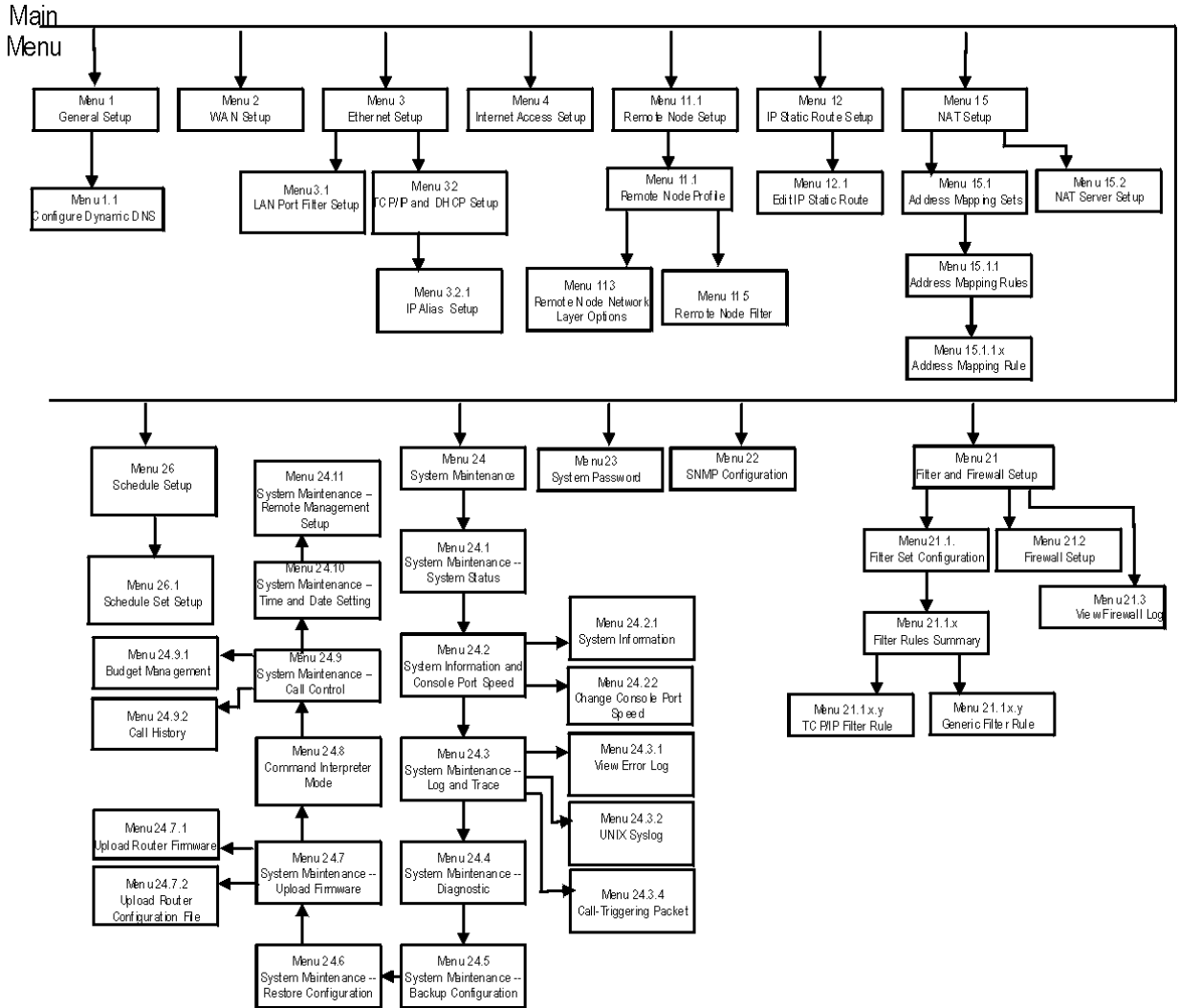
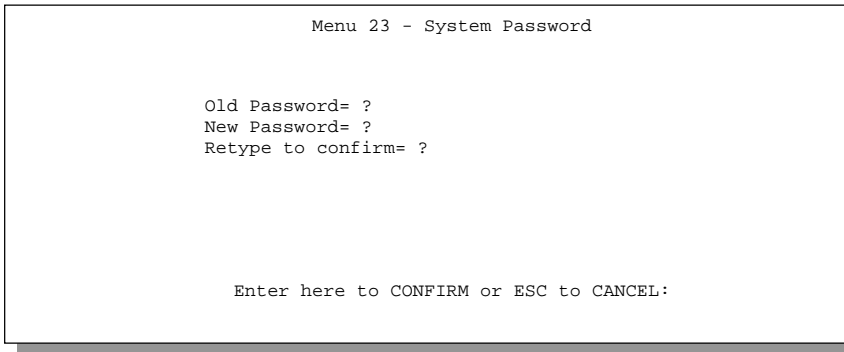


Figure 2-6 SMT Menus at a Glance

## 2.6 Changing the System Password

The first thing you should do is change the default system password by following the steps shown next.

**Step 1.** Enter 23 in the main menu to open **Menu 23 - System Password** as shown below.



**Figure 2-7 Menu 23 — System Password**

**Step 2.** Enter your existing password and press [ENTER].

**Step 3.** Enter your new system password and press [ENTER].

**Step 4.** Re-type your new system password for confirmation and press [ENTER].

Note that as you type a password, the screen displays an (X) for each character you type.

### 2.6.1 Resetting the ZyWALL

If you have forgotten your password or cannot access the SMT menu you will need to reinstall the configuration file. Uploading the configuration file replaces the current configuration file with the default configuration file, you will lose all configurations that you had before and the speed of the console port will be reset to the default of 9600bps with 8 data bit, no parity and 1 stop bit (8n1). The password will be reset to the default of 1234, also.

Turn off the ZyWALL and begin a Terminal session with the current console port settings. Turn on the ZyWALL again. When you see the message "Press Any key to enter Debug Mode within 3 seconds", press any key to enter debug mode. You should already have downloaded the correct file from your nearest ZyXEL FTP site. See *Chapter 9* for more information on how to transfer the configuration file to your ZyWALL.

## 2.7 General Setup

**Menu 1 - General Setup** contains administrative and system-related information. **System Name** is for identification purposes. ZyXEL recommends you enter your computer's "Computer name". Click Start -> Settings -> Control Panel -> Network; click the Identification tab and note the entry for the "Computer name" field.

The **Domain Name** entry is what is propagated to the DHCP clients on the LAN. If you leave this field blank, the domain name obtained by DHCP from the ISP is used. While you must enter the host name (**System Name**) on each individual machine, the domain name can be assigned from the ZyWALL via DHCP.

## 2.7.1 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 (e.g. *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. To use this service, you must register with the Dynamic DNS client. The Dynamic DNS Client service provider will give you a password or key. The ZyWALL at the time of writing supports [www.ddns.org](http://www.ddns.org) and [www.dyndns.org](http://www.dyndns.org) clients. You can apply to either of these clients for Dynamic DNS service.

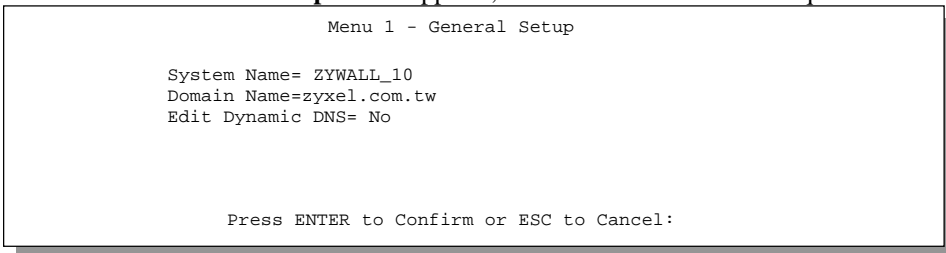
### DYNDNS Wildcard

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

## 2.7.2 Procedure For Configuring Menu 1

**Step 1.** Enter 1 in the Main Menu to open **Menu 1 — General Setup**.

**Step 2.** The **Menu 1 - General Setup** screen appears, as shown next. Fill in the required fields.



**Figure 2-8 Menu 1 — General Setup**

**Table 2-4 General Setup Menu Field**

FIELD	DESCRIPTION	EXAMPLE
System Name	Choose a descriptive name for identification purposes. It is recommended you enter your computer's "Computer name" in this field. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.	ZyWALL_10
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. You can go to menu 24.8 and type "sys domain name" to see the current domain name used by your router.  If you want to clear this field just press the [SPACE BAR]. The domain name entered by you is given priority over the ISP assigned domain name.	zyxel.com.tw
Edit Dynamic DNS	Press the [SPACE BAR] to select <b>Yes</b> or <b>No</b> (default). Select <b>Yes</b> to configure <b>Menu 1.1 — Configure Dynamic DNS</b> discussed next.	
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.		

### 2.7.3 Configuring Dynamic DNS

To configure Dynamic DNS, go to **Menu 1 — General Setup** and use the [SPACE BAR] to select **Yes** in the **Edit Dynamic DNS** field. Press [ENTER] to display **Menu 1.1— Configure Dynamic DNS** (shown next).

```

Menu 1.1 - Configure Dynamic DNS

Service Provider = WWW.DynDNS.ORG
Active= Yes
Host= me.ddns.org
EMAIL= mail@mailserver
User= username
Password= *****
Enable Wildcard= No

Press ENTER to confirm or ESC to cancel:

```

**Figure 2-9 Configure Dynamic DNS**

Follow the instructions in the next table to configure Dynamic DNS parameters.

**Table 2-5 Configure Dynamic DNS Menu Fields**

FIELD	DESCRIPTION	EXAMPLE
Service Provider	Enter the name of your Dynamic DNS client.	www.dyndns.org
Active	Press [SPACE BAR] to cycle between <b>Yes</b> or <b>No</b> .	<b>Yes</b>
Host	Enter the domain name assigned to your ZyWALL by your Dynamic DNS provider.	me.dyndns.org
EMAIL	Enter your e-mail address.	mail@mailserver
User	Enter your user name.	
Password	Enter the password assigned to you.	
Enable Wildcard	Your ZyWALL supports DYNDNS Wildcard. Press [SPACE BAR] to cycle between <b>Yes</b> or <b>No</b> This field is <b>N/A</b> when you choose DDNS client as your service provider.	<b>Yes</b>
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.		

The IP address will be updated when you reconfigure Menu 1 or perform DHCP client renewal.

---

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

---

## 2.8 WAN Setup

This section describes how to configure the WAN using **Menu 2 — WAN Setup**. From the main menu, enter 2 to open menu 2.

---

ZyXEL recommends you configure this menu even if your ISP does not require MAC address authentication.

---

```

Menu 2 - WAN Setup
MAC Address:
Assigned By=IP address attached on LAN
IP Address= 192.168.1.12

Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle
    
```

**Figure 2-10 Menu 2 — WAN Setup**

The MAC address field allows users to configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a computer on your LAN. 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 in menu 2 or upload a different rom file.

The following table contains instructions on how to configure your WAN setup.

**Table 2-6 WAN Setup Menu Fields**

FIELD	DESCRIPTION	EXAMPLE
MAC Address		
Assigned By	Press the [SPACE BAR] to choose either of the two methods of assigning a MAC Address. Choose <b>Factory Default</b> to select the factory assigned default MAC Address. Choose <b>IP Address attached on LAN</b> to use the MAC Address of that workstation whose IP you give in the following field.	<b>Factory Default</b>
IP Address	This field is applicable only if you choose the <b>IP Address attached on LAN</b> method. Enter the IP address of the workstation on the LAN whose MAC you are cloning.	192.168.1.1
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.		

## 2.9 LAN Setup

This section describes how to configure the LAN using **Menu 3 — LAN Setup**. From the main menu, enter 3 to open menu 3.

```
Menu 3 - LAN Setup

1. LAN Port Filter Setup
2. TCP/IP and DHCP Setup

Enter Menu Selection Number:
```

**Figure 2-11 Menu 3 — LAN Setup**

### 2.9.1 LAN Port Filter Setup

This menu allows you to specify the filter sets that you wish to apply to the LAN traffic. You seldom need to filter the LAN traffic, however, the filter sets may be useful to block certain packets, reduce traffic and prevent security breaches.

```
Menu 3.1 - LAN Port Filter Setup

Input Filter Sets:
  protocol filters= 2
  device filters=
Output Filter Sets:
  protocol filters=
  device filters=

Press ENTER to Confirm or ESC to Cancel:
```

**Figure 2-12 Menu 3.1 — LAN Port Filter Setup**

Menu 3.2 is discussed in the next chapter. Please read on.



# Chapter 3

## Internet Access

*This chapter shows you how to configure the LAN as well as the WAN of your ZyWALL for Internet access.*

### 3.1 TCP/IP and DHCP for LAN

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

#### 3.1.1 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 an explicit DNS server address(es), skip ahead to section 3.2 to see how to enter the DNS server address(es).

#### 3.1.2 DHCP Configuration

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows the individual clients to obtain the 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 sever on your LAN, or else the workstation must be manually configured.

##### 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 machines, e.g., server for mail, FTP, telnet, web, etc., that you may have.

##### DNS Server Address

DNS (Domain Name System) is to map a domain name to its corresponding IP address and vice versa, e.g., the IP address of *www.zyxel.com* is 204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it.

There are two ways that an ISP disseminates the DNS server addresses. The first is for an ISP to tell a customer the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP does give you the DNS server addresses, enter them in the **DNS Server** fields in DHCP Setup. The second is to leave this field blank, i.e., 0.0.0.0 — in this case the ZyWALL acts as a DNS proxy.

### 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)

### 3.1.3 IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, the machines on a LAN share one common network number, also.

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 3 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, e.g., 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.

### 3.1.4 Private IP Addresses

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

10.0.0.0 — 10.255.255.255  
172.16.0.0 — 172.31.255.255  
192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP or 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*.

---

### 3.1.5 RIP Setup

RIP (Routing Information Protocol, RFC1058 and RFC 1389) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. 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.

The **Version** field controls the format and the broadcasting method of the RIP packets that the ZyWALL sends (it recognizes both formats when receiving). **RIP-1** is universally supported; but **RIP-2** carries more information. **RIP-1** is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also.

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

### 3.1.6 IP 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.

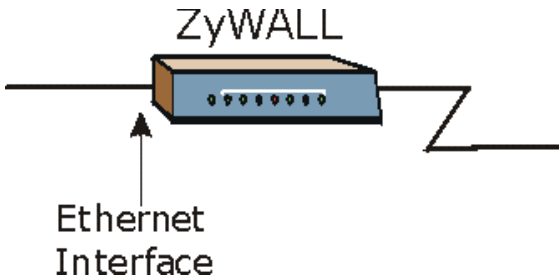
IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed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

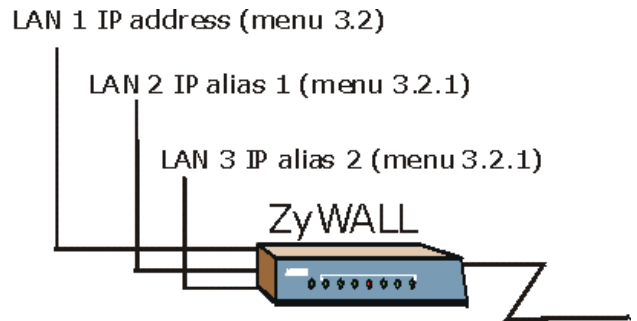
WAN interfaces using menus 3.2 (LAN) and 11.3 (WAN). Select **None** to disable IP Multicasting on these interfaces.

### 3.1.7 IP Alias

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



**Figure 3-1 Physical Network**

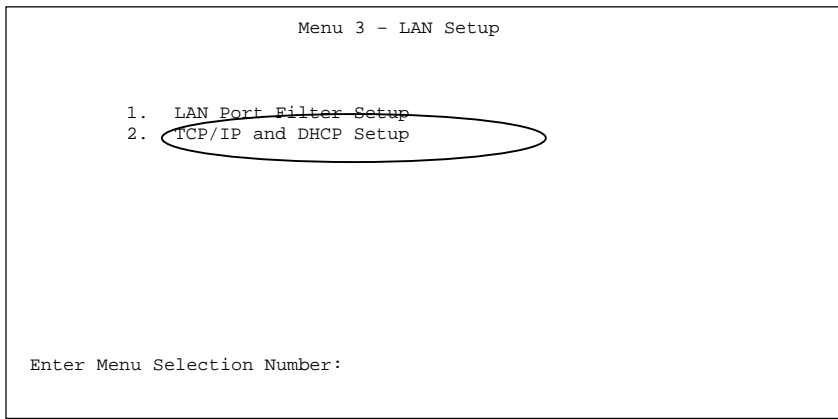


**Figure 3-2 Partitioned Logical Networks**

Use menu 3.2.1 to configure IP Alias on your ZyWALL.

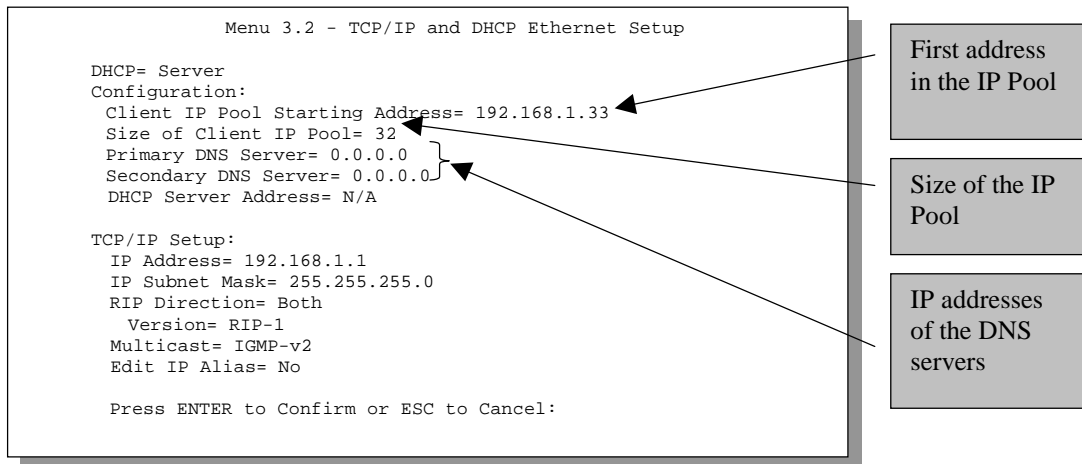
## 3.2 TCP/IP and DHCP Ethernet Setup

From the main menu, enter 3 to open **Menu 3 - LAN Setup** to configure TCP/IP (RFC 1155) and DHCP Ethernet setup.



**Figure 3-3 Menu 3 — LAN Setup**

From menu 3, select the submenu option **TCP/IP and DHCP Setup** and press [ENTER]. The screen now displays **Menu 3.2 — TCP/IP and DHCP Ethernet Setup**, as shown.



**Figure 3-4 Menu 3.2 — TCP/IP and DHCP Ethernet Setup**

Follow the instructions in the next table on how to configure the DHCP fields.

**Table 3-1 DHCP Ethernet Setup Menu Fields**

FIELD	DESCRIPTION	EXAMPLE
DHCP	This field enables/disables the DHCP server. If set to <b>Server</b> , your ZyWALL will act as a DHCP server. If set to <b>None</b> , the DHCP server will be disabled. If set to <b>Relay</b> , the ZyWALL acts as a surrogate DHCP server and relays requests and responses between the remote server and the clients.  When set to <b>Server</b> , the following four items need to be set:	<b>Server</b>
Configuration		
Client IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.	192.168.1.33
Size of Client IP Pool	This field specifies the size, or count of the IP address pool.	32
Primary DNS Server	Type in the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.	
Secondary DNS Server		
DHCP Server Address	If <b>Relay</b> is selected in the <b>DHCP</b> field above, then type in the IP address of the actual, remote DHCP server here.	

Follow the instructions in the following table to configure TCP/IP parameters for the LAN port.

**Table 3-2 LAN TCP/IP Setup Menu Fields**

FIELD	DESCRIPTION	EXAMPLE
TCP/IP Setup		
IP Address	Enter the IP address of your ZyWALL in dotted decimal notation	192.168.1.1 (default)
IP Subnet Mask	Your ZyWALL will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyWALL	255.255.255.0
RIP Direction	Press the [SPACE BAR] to select the RIP direction from <b>Both, In Only, Out Only or None</b> .	<b>Both</b> (default)
Version	Press the [SPACE BAR] to select the RIP version from <b>RIP-1/RIP-2B/RIP-2M</b> .	<b>RIP-1</b> (default)

FIELD	DESCRIPTION	EXAMPLE
Multicast	IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group. The ZyWALL supports both IGMP version 1 ( <b>IGMP-v1</b> ) and version 2 ( <b>IGMP-v2</b> ). Press the [SPACE BAR] to enable IP Multicasting or select <b>None</b> (default) to disable it.	<b>None</b>
Edit IP Alias	The ZyWALL supports three logical LAN interfaces via its single physical Ethernet interface with the ZyWALL itself as the gateway for each LAN network. Press the [SPACE BAR] to toggle <b>No</b> to <b>Yes</b> , then press [ENTER] to bring you to menu 3.2.1	<b>Yes</b>

When you have completed this menu, press [ENTER] at the prompt [Press ENTER to Confirm...] to save your configuration, or press [ESC] at any time to cancel.

### 3.2.1 IP Alias Setup

You must use menu 3.2 to configure the first network and move the cursor to the **Edit IP Alias** field and press [SPACE BAR] to choose **Yes** and press [ENTER] to configure the second and third network. Pressing [ENTER] opens **Menu 3.2.1 - IP Alias Setup**, as shown next.

```

Menu 3.2.1 - IP Alias Setup

IP Alias 1= No
IP Address= N/A
IP Subnet Mask= N/A
RIP Direction= N/A
Version= N/A
Incoming protocol filters= N/A
Outgoing protocol filters= N/A
IP Alias 2= No
IP Address= N/A
IP Subnet Mask= N/A
RIP Direction= N/A
Version= N/A
Incoming protocol filters= N/A
Outgoing protocol filters= N/A

Enter here to CONFIRM or ESC to CANCEL:

Press Space Bar to Toggle.

```

**Figure 3-5 Menu 3.2.1 — IP Alias Setup**

Use the instructions in the following table to configure IP Alias parameters.

**Table 3-3 IP Alias Setup Menu Fields**

<b>FIELD</b>	<b>DESCRIPTION</b>	<b>EXAMPLE</b>
IP Alias	Choose <b>Yes</b> to configure the LAN network for the ZyWALL.	<b>Yes</b>
IP Address	Enter the IP address of your ZyWALL in dotted decimal notation	192.168.2.1
IP Subnet Mask	Your ZyWALL will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyWALL	255.255.255.0
RIP Direction	Press the [SPACE BAR] to select the RIP direction from <b>Both, In Only, Out Only or None</b> .	<b>None</b>
Version	Press the [SPACE BAR] to select the RIP version from <b>RIP-1, RIP-2B or RIP-2M</b> .	<b>RIP-1</b>
Incoming Protocol Filters	Enter the filter set(s) you wish to apply to the incoming traffic between this node and the ZyWALL.	1
Outgoing Protocol Filters	Enter the filter set(s) you wish to apply to the outgoing traffic between this node and the ZyWALL.	2
When you have completed this menu, press [ENTER] at the prompt [Press ENTER to Confirm...] to save your configuration, or press [ESC] at any time to cancel.		

## 3.3 Internet Access Setup

You will see three different menu 4 screens depending on whether you chose **Ethernet, PPTP** or **PPPoE Encapsulation**.

### 3.3.1 Ethernet Encapsulation

You must choose the **Ethernet** option when the WAN port is used as a regular Ethernet. The PPPoE choice is for a dial-up connection using PPPoE. If you choose **Ethernet** in menu 4 you will see the next screen.



```

Menu 4 - Internet Access Setup

ISP's Name= ChangeMe
Encapsulation= Ethernet
  Service Type= Standard
  My Login= N/A
  My Password= N/A
  Login Server IP= N/A

IP Address Assignment= Dynamic
  IP Address= N/A
  IP Subnet Mask= N/A
  Gateway IP Address= N/A
Network Address Translation= Full Feature

Press ENTER to Confirm or ESC to Cancel:

```

**Figure 3-6 Menu 4 — Internet Access Setup (Ethernet)**

The following table describes this screen.

**Table 3-4 Internet Access Setup Menu Fields**

FIELD	DESCRIPTION
ISP's Name	Enter the name of your Internet Service Provider, e.g., myISP. This information is for identification purposes only.
Encapsulation	Press [SPACE BAR] and then press [ENTER] to choose <b>Ethernet</b> . The encapsulation method influences your choices for IP Address.
Service Type	Press the [SPACE BAR] to select <b>Standard</b> , <b>RR-Toshiba</b> (RoadRunner Toshiba authentication method) or <b>RR-Manager</b> (RoadRunner Manager authentication method). Choose a RoadRunner flavor if your ISP is Time Warner's RoadRunner; otherwise choose <b>Standard</b> .
Note: xDSL users must choose the <b>Standard</b> option only. The <b>Server IP</b> , <b>My Login IP</b> and <b>My Password</b> fields are not applicable in this case.	
My Login Name	Enter the login name given to you by your ISP.
My Password	Enter the password associated with the login name above.
Login Server IP	The ZyWALL will find the RoadRunner Server IP if this field is left blank. If it does not, then you must enter the authentication server IP address.
IP Address Assignment	If your ISP did not assign you a fixed IP address, select <b>Dynamic</b> , otherwise select <b>Static</b> and enter the IP address & subnet mask in the following fields.

FIELD	DESCRIPTION
IP Address	Enter the (fixed) IP address assigned to you by your ISP (Static IP Address Assignment is selected in the previous field).
IP Subnet Mask	Enter the subnet mask associated with your static IP.
Gateway IP Address	Enter the gateway IP address associated with your static IP.
Network Address Translation	Please see the NAT chapter for a more detailed discussion on the Network Address Translation feature. The choices are <b>Full Feature</b> , <b>None</b> and <b>SUA Only</b> .
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.	

### 3.3.2 PPTP Encapsulation

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks. PPTP supports on-demand, multi-protocol, and virtual private networking over public networks, such as the Internet.

---

The ZyWALL 10 supports only one PPTP server connection at any given time.

---

### 3.3.3 Configuring the PPTP Client

To configure a PPTP client, you must configure the **My Login** and **Password** fields for a PPP connection and the PPTP parameters for a PPTP connection.

After configuring **My Login** and **Password** for PPP connection, press [SPACE BAR] in the **Encapsulation** field in **Menu 4 -Internet Access Setup** to choose **PPTP** as your encapsulation option. This brings up the following screen.

```

Menu 4 - Internet Access Setup

ISP's Name= ChangeMe
Encapsulation= PPTP
Service Type= N/A
My Login= username
My Password= *****
Idle Timeout= 100

IP Address Assignment= Dynamic
IP Address= N/A
IP Subnet Mask= N/A
Gateway IP Address=N/A
Network Address Translation= SUA Only

Press ENTER to Confirm or ESC to Cancel:

```

**Figure 3-7 Internet Access Setup (PPTP)**

The following table contains instructions about the new fields when you choose **PPTP** in the **Encapsulation** field in **Menu 4**.

**Table 3-5 New Fields in Menu 4 (PPTP) screen**

FIELD	DESCRIPTION	EXAMPLE
Encapsulation	Press the [SPACE BAR] and then press [ENTER] to choose <b>PPTP</b> . The encapsulation method influences your choices for IP Address.	<b>PPTP</b>
Idle Timeout	This value specifies the time in seconds that elapses before the ZyWALL automatically disconnects from the PPTP server.	100 (default)

### 3.3.4 PPPoE Encapsulation

The ZyWALL supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF Draft standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (i.e. xDSL, cable, wireless, etc.) connection.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (e.g., Radius). For the user, PPPoE provides a login & 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 10 (rather than individual computer's), 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.

If you enable PPPoE in menu 4, you will see the next screen. For more information on PPPoE, please see *the Appendices*.

```

Menu 4 - Internet Access Setup

ISP's Name= ChangeMe
Encapsulation= PPPoE
Service Type=
My Login=
My Password= *****
Idle Timeout= 100

IP Address Assignment= Dynamic
IP Address= N/A
IP Subnet Mask= N/A
Gateway IP Address= N/A
Network Address Translation= Full Feature

Press ENTER to Confirm or ESC to Cancel:
    
```

**Figure 3-8 Internet Access Setup (PPPoE)**

**Table 3-6 New Fields in Menu 4 (PPPoE) screen**

FIELD	DESCRIPTION	EXAMPLE
Encapsulation	Press the [SPACE BAR] and then press [ENTER] to choose <b>PPPoE</b> . The encapsulation method influences your choices for IP Address.	<b>PPPoE</b>
Idle Timeout	This value specifies the time in seconds that elapses before the ZyWALL automatically disconnects from the PPPoE server.	100 (default)

If you need a PPPoE service name to identify and reach the PPPoE server, please go to menu 11 and enter the PPPoE service name provided to you in the **Service Name** field.

## 3.4 Basic Setup Complete

Well done! You have successfully connected, installed and set up your ZyWALL to operate on your network as well as access the Internet.

---

**Please note that when the firewall is activated, the default policy allows all communications to the Internet that originate from the LAN, and blocks all traffic to the LAN that originates from the Internet.**

---

You may deactivate the firewall in menu 21.2 or via the ZyWALL Web Configurator. You may also define additional firewall rules or modify existing ones but please exercise extreme caution in doing so. See *Part 4* for more information on the firewall.

---

---

# Part II:

---

## Advanced Applications

---

Chapters 4 — 6 describe advanced applications including Remote Node Setup, IP Static routes and NAT.

# Chapter 4

## Remote Node Setup

*This chapter shows you how to configure a remote node.*

A remote node is required for placing calls to a remote gateway. A remote node represents both the remote gateway and the network behind it across a WAN connection. Note that when you use menu 4 to set up Internet access, you are actually configuring a remote node. We will show you how to configure **Menu 11.1 Remote Node Profile**, **Menu 11.3 - Remote Node Network Layer Options** and **Menu 11.5 - Remote Node Filter**.

### 4.1 Remote Node Profile

From the main menu, select menu option 11 to open **Menu 11.1 - Remote Node Profile**. There are two variations of this menu depending on whether you choose **Ethernet Encapsulation** or **PPPoE Encapsulation**.

#### 4.1.1 Ethernet Encapsulation

You must choose the **Ethernet** option when the WAN port is used as a regular Ethernet. The first menu 11.1 screen you see is for Ethernet encapsulation shown next.

```
Menu 11.1 - Remote Node Profile

Rem Node Name= ChangeMe           Route= IP
Active= Yes

Encapsulation= Ethernet           Edit IP= No
Service Type= Standard           Session Options:
Service Name= N/A                Edit Filter Sets= No
Outgoing:
  My Login= N/A
  My Password= N/A
  Server IP= N/A

Press ENTER to Confirm or ESC to Cancel:
```

**Figure 4-1 Menu 11.1 — Remote Node Profile for Ethernet Encapsulation**

Table 4-1 Fields in Menu 11.1

FIELD	DESCRIPTION	EXAMPLE
Rem Node Name	Enter a descriptive name for the remote node. This field can be up to eight characters.	LAoffice
Active	Press [SPACE BAR] to select <b>Yes</b> (activate remote node) or <b>No</b> (deactivate remote node).	<b>Yes</b>
Encapsulation	<b>Ethernet</b> is the default encapsulation. Press the [SPACE BAR] if you wish to change to <b>PPPoE</b> encapsulation.	<b>Ethernet</b>
Service Type	Press [SPACE BAR] to select from <b>Standard</b> , <b>RR-Toshiba</b> (RoadRunner Toshiba authentication method) or <b>RR-Manager</b> (RoadRunner Manager authentication method). Choose one of the RoadRunner methods if your ISP is Time Warner's RoadRunner; otherwise choose <b>Standard</b> .	<b>Standard</b>
Service Name	This is valid only when you have chosen <b>PPPoE</b> encapsulation. If you are using <b>PPPoE</b> encapsulation, then type the name of your PPPoE service here.	poellc
Outgoing		
My Login	This field is applicable for <b>PPPoE</b> encapsulation only. Enter the login name assigned by your ISP when the ZyWALL calls this remote node. Some ISPs append this field to the <b>Service Name</b> field above (e.g., jim@poellc) to access the PPPoE server.	<b>jim</b>
My Password	Enter the password assigned by your ISP when the ZyWALL calls this remote node. Valid for <b>PPPoE</b> encapsulation only.	*****
Server IP	This field is valid for RoadRunner service type only. The ZyWALL will find the RoadRunner Server IP automatically if this field is left blank. If it does not, then you must enter the authentication server IP address here.	
Route	This field refers to the protocol that will be routed by your ZyWALL – IP is the only option for the ZyWALL 10.	<b>IP</b>
Edit IP	This field leads to a “hidden” menu. Press [SPACE BAR] to select <b>Yes</b> and press [ENTER] to go to <b>Menu 11.3 - Remote Node Network Layer Options</b> .	<b>Yes</b>
Session Options		
Edit Filter sets	This field leads to another “hidden” menu. Use the [SPACE BAR] to select <b>Yes</b> and press [ENTER] to open menu 11.5 to edit the filter sets. See the <i>Remote Node Filter</i> section for more details.	<b>Yes</b>



Once you have configured the Remote Node Profile Menu, press [ENTER] to return to menu 11. Press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.

### 4.1.2 PPPoE Encapsulation

The ZyWALL supports PPPoE (Point-to-Point Protocol over Ethernet). You can only use PPPoE encapsulation when you're using the ZyWALL with an xDSL modem as the WAN device. If you change the Encapsulation to **PPPoE**, then you will see the next screen. Please see the *Appendices* for more information on PPPoE.

```

Menu 11.1 - Remote Node Profile

Rem Node Name= ChangeMe          Route= IP
Active= Yes

Encapsulation= PPPoE             Edit IP= No
Service Type= Standard          Telco Option:
Service Name=                   Allocated Budget(min)= 0
Outgoing=                       Period(hr)= 0
  My Login=                      Schedules=
  My Password= *****          Nailed-Up Connection= No
  Authen= CHAP/PAP              Session Options:
                                Edit Filter Sets= No
                                Idle Timeout(sec)= 100

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.

```

**Figure 4-2 Menu 11.1 — Remote Node Profile for PPPoE Encapsulation**

#### Outgoing Authentication Protocol

Generally speaking, you should employ the strongest authentication protocol possible, for obvious reasons. However, some vendor's implementation includes specific authentication protocol in the user profile. It will disconnect if the negotiated protocol is different from that in the user profile, even when the negotiated protocol is stronger than specified. If you encounter the case where the peer disconnects right after a successful authentication, please make sure that you specify the correct authentication protocol when connecting to such an implementation.

#### Nailed-Up Connection

A nailed-up connection is a dial-up line where the connection is always up regardless of traffic demand. The ZyWALL does two things when you specify a nailed-up connection. The first is that idle timeout is disabled. The second is that the ZyWALL will try to bring up the connection when turned on and whenever the connection is down. A nailed-up connection can be very expensive for obvious reasons.

Do not specify a nailed-up connection unless your telephone company offers flat-rate service or you need a constant connection and the cost is of no concern.

The following table describes the fields not already described in *Table 4-1*.

**Table 4-2 Fields in Menu 11.1 (PPPoE Encapsulation Specific)**

FIELD	DESCRIPTION	EXAMPLE
Authen	This field sets the authentication protocol used for outgoing calls.  Options for this field are: <b>CHAP/PAP</b> - Your ZyWALL will accept either <b>CHAP</b> or <b>PAP</b> when requested by this remote node. <b>CHAP</b> - accept CHAP only. <b>PAP</b> - accept PAP only.	<b>CHAP/PAP</b>
Telco Option		
Allocated Budget	The field sets a ceiling for outgoing call time for this remote node. The default for this field is 0 meaning no budget control.	10
Period(hr)	This field is the time period that the budget should be reset. For example, if we are allowed to call this remote node for a maximum of 10 minutes every hour, then the <b>Allocated Budget</b> is (10 minutes) and the <b>Period(hr)</b> is 1 (hour).	1
Schedules	You can apply up to four schedule sets here. For more details please refer to the <i>Call Schedule Setup chapter</i> .	
Nailed-Up Connection	This field specifies if you want to make the connection to this remote node a nailed-up connection. More details are given earlier in this section.	
Session Options		
Idle Timeout	This value specifies the idle time (i.e., the length of time there is no traffic from the ZyWALL to the remote node) in seconds that can elapse before the ZyWALL automatically disconnects the PPPoE connection. <i>This option only applies when the ZyWALL initiates the call.</i>	100 seconds (default)

### 4.1.3 PPTP Encapsulation

If you change the Encapsulation to **PPTP** in menu 11.1, then you will see the next screen. Please see the *appendices* for information on PPTP.

```

Menu 11.1 - Remote Node Profile

Rem Node Name= ChangeMe           Route= IP
Active= Yes

Encapsulation= PPTP               Edit IP= No
Service Type= Standard           Telco Option:
Service Name=N/A                 Allocated Budget(min)= 0
Outgoing=                         Period(hr)= 0
  My Login=                       Schedules=
  My Password= *****           Nailed-up Connections=
  Authen= CHAP/PAP

PPTP :
  My IP Addr=                     Session Options:
  Server IP Addr=                 Edit Filter Sets= No
  Connection ID/Name=             Idle Timeout(sec)= 100

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.

```

**Figure 4-3 Menu 11.1 — Remote Node Profile for PPTP Encapsulation**

The next table shows how to configure fields in menu 11.1 not previously discussed above.

**Table 4-3 Fields in Menu 11.1 (PPTP Encapsulation)**

FIELD	DESCRIPTION	EXAMPLE
Encapsulation	Toggle the space bar to choose <b>PPTP</b> . You must also go to menu 11.3 to check the IP Address setting once you have selected the encapsulation method.	<b>PPTP</b>
My IP Addr	Enter the IP address of the WAN Ethernet port.	10.0.0.140
My Server IP Addr	Enter the IP address of the ANT modem.	10.0.0.138
Connection ID/Name	Enter the connection ID or connection name in the ANT. It must follow the "c:id" and "n:name" format.  This field is optional and depends on the requirements of your xDSL Modem.	N:My ISP
Schedules	You can apply up to four schedule sets here. For more details please refer to the <i>Call Schedule Setup</i> chapter.	
Nailed-Up Connections	Use the [SPACE BAR] to select <b>Yes</b> if you want to make the connection to this remote node a nailed-up connection.	<b>No</b>

## 4.2 Editing TCP/IP Options (with Ethernet Encapsulation)

Move the cursor to the **Edit IP** field in menu 11.1, then press the [SPACE BAR] to toggle and set the value to **Yes**. Press [ENTER] to open **Menu 11.3 - Network Layer Options**.

```

Menu 11.3 - Remote Node Network Layer Options

IP Address Assignment= Dynamic
IP Address= N/A
IP Subnet Mask= N/A
Gateway IP Addr= N/A

Network Address Translation= SUA Only
Metric= N/A
Private= N/A
RIP Direction= None
  Version= N/A
Multicast= None

Enter here to CONFIRM or ESC to CANCEL:
Press Space Bar to Toggle

```

**Figure 4-4 Menu 11.3 — Remote Node Network Layer Options**

The next table gives you instructions about configuring remote node network layer options.

**Table 4-4 Remote Node Network Layer Options Menu Fields**

FIELD	DESCRIPTION	EXAMPLE
IP Address Assignment	If your ISP did not assign you an explicit IP address, select <b>Dynamic</b> ; otherwise select <b>Static</b> and enter the IP address & subnet mask in the following fields.	<b>Dynamic</b>
IP Address	If you have a Static IP Assignment, enter the IP address assigned to you by your ISP.	
IP Subnet Mask	If you have a Static IP Assignment, enter the subnet mask assigned to you.	
Gateway IP Addr	If you have a Static IP Assignment, enter the gateway IP address assigned to you.	
Network Address Translation	Use the [SPACE BAR] to select either <b>Full Feature</b> , <b>None</b> or <b>SUA Only</b> . See the <i>NAT chapter</i> for a full discussion on this feature.	<b>SUA Only</b>
Metric	This field is valid only for PPTP/PPPoE encapsulation. The metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.	3

FIELD	DESCRIPTION	EXAMPLE
Private	This field is valid only for PPTP/PPPoE encapsulation. This parameter determines if the ZyWALL will include the route to this remote node in its RIP broadcasts. If set to <b>Yes</b> , this route is kept private and not included in RIP broadcast. If <b>No</b> , the route to this remote node will be propagated to other hosts through RIP broadcasts.	<b>Yes</b>
RIP	Press the [SPACE BAR] to select the RIP direction from <b>Both/None/In Only/Out Only</b> . Please see the <i>RIP Setup</i> section for more information on RIP. The default for RIP on the WAN side is <b>None</b> . It is recommended that you do not change this setting.	<b>None</b>
Version	Press the [SPACE BAR] to select the RIP version from <b>RIP-1/RIP-2B/RIP-2M</b> or <b>None</b> .	<b>None</b>
Multicast	IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group. The ZyWALL supports both IGMP version 1 ( <b>IGMP-v1</b> ) and version 2 ( <b>IGMP-v2</b> ). Press [SPACE BAR] to enable IP Multicasting or select <b>None</b> to disable it. See the previous <i>Part</i> for more information on this feature.	<b>IGMP-v2</b>
Once you have completed filling in the Network Layer Options Menu, press [ENTER] to return to menu 11. Press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.		

### 4.2.1 Editing TCP/IP Options (with PPTP Encapsulation)

Make sure that **Encapsulation** is set to **PPTP** in menu 11.1. Then move the cursor to the **Edit IP** field in menu 11.1, press the [SPACE BAR] to toggle **No** to **Yes**. Press [ENTER] to open **Menu 11.3 - Network Layer Options**.

```

Menu 11.3 - Remote Node Network Layer Options

IP Address Assignment= Dynamic
Rem IP Address= N/A
Rem Subnet Mask= N/A
My WAN Addr= 0.0.0.0

Network Address Translation= Full Feature
Metric= 1
Private= No
RIP Direction= None
Version= N/A
Multicast= None

Enter here to CONFIRM or ESC to CANCEL:
Press Space Bar to Toggle.
    
```

**Figure 4-5 Menu 11.3 — Remote Node Network Layer Options**

The next table gives you instructions about configuring remote node network layer options.

**Table 4-5 Remote Node Network Layer Options Menu Fields**

FIELD	DESCRIPTION	EXAMPLE
IP Address Assignment	If your ISP did not assign you an explicit IP address, select <b>Dynamic</b> ; otherwise select <b>Static</b> and enter the IP address & subnet mask in the following fields.	<b>Dynamic</b>
Rem IP Address	If you have a <b>Static IP Assignment</b> , enter the IP address assigned to the remote node.	192.168.1.1
Rem IP Subnet Mask	If you have a <b>Static IP Assignment</b> , enter the subnet mask assigned to the remote node.	255.255.255.0
My WAN Addr	Some implementations, especially the UNIX derivatives, require the WAN link to have a separate IP network number from the LAN and each end must have a unique address within the WAN network number. If this is the case, enter the IP address assigned to the WAN port of your ZyWALL.  Note that this is the address assigned to your local ZyWALL, not the remote router.	
Network Address Translation	Use the [SPACE BAR] to select either <b>Full Feature</b> , <b>None</b> or <b>SUA Only</b> . See the <i>NAT chapter</i> for a full discussion on this feature.	<b>SUA Only</b>
Metric	The metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good	1 to 15

FIELD	DESCRIPTION	EXAMPLE
	number.	
Private	This parameter determines if the ZyWALL will include the route to this remote node in its RIP broadcasts. If set to <b>Yes</b> , this route is kept private and not included in RIP broadcast. If <b>No</b> , the route to this remote node will be propagated to other hosts through RIP broadcasts.	<b>Yes</b>
RIP	Press the [SPACE BAR] to select the <b>RIP direction</b> from <b>Both/None/In Only/Out Only</b> and <b>None</b> .	<b>None</b> (default)
Version	Press the [SPACE BAR] to select the RIP version from <b>RIP-1/RIP-2B/RIP-2M</b> .	<b>RIP-1</b>
Multicast	IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group. The ZyWALL supports both IGMP version 1 ( <b>IGMP-v1</b> ) and version 2 ( <b>IGMP-v2</b> ). Press the [SPACE BAR] to enable IP Multicasting or select <b>None</b> to disable it. See the previous Part for more information on this feature.	<b>None</b>
Once you have completed filling in the Network Layer Options Menu, press [ENTER] to return to menu 11. Press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.		

### 4.2.2 Editing TCP/IP Options (with PPPoE Encapsulation)

Make sure **Encapsulation** is set to **PPPoE** in menu 11.1. Move the cursor to the **Edit IP** field in **Menu 11.1** and press the [SPACE BAR] to select **Yes**. Press [ENTER] to open **Menu 11.3 - Network Layer Options**. The menu and fields are the same as described for PPTP encapsulation above.

### 4.3 Remote Node Filter

Move the cursor to the field **Edit Filter Sets** in menu 11.1, then press the [SPACE BAR] to set the value to **YES**. Press [ENTER] to open **Menu 11.5 - Remote Node Filter**.

Use menu 11.5 to specify the filter set(s) to apply to the incoming and outgoing traffic between this remote node and the ZyWALL to prevent certain packets from triggering calls. You can specify up to 4 filter sets separated by commas, e.g., 1, 5, 9, 12, in each filter field. Note that spaces are accepted in this field. For more information on defining the filters, please refer to the *Filters chapter*. For PPPoE or PPTP encapsulation, you can also specify remote node call filter sets.

```
Menu 11.5 - Remote Node Filter

Input Filter Sets:
  protocol filters= 3
  device filters=
Output Filter Sets:
  protocol filters= 1
  device filters=

Enter here to CONFIRM or ESC to CANCEL:
```

**Figure 4-6 Menu 11.5 — Remote Node Filter (Ethernet Encapsulation)**

```
Menu 11.5 - Remote Node Filter

Input Filter Sets:
  protocol filters= 3
  Device filters=
Output Filter Sets:
  protocol filters= 1
  device filters=
Call Filter Sets:
  protocol filters= 1
  Device filters=

Enter here to CONFIRM or ESC to CANCEL:
```

**Figure 4-7 Menu 11.5 — Remote Node Filter (PPPoE or PPTP Encapsulation)**



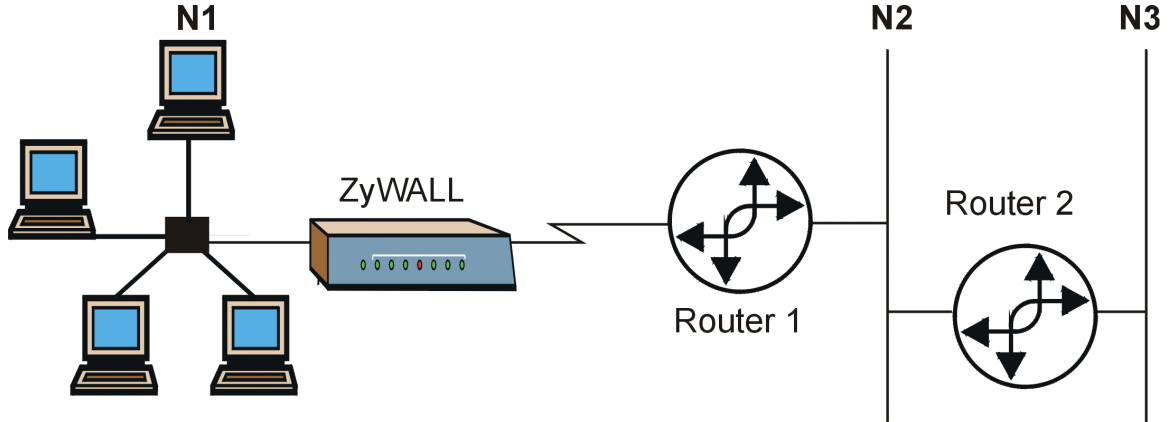
# Chapter 5

## IP Static Route Setup

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

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.

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 diagram 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 5-1 Example of Static Routing Topology**

## 5.1 IP Static Route Setup

You configure IP static routes in menu 12. 1, by selecting one of the IP static routes as shown below. Enter 12 from the main menu.

```
Menu 12 - IP Static Route Setup

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____

Enter selection number:
```

**Figure 5-2 Menu 12 — IP Static Route Setup**

Now, enter the index number of one of the static routes you want to configure.

```
Menu 12.1 - Edit IP Static Route

Route #: 1
Route Name= ?
Active= No
Destination IP Address= ?
IP Subnet Mask= ?
Gateway IP Address= ?
Metric= 2
Private= No

Press ENTER to CONFIRM or ESC to CANCEL:
```

**Figure 5-3 Menu 12. 1 — Edit IP Static Route**

The following table describes the IP Static Route Menu fields.

**Table 5-1 IP Static Route Menu Fields**

FIELD	DESCRIPTION
Route #	This is the index number of the static route that you chose in menu 12.
Route Name	Enter a descriptive name for this route. This is for identification purposes only.
Active	This field allows you to activate/deactivate this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask for this destination.
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your ZyWALL that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your ZyWALL; over the WAN, the gateway must be the IP address of one of the Remote Nodes.
Metric	Metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Private	This parameter determines if the ZyWALL will include the route to this remote node in its RIP broadcasts. If set to <b>Yes</b> , this route is kept private and not included in RIP broadcast. If <b>No</b> , the route to this remote node will be propagated to other hosts through RIP broadcasts.
Once you have completed filling in this menu, press [ENTER] at the message “Press ENTER to Confirm...” to save your configuration, or press [ESC] to cancel.	



# Chapter 6

## Network Address Translation (NAT)

*This chapter discusses how to configure NAT on the ZyWALL.*

### 6.1 Introduction

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet, e.g., the source address of an outgoing packet, used within one network to a different IP address known within another network.

#### 6.1.1 NAT Definitions

Inside/outside denotes where a host is located relative to the ZyWALL, e.g., the workstations of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router, e.g., the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is travelling in the WAN side.

Note that inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

**Table 6-1 NAT Definitions**

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

The IP address (either local or global) of an outside host is never changed.

#### 6.1.2 What NAT Does

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, e.g., a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping – see below), NAT offers the additional benefit of firewall protection. If no server is defined in these cases, all incoming inquiries will be filtered out by your ZyWALL, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631, The IP Network Address Translator (NAT)*.

### 6.1.3 How NAT works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The ZyWALL keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

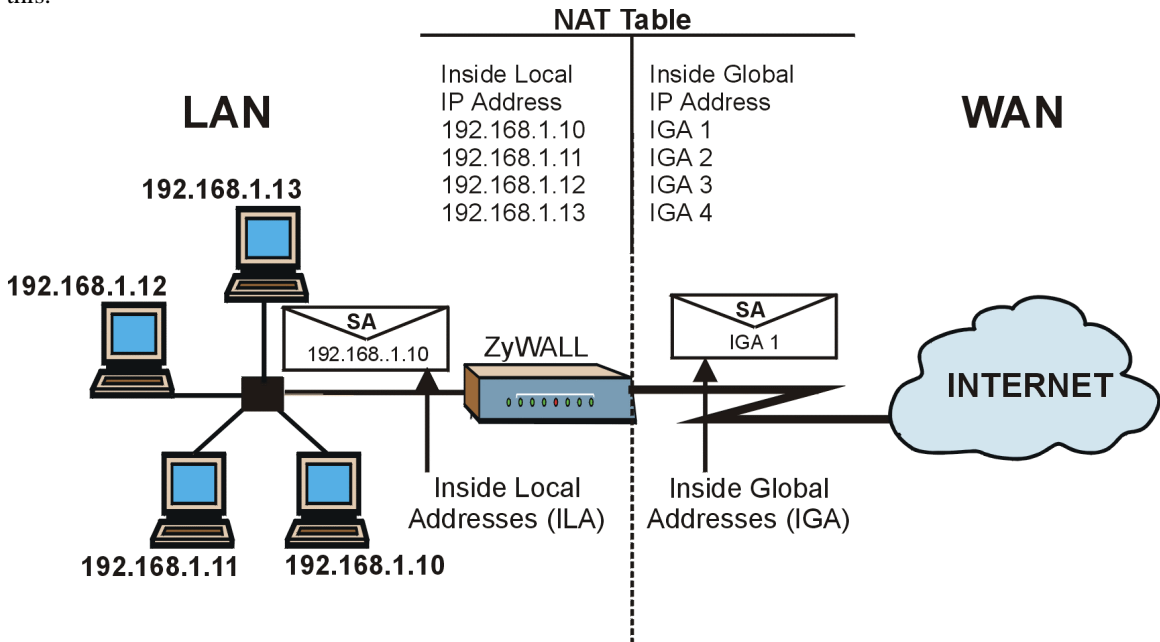


Figure 6-1 How NAT Works

## 6.1.4 NAT Mapping Types

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

1. **One to One:** In One-to-One mode, the ZyWALL maps one local IP address to one global IP address.
2. **Many to One:** In Many-to-One mode, the ZyWALL maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported (the SUA Only option in today's routers).
3. **Many to Many Overload:** In Many-to-Many Overload mode, the ZyWALL maps the multiple local IP addresses to shared global IP addresses.
4. **Many to Many No Overload:** In Many-to-Many No Overload mode, the ZyWALL maps the each local IP addresses to unique global IP addresses.
5. **Server:** This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.

---

Port numbers do *not* change for One-to-One and Many-to-Many-No Overload NAT mapping types.

---

The following table summarizes these types.

**Table 6-2 NAT Mapping Types**

TYPE	IP MAPPING	SMT ABBREVIATION
One-to-One	ILA1 ↔ IGA1	1:1
Many-to-One (SUA/PAT)	ILA1 ↔ IGA1 ILA2 ↔ IGA1 ...	M:1
Many-to-Many Overload	ILA1 ↔ IGA1 ILA2 ↔ IGA2 ILA3 ↔ IGA1 ILA4 ↔ IGA2 ...	M:M Ov
Many-to-Many No Overload	ILA1 ↔ IGA1 ILA2 ↔ IGA2 ILA3 ↔ IGA3 ...	M:M No Ov

TYPE	IP MAPPING	SMT ABBREVIATION
Server	Server 1 IP $\leftrightarrow$ IGA1 Server 2 IP $\leftrightarrow$ IGA1 Server 3 IP $\leftrightarrow$ IGA1	Server

### 6.1.5 SUA (Single User Account) Versus NAT

SUA (Single User Account) in previous ZyNOS versions is a subset of NAT that supports two types of mapping, Many-to-One and Server. See section 6.2.3 for a detailed description of the NAT set for SUA. The ZyWALL now has Full Feature NAT support to map global IP addresses to local IP addresses of clients or servers using all mapping types as outlined in Table 6-2. The ZyWALL supports NAT sets on a remote node basis. They are reusable, but only one set is allowed for each remote node. The ZyWALL 10 supports 2 sets since there is only one remote node. The second set (**SUA Only** option in menu 15.1) is a convenient, pre-configured, read only Many-to-One port mapping set, sufficient for most purposes (see section 6.4 for some examples) and helpful to people already familiar with SUA in previous ZyNOS versions.

### 6.1.6 NAT Application

The following figure illustrates a possible NAT application, where three inside LANs (logical LANs using IP Alias) behind the ZyWALL can “talk” to three distinct Internet destinations. More examples follow at the end of this chapter.



Corporation B

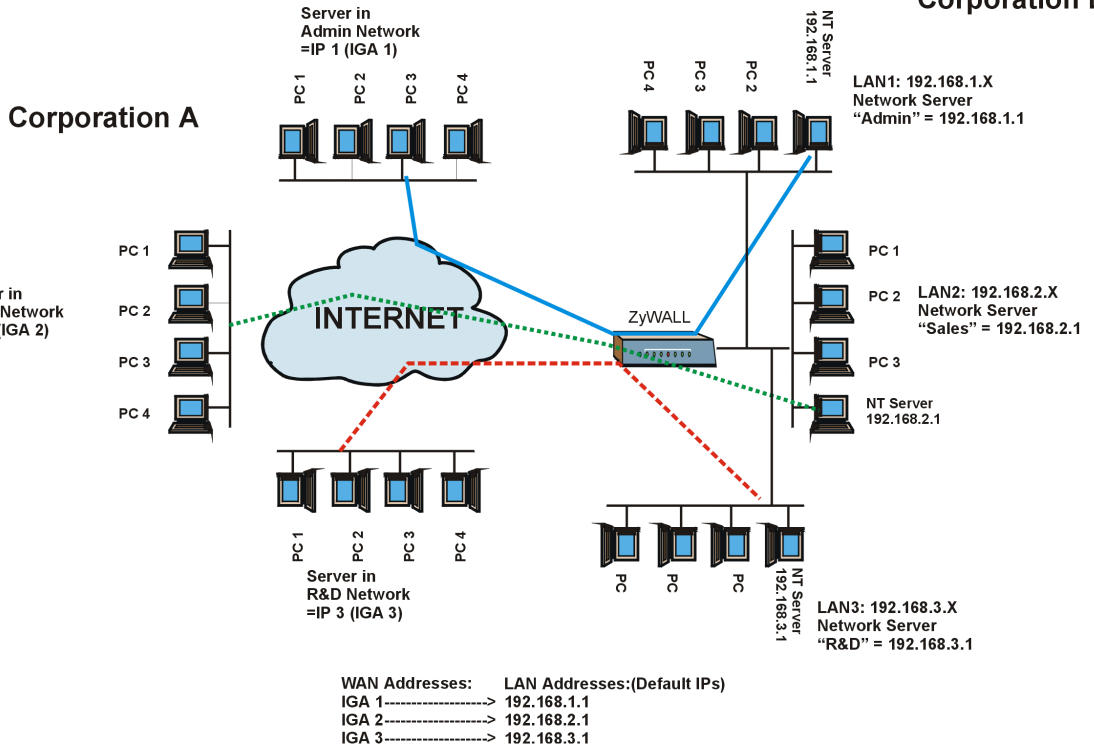


Figure 6-2 NAT Application

## 6.2 SMT Menus

### 6.2.1 Applying NAT in the SMT Menus

You apply NAT via menus 4 or 11.3 as displayed next. The next figure shows you how to apply NAT for Internet access in menu 4. Enter 4 from the main menu to go to **Menu 4 - Internet Access Setup**.

```
Menu 4 - Internet Access Setup

ISP's Name= ChangeMe
Encapsulation= Ethernet
Service Type= Standard
My Login= N/A
My Password= N/A
Login Server IP= N/A

IP Address Assignment= Dynamic
IP Address= N/A
IP Subnet Mask= N/A
Gateway IP Address= N/A
Network Address Translation= SUA Only

Press ENTER to Confirm or ESC to Cancel:
```

**Figure 6-3 Menu 4 — Applying NAT for Internet Access**

The following figure shows how you apply NAT to the remote node in menu 11.1.

- Step 1.** Enter 11 from the main menu.
- Step 2.** Move the cursor to the **Edit IP** field, press the [SPACE BAR] to select **Yes** and then press [ENTER] to bring up **Menu 11.3 - Remote Node Network Layer Options**.

```
Menu 11.3 - Remote Node Network Layer Options

IP Address Assignment= Dynamic
IP Address= N/A
IP Subnet Mask= N/A
Gateway IP Addr= N/A

Network Address Translation= Full Feature
Metric= N/A
Private= N/A
RIP Direction= None
Version= N/A
Multicast= None
```

**Figure 6-4 Menu 11.3 — Applying NAT to the Remote Node**

The following table describes the options for Network Address Translation.

**Table 6-3 Applying NAT in Menus 4 & 11.3**

FIELD	OPTIONS	DESCRIPTION
Network Address Translation	<b>Full Feature</b>	When you select this option the SMT will use Address Mapping Set 1 (menu 15.1 - see section 6.2.3 for further discussion). You can configure any of the mapping types described in <i>Table 6-2</i> .
	<b>None</b>	NAT is disabled when you select this option.
	<b>SUA Only</b>	When you select this option the SMT will use Address Mapping Set 255 (menu 15.1 - see section 6.2.3). It is a convenient, pre-configured, read only Many-to-One port mapping set, sufficient for most purposes and helpful to people already familiar with SUA in previous ZyNOS versions. Note that there is also a Server type whose IGA is 0.0.0.0 in this set.

## 6.2.2 Configuring NAT

To configure NAT, enter 15 from the main menu to bring up the following screen.

```

Menu 15 - NAT Setup

1.  Address Mapping Sets
2.  Server Set

Enter Menu Selection Number:

```

**Figure 6-5 Menu 15 — NAT Setup**

## 6.2.3 Address Mapping Sets and NAT Server Sets:

Use the Address Mapping Sets menus and submenus to create the mapping table used to assign global addresses to machines on the LAN. Each remote node must specify which NAT Address Mapping Set to use. The ZyWALL 10 has one remote node and so allows you to configure only one NAT Address Mapping Set. You can see two NAT Address Mapping sets in menu 15.1. You can only configure Set 1. Set 255 is used for SUA. When you select **Full Feature** in menu 4 or 11.3, the SMT will use Set 1, which supports all mapping types as outlined in *Table 6-2*. When you select **SUA Only**, the SMT will use the pre-configured Set 255 (read only) – see *section 6.1.5*.

The Server Set is a list of LAN side servers mapped to external ports. To use this set (one set for the ZyWALL 10), a server rule must be set up inside the NAT Address Mapping set. Please see *section 6.3* for further information on these menus.

Enter 1 to bring up **Menu 15.1 — Address Mapping Sets.**

```

Menu 15.1 - Address Mapping Sets

    1. NAT_SET
    255. SUA (read only)

Enter Menu Selection Number:
    
```

**Figure 6-6 Menu 15.1 — Address Mapping Sets**

---

1. NAT\_SET is a set name that was created as an example. Information about creating your own address mapping sets is provided later in the chapter.

---

Let’s look first at Option 255. Option 255 is equivalent to SUA in previous ZyXEL routers (see *section 6.1.5*). The fields in this menu cannot be changed. Entering 255 brings up this screen.

```

Menu 15.1.255 - Address Mapping Rules

Set Name= SUA

Idx  Local Start IP  Local End IP  Global Start IP  Global End IP  Type
---  -
1.   0.0.0.0         255.255.255.255  0.0.0.0         0.0.0.0       M-1
2.
3.
4.
5.
6.
7.
8.
9.
10.

Press ENTER to Confirm or ESC to Cancel:
    
```

**Figure 6-7 Menu 15.1.255 — SUA Address Mapping Rules**

The following table explains the fields in this screen.

---

The fields in this menu are read-only. The Type, Local and Global Start/End IPs are normally (not for this read-only menu) configured in menu 15.1.1.1 (described later) and the values are displayed here.

---

**Table 6-4 SUA Address Mapping Rules**

FIELD	DESCRIPTION	EXAMPLE
Set Name	This is the name of the set you selected in menu 15.1 or enter the name of a new set you want to create.	<b>SUA</b>
Idx	This is the index or rule number.	1
Local Start IP Local End IP	<b>Local Start IP</b> is the starting local IP address (ILA) (see <i>Figure 6-1</i> ). <b>Local End IP</b> is the ending local IP address (ILA). If the rule is for all local IPs, then the Start IP is 0.0.0.0 and the End IP is 255.255.255.255.	0.0.0.0 255.255.255.255
Global Start IP	This is the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the <b>Global Start IP</b> .	0.0.0.0
Global End IP	This is the ending global IP address (IGA).	<b>N/A</b>
Type	These are the mapping types discussed above (see <i>Table 6-2</i> ). Type Server allows us to specify multiple servers of different types behind NAT to this machine. See <i>section 6.4.3</i> below for some examples.	<b>Server</b>
Press [ENTER] to confirm or [ESC] to cancel.		

For all Local and Global IPs, the End IP address must begin after the IP Start address.

Now let's look at Option 1 in menu 15.1. Enter 1 to bring up this menu. We'll just look at the differences from the previous menu. Note that, this screen is not read only, so we have extra **Action** and **Select Rule** fields. Note also that the [?] in the **Set Name** field means that this is a required field and you must enter a name for the set.

If the Set Name field is left blank, the entire set will be deleted.

```

Menu 15.1.1 - Address Mapping Rules

Set Name= NAT_SET

Idx  Local Start IP  Local End IP  Global Start IP  Global End IP  Type
---  -
1.
2.
3.
4.
5.
6.
7.
8.
9.
10.

Action= Edit      Select Rule=

Press ENTER to Confirm or ESC to Cancel:
    
```

**Figure 6-8 Menu 15.1.1 — First Set**

---

The Type, Local and Global Start/End IPs are configured in menu 15.1.1.1 (described later) and the values are displayed here.

---

### Ordering Your Rules

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

The description of the other fields is as described above. The Type, Local and Global Start/End IPs are configured in menu 15.1.1.1 (described later) and the values are displayed here.

**Table 6-5 Fields in Menu 15.1.1**

FIELD	DESCRIPTION	EXAMPLE
Set Name	Enter a name for this set of rules. This is a required field. Please note that if this field is left blank, the entire set will be deleted.	NAT_SET
Action	There are four actions. The default is <b>Edit</b> . <b>Edit</b> means you want to edit a selected rule (see following field). <b>Insert Before</b> means to insert a rule before the rule selected. The rules after the selected rule will then be moved down by one rule. <b>Delete</b> means to delete the selected rule and then all the rules after the selected one will be advanced one rule. <b>None</b> disables the <b>Select Rule</b> item.	<b>Edit</b>
Select Rule	When you choose <b>Edit</b> , <b>Insert Before</b> or <b>Delete</b> in the previous field the cursor jumps to this field to allow you to select the rule to apply the action in question.	1

You must press [ENTER] at the bottom of the screen to save the whole set. You must do this again if you make any changes to the set – including deleting a rule. No changes to the set take place until this action is taken.

Be careful when ordering your rules as each rule is executed in turn beginning from rule 1.

Selecting **Edit** in the **Action** field and then selecting a rule brings up the following menu, **Menu 15.1.1.1 - Address Mapping Rule** in which you can edit an individual rule and configure the **Type**, **Local** and **Global Start/End IPs**.

```

Menu 15.1.1.1 Address Mapping Rule

Type= One-to-One

Local IP:
  Start=
  End = N/A

Global IP:
  Start=
  End = N/A

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.

```

**Figure 6-9 Menu 15.1.1.1 — Editing an Individual Rule in a Set**

The following table describes the fields in this screen.

**Table 6-6 Menu 15.1.1.1 — Configuring an Individual Rule**

FIELD	DESCRIPTION	EXAMPLE
Type	Press the [SPACE BAR] to toggle through a total of five types. These are the mapping types discussed above (see <i>Table 6-2</i> ). Type Server allows you to specify multiple servers of different types behind NAT to this machine. See <i>section 6.4.3 below</i> shown next for some examples.	<b>One-to-One</b>
Local IP	Only local IP fields are <b>N/A</b> for server; Global IP fields <b>MUST</b> be set for Server.	
Start	This is the starting local IP address (ILA).	0.0.0.0
End	This is the ending local IP address (ILA). If the rule is for all local IPs, then put the Start IP as 0.0.0.0 and the End IP as 255.255.255.255. This field is <b>N/A</b> for One-to-One and Server types.	255.255.255.255
Global IP		
Start	This is the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the <b>Global IP Start</b> . Note that <b>Global IP Start</b> can be set to 0.0.0.0 only if the types are Many-to-One or Server.	0.0.0.0
End	This is the ending global IP address (IGA). This field is <b>N/A</b> for <b>One-to-One</b> , <b>Many-to-One</b> and <b>Server types</b> .	172.16.23.55
Once you have finished configuring a rule in this menu, press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration, or press [ESC] to cancel.		

For all Local and Global IPs, the End IP address must begin after the IP Start address, i.e., you cannot have an End IP address beginning before the Start IP address.

## 6.3 NAT Server Sets

A NAT server set is a list of inside servers (behind NAT on the LAN) that you can make visible to the outside world. **Menu 15.2 — NAT Server Sets** is used to configure these servers. Entry 12 set to port 1026 is displayed in *Figure 6-11* and is non-editable.



### 6.3.1 Multiple Servers behind NAT

If you wish, you can make inside servers for different services, e.g., web or FTP, visible to the outside users, even though NAT makes your whole inside network appear as a single machine to the outside world. A service is identified by the port number, e.g., web service is on port 80 and FTP on port 21.

As an example (see the following figure), if you have a web server at 192.168.1.36 and an FTP server at 192.168.1.33, then you need to specify for port 80 (web) the server at IP address 192.168.1.36 and for port 21 (FTP) another at IP address 192.168.1.33.

Please note that a server can support more than one service, e.g., a server can provide both FTP and DNS service, while another provides only web service.

In addition to the servers for specified services, SUA supports a default server. A service request that does not have a server explicitly designated for it is forwarded to the default server. If the default is not defined, the service request is simply discarded.

To make a server visible to the outside world, specify the port number of the service and the inside IP address of the Server in **Menu 15 SUA Server Setup**.

Private Network IP Addresses  
Assigned by User

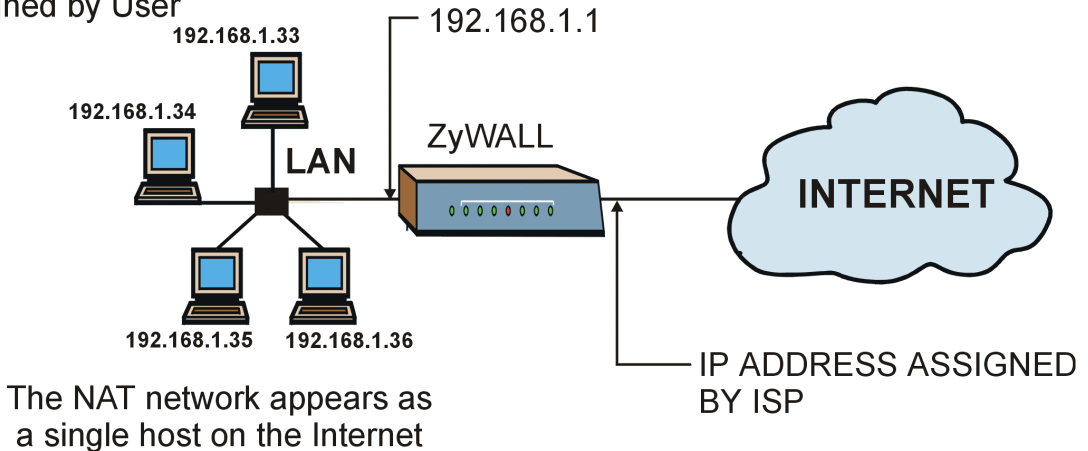


Figure 6-10 Multiple Servers Behind NAT

### 6.3.2 Configuring a Server behind NAT

Follow the steps below to configure a server behind NAT:

- Step 1.** Enter 15 in the main menu to go to **Menu 15 - NAT Setup**.
- Step 2.** Enter 2 to go to **Menu 15.2 - NAT Server Setup**.
- Step 3.** Enter the service port number in the **Port #** field and the inside IP address of the server in the **IP Address** field.

**Step 4.** Press [ENTER] at the “Press ENTER to confirm ...” prompt to save your configuration after you define all the servers or press [ESC] at any time to cancel.

**If you're using Ethernet Encapsulation the SMT does not allow you to change the port 1026 entry.**

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 our included disk for more examples and details on NAT.

```

Menu 15.2 - NAT Server Setup
Port #      IP Address
-----
1.Default   0.0.0.0
2.21        192.168.1.33
3.23        192.168.1.34
4.25        192.168.1.35
5.80        192.168.1.36
6. 0        0.0.0.0
7. 0        0.0.0.0
8. 0        0.0.0.0
9. 0        0.0.0.0
10. 0       0.0.0.0
11. 0       0.0.0.0
12. 1026    RR Reserved

Press ENTER to Confirm or ESC to Cancel:
    
```

**Figure 6-11 Menu 15.2 — NAT Server Setup**

**Table 6-7 Services & Port numbers**

SERVICES	PORT NUMBER
FTP (File Transfer Protocol)	21
Telnet	23
SMTP (Simple Mail Transfer Protocol)	25
DNS(Domain Name System)	53
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
PPTP (Point-to-Point Tunneling Protocol)	1723

## 6.4 Examples

### 6.4.1 Internet Access Only

In the following Internet access example, you only need one rule where all your ILAs (Inside Local addresses) map to one dynamic IGA (Inside Global Address) assigned by your ISP.

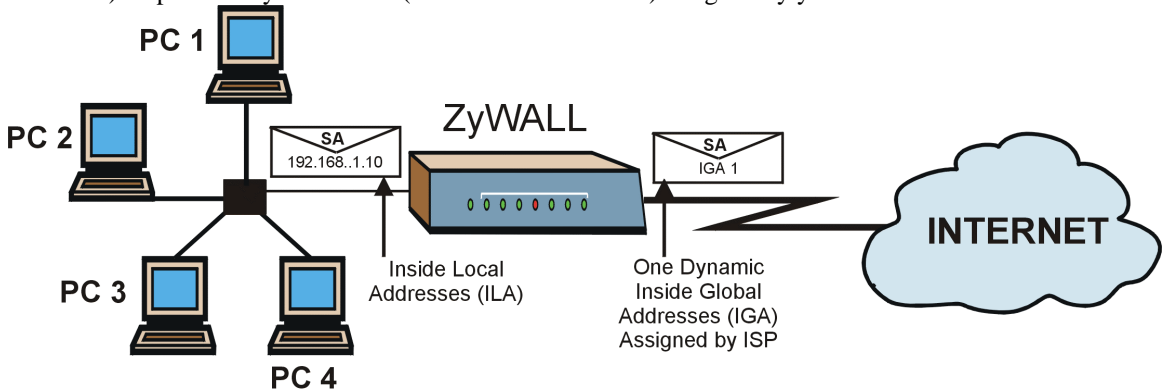


Figure 6-12 NAT Example 1

```

Menu 4 - Internet Access Setup

ISP's Name= ChangeMe
Encapsulation= Ethernet
Service Type= Standard
My Login= N/A
My Password= N/A
Login Server IP= N/A

IP Address Assignment= Dynamic
IP Address= N/A
IP Subnet Mask= N/A
Gateway IP Address= N/A
Network Address Translation= SUA Only

Press ENTER to Confirm or ESC to Cancel:

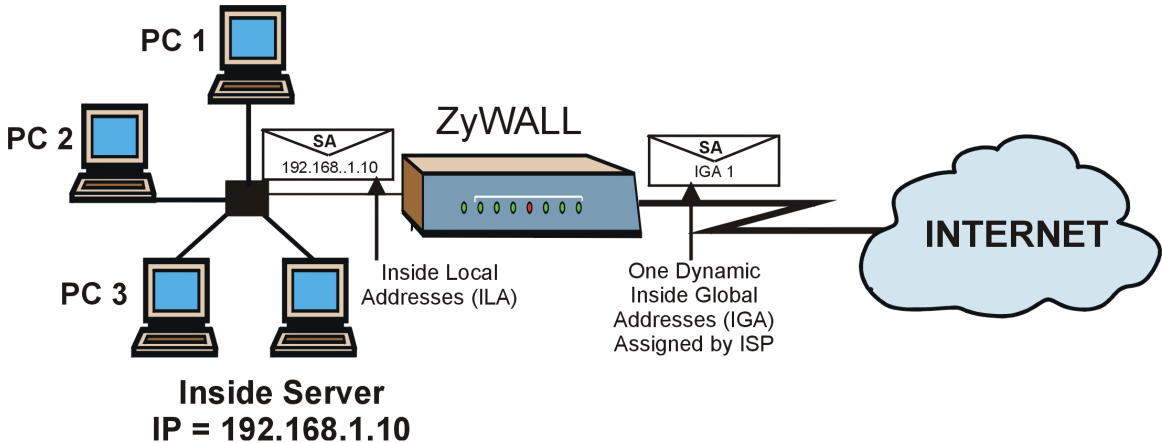
```

Figure 6-13 Menu 4 — Internet Access & NAT Example

From menu 4 shown above, simply choose the **SUA Only** option from the **Network Address Translation** field. This is the Many-to-One mapping discussed in *section 6.1.4*. The **SUA Only** read only option from

the **Network Address Translation** field in menus 4 and 11.3 is specifically pre-configured to handle this case.

### 6.4.2 Example 2: Internet Access with an Inside Server



**Figure 6-14 NAT Example 2**

In this case, you do exactly as above (use the convenient pre-configured **SUA Only** set) and also go to menu 15.2 to specify the Inside Server behind the NAT as shown in the next figure.

```

Menu 15.2 - NAT Server Setup
Port #      IP Address
-----
1.Default   192.168.1.10
2. 0        0.0.0.0
3. 0        0.0.0.0
4. 0        0.0.0.0
5. 0        0.0.0.0
6. 0        0.0.0.0
7. 0        0.0.0.0
8. 0        0.0.0.0
9. 0        0.0.0.0
10. 0       0.0.0.0
11. 0       0.0.0.0
12. 1026    RR Reserved

Press ENTER to Confirm or ESC to Cancel:
    
```

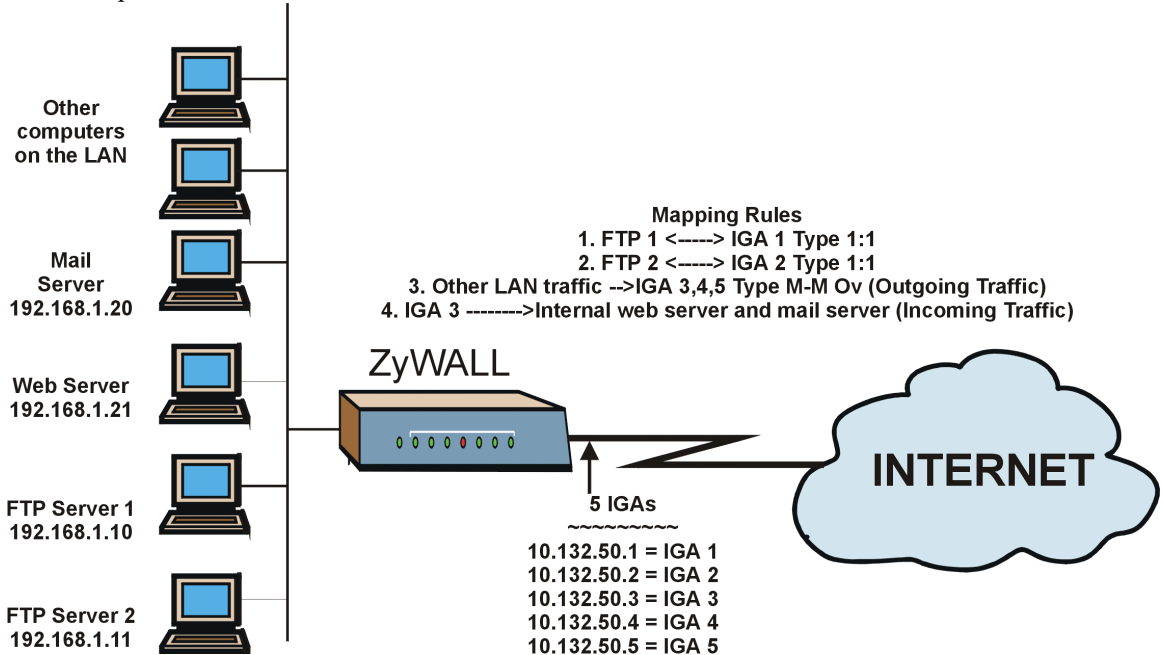
**Figure 6-15 Menu 15.2 — Specifying an Inside Server**

### 6.4.3 Example 3: General Case

In this example, there are 3 IGAs from our ISP. There are many departments but two have their own FTP server. All departments share the same router. The example will reserve one IGA for each department with an FTP server and the other IGA is used by all. Now you map the FTP servers to the first two IGAs and the other LAN traffic to the remaining IGA. Map the third IGA to an inside web server and mail server. Four rules need to be configured, two bi-directional and two one directional as follows.

- Rule 1.** Map the first IGA to the first inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).
- Rule 2.** Map the second IGA to our second inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).
- Rule 3.** Map the other outgoing LAN traffic to IGA3 (**Many : 1** mapping).
- Rule 4.** You also map your third IGA to the web server and mail server on the LAN. Type **Server** allows you to specify multiple servers, of different types, to other machines behind NAT on the LAN.

The example situation looks somewhat like this:



**Figure 6-16 NAT Example 3**

- Step 1.** In this case you need to configure Address Mapping Set 1 from **Menu 15.1 - Address Mapping Sets**. Therefore you must choose the **Full Feature** option from the **Network Address Translation** field (in menu 4 or menu 11.3) in *Figure 6-17*.
- Step 2.** Then enter 15 from the main menu.

- Step 3.** Enter 1 to configure the Address Mapping Sets.
- Step 4.** Enter 1 to begin configuring this new set. Enter a Set Name, choose the **Edit Action** and then enter 1 for the **Select Rule** field. Press [ENTER] to confirm.
- Step 5.** Select **Type** as **One-to-One** (direct mapping for packets going both ways), and enter the local **Start IP** as 192.168.1.10 (the IP address of FTP Server 1), the global **Start IP** as 10.132.50.1 (our first IGA). (See *Figure 6-18*)
- Step 6.** Repeat the previous step for rules 2 to 4 as outlined above.
- Step 7.** When finished, menu 15.1.1 should look like as shown in *Figure 6-19*.

```
Menu 11.3 - Remote Node Network Layer Options

IP Address Assignment= Dynamic
IP Address= N/A
IP Subnet Mask= N/A
Gateway IP Addr= N/A

Network Address Translation= Full Feature
Metric= N/A
Private= N/A
RIP Direction= None
Version= N/A
```

**Figure 6-17 Example 3: Menu 11.3**

The following figure shows how to configure the first rule.

```
Menu 15.1.1.1 Address Mapping Rule

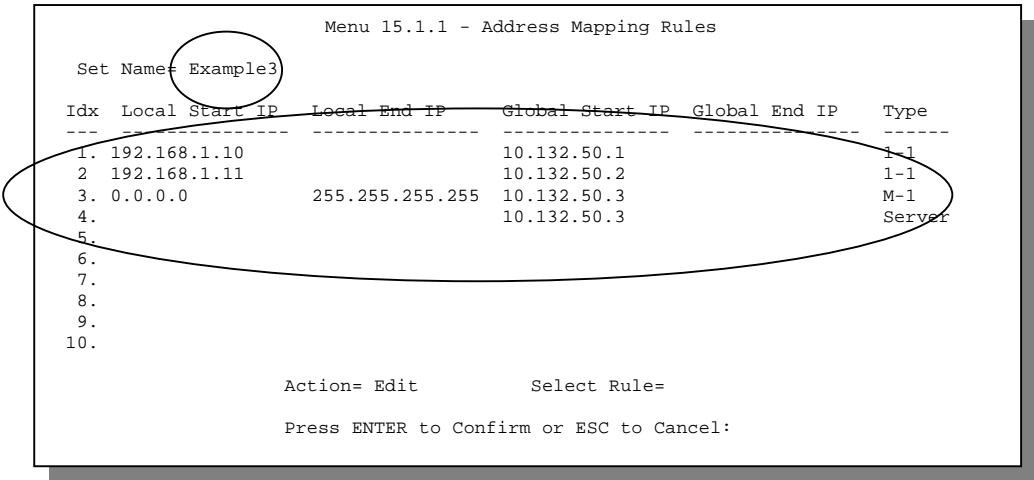
Type= One-to-One
Local IP:
  Start= 192.168.1.10
  End = N/A
Global IP:
  Start= 10.132.50.1
  End = N/A

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

**Figure 6-18 Example 3: Menu 15.1.1.1**

When you have configured all four rules, Menu 15.1.1 should look as follows.

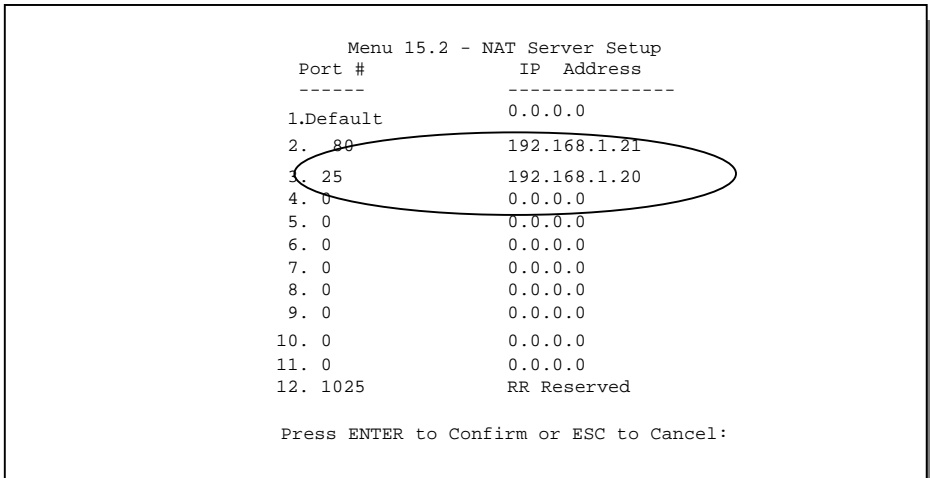


**Figure 6-19 Example 3: Final Menu 15.1.1**

Now configure the IGA3 to map to our web server and mail server on the LAN.

**Step 8.** Enter 15 from the main menu.

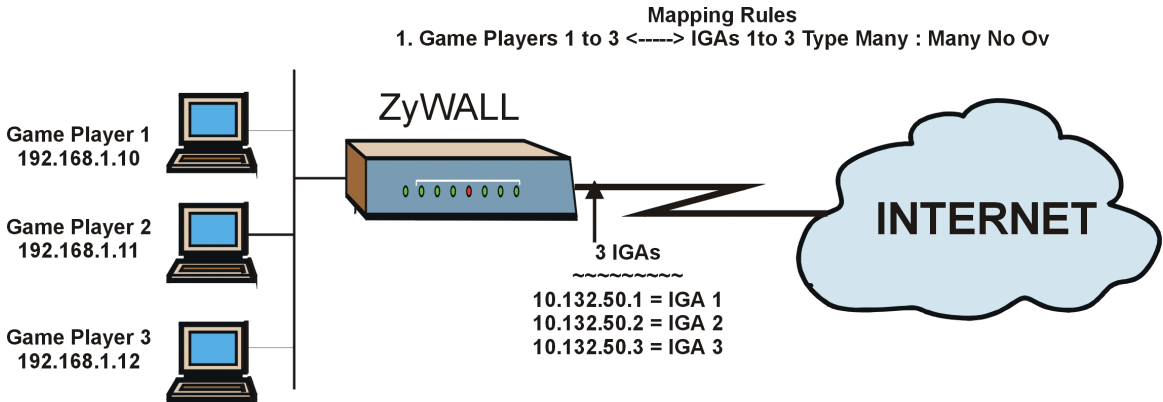
**Step 9.** Now enter 2 from this menu and configure it as shown in *Figure 6-20*.



**Figure 6-20 Example 3: Menu 15.2**

### 6.4.4 Example 4: NAT Unfriendly Application Programs

Some applications do not support NAT Mapping using TCP or UDP port address translation. In this case it is better to use **Many-to-Many No Overload** mapping as port numbers do *not* change for **Many-to-Many No Overload** (and **One-to-One**) NAT mapping types. The following figure illustrates this.



**Figure 6-21 NAT Example 4**

---

Other applications, e.g., gaming programs are NAT unfriendly because they embed addressing information in the data stream. These applications still won't work through NAT even when using One-to-One and Many-to-Many No Overload mapping types.

---

Follow the steps outlined in example 3 above to configure these two menus as follows.



```

Menu 15.1.1.1 Address Mapping Rule

Type= Many-to-Many No Overload

Local IP:
  Start= 192.168.1.10
  End   = 192.168.1.12

Global IP:
  Start= 10.132.50.1
  End   = 10.132.50.3

Press ENTER to Confirm or ESC to Cancel:

```

**Figure 6-22 Example 4: Menu 15.1.1.1 — Address Mapping Rule**

After you've configured your rule, you should be able to check the settings in menu 15.1.1 as shown next.

```

Menu 15.1.1 - Address Mapping Rules

Set Name= Example4

Idx  Local Start IP  Local End IP  Global Start IP  Global End IP  Type
-----
 1.  192.168.1.10    192.168.1.12  10.132.50.1     10.132.50.3   M-M No Ov
 2.
 3.
 4.
 5.
 6.
 7.
 8.
 9.
10.

Action= Edit      Select Rule=

Press ENTER to Confirm or ESC to Cancel:

```

**Figure 6-23 Example 4: Menu 15.1.1 — Address Mapping Rules**

---

---

# Part III:

---

## Advanced Management

---

Chapters 7 — 12 provides information on ZyWALL Filtering, SNMP Configuration, System Information and Diagnosis, Transferring Files, System Maintenance and Telnet.



# Chapter 7

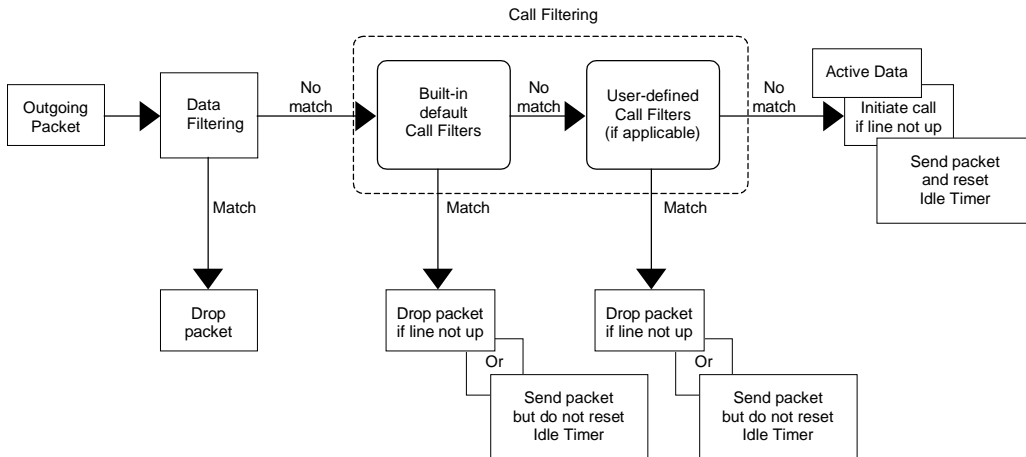
## Filter Configuration

*This chapter shows you how to create and apply filters.*

### 7.1 About Filtering

Your ZyWALL uses filters to decide whether to allow passage of a data packet and/or to make a call. There are two types of filter applications: data filtering and call filtering. Filters are subdivided into device and protocol filters, which are discussed later.

Data filtering screens the data to determine if the packet should be allowed to pass. Data filters are divided into incoming and outgoing filters, depending on the direction of the packet relative to a port. Data filtering can be applied on either the WAN side or the LAN side. Call filtering is used to determine if a packet should be allowed to trigger a call. Remote node call filtering is only applicable when using PPPoE encapsulation. Outgoing packets must undergo data filtering before they encounter call filtering as shown in the following figure.



**Figure 7-1 Outgoing Packet Filtering Process**

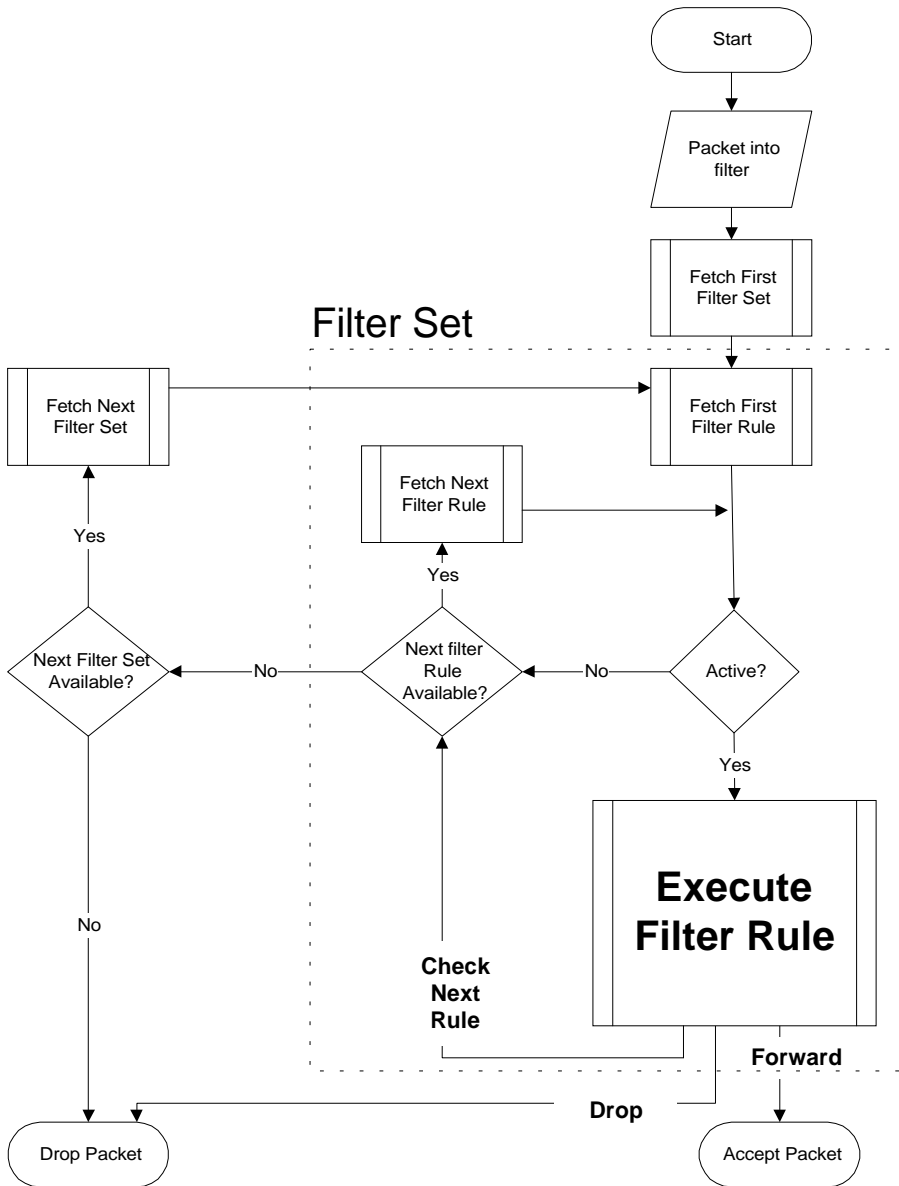
For incoming packets, your ZyWALL applies data filters only. Packets are processed depending upon whether a match is found. The following sections describe how to configure filter sets.

### 7.1.1 The Filter Structure of the ZyWALL

A filter set consists of one or more filter rules. Usually, you would group related rules, e.g., all the rules for NetBIOS, into a single set and give it a descriptive name. The ZyWALL allows you to configure up to twelve filter sets with six rules in each set, for a total of 72 filter rules in the system. You cannot mix device filter rules and protocol filter rules within the same set. You can apply up to four filter sets to a particular port to block multiple types of packets. With each filter set having up to six rules, you can have a maximum of 24 rules active for a single port.

Sets of factory default filter rules have been configured in menu 21 to prevent NetBIOS traffic from triggering calls and to prevent incoming telnetting. A summary of their filter rules is shown in the figures that follow.

The following figure illustrates the logic flow when executing a filter rule. See also *Figure 7-10* for the logic flow when executing an IP filter.



**Figure 7-2 Filter Rule Process**

You can apply up to four filter sets to a particular port to block multiple types of packets. With each filter set having up to six rules, you can have a maximum of 24 rules active for a single port.

## 7.2 Configuring a Filter Set

To configure a filter set, follow the procedure below. For more information on menus 21.2 and 21.3, please see *Part 4*.

**Step 1.** Select option 21. **Filter Set Configuration** from the main menu to open menu 21.

```

Menu 21 - Filter and Firewall Setup

1. Filter Setup
2. Firewall Setup
3. View Firewall Log

Enter Menu Selection Number:

```

**Figure 7-4 Menu 21 — Filter and Firewall Setup**

**Step 2.** Enter 1 to bring up the following menu.

```

Menu 21.1 - Filter Set Configuration

Filter          Filter
Set #          Set #
-----          -----
1      NetBIOS_WAN      7      _____
2      NetBIOS_LAN      8      _____
3      -----          9      _____
4      -----          10     _____
5      _____        11     _____
6      _____        12     _____

Enter Filter Set Number to Configure= 0

Edit Comments= N/A

Press ENTER to Confirm or ESC to Cancel:

```

**Figure 7-5 Menu 21.1 — Filter Set Configuration**

**Step 3.** Select the filter set you wish to configure ( 1-12) and press [ENTER].

**Step 4.** Enter a descriptive name or comment in the **Edit Comments** field and press [ENTER].

**Step 5.** Press [ENTER] at the message [Press ENTER to confirm] to open **Menu 21.1.1 - Filter Rules Summary**.

```

Menu 21.1.1 - Filter Rules Summary

# A Type                               Filter Rules                               M m n
-----
1 Y IP  Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=137      N D N
2 Y IP  Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=138      N D N
3 Y IP  Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=139      N D N
4 Y IP  Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=137     N D N
5 Y IP  Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=138     N D N
6 Y IP  Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=139     N D F

Enter Filter Rule Number (1-6) to Configure:

Press ENTER to Confirm or ESC to Cancel:
    
```

**Figure 7-6 NetBIOS\_WAN Filter Rules Summary**

```

Menu 21.1.2 - Filter Rules Summary

# A Type                               Filter Rules                               M m n
-----
1 Y IP  Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=53      N D F
2 Y
3 Y
4 Y
5 Y
6 Y

Enter Filter Rule Number (1-6) to Configure:
    
```

**Figure 7-7 NetBIOS\_LAN Filter Rules Summary**

```

Menu 21.3 - Filter Rules Summary

# A Type                               Filter Rules                               M m n
-----
1 Y IP  Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=23      N D N
2 Y IP  Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=21      N D N
3 Y IP  Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=80      N D F
4 N
5 N
6 N

Enter Filter Rule Number (1-6) to Configure:
    
```

**Figure 7-8 TEL\_FTP\_WEB\_WAN Filter Rules Summary**



## 7.2.1 Filter Rules Summary Menu

This screen shows the summary of the existing rules in the filter set. The following tables contain a brief description of the abbreviations used in the previous menus.

**Table 7-1 Abbreviations Used in the Filter Rules Summary Menu**

FIELD	DESCRIPTION
#	The filter rule number: 1 to 6.
A	Active: "Y" means the rule is active. "N" means the rule is inactive.
Type	The type of filter rule: "GEN" for Generic, "IP" for TCP/IP.
Filter Rules	These parameters are displayed here.
M	More. "Y" means there are more rules to check which form a rule chain with the present rule. An action cannot be taken until the rule chain is complete.  "N" means there are no more rules to check. You can specify an action to be taken i.e., forward the packet, drop the packet or check the next rule. For the latter, the next rule is independent of the rule just checked.
m	Action Matched. "F" means to forward the packet immediately and skip checking the remaining rules. "D" means to drop the packet. "N" means to check the next rule.
n	Action Not Matched. "F" means to forward the packet immediately and skip checking the remaining rules. "D" means to drop the packet. "N" means to check the next rule.

The protocol dependent filter rules abbreviation are listed as follows:

**Table 7-2 Rule Abbreviations Used**

ABBREVIATION	DESCRIPTION
IP	
Pr	Protocol
SA	Source Address
SP	Source Port number
DA	Destination Address
DP	Destination Port number

ABBREVIATION	DESCRIPTION
GEN	
Off	Offset
Len	Length

Refer to the next section for information on configuring the filter rules.

## 7.2.2 Configuring a Filter Rule

To configure a filter rule, type its number in **Menu 21.1 - Filter Rules Summary** and press [ENTER] to open menu 21.1.1 for the rule.

To speed up filtering, all rules in a filter set must be of the same class, i.e., protocol filters or generic filters. The class of a filter set is determined by the first rule that you create. When applying the filter sets to a port, separate menu fields are provided for protocol and device filter sets. If you include a protocol filter set in a device filter field or vice versa, the ZyWALL will warn you and will not allow you to save.

## 7.2.3 TCP/IP Filter Rule

This section shows you how to configure a TCP/IP filter rule. TCP/IP rules allow you to base the rule on the fields in the IP and the upper layer protocol, e.g., UDP and TCP headers.

To configure TCP/IP rules, select **TCP/IP Filter Rule** from the **Filter Type** field and press [ENTER] to open **Menu 21.1.1 - TCP/IP Filter Rule**, as shown next.

```

Menu 21.1.1.1 - TCP/IP Filter Rule

Filter #: 1,1
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 6      IP Source Route= No
Destination: IP Addr= 0.0.0.0
              IP Mask= 0.0.0.0
              Port #= 137
              Port # Comp= Equal
Source: IP Addr= 0.0.0.0
        IP Mask= 0.0.0.0
        Port #=
        Port # Comp= None

TCP Estab= No
More= No      Log= None
Action Matched= Drop

Action Not Matched= Check Next Rule

Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.

```

**Figure 7-9 Menu 21.1.1.1 — TCP/IP Filter Rule**

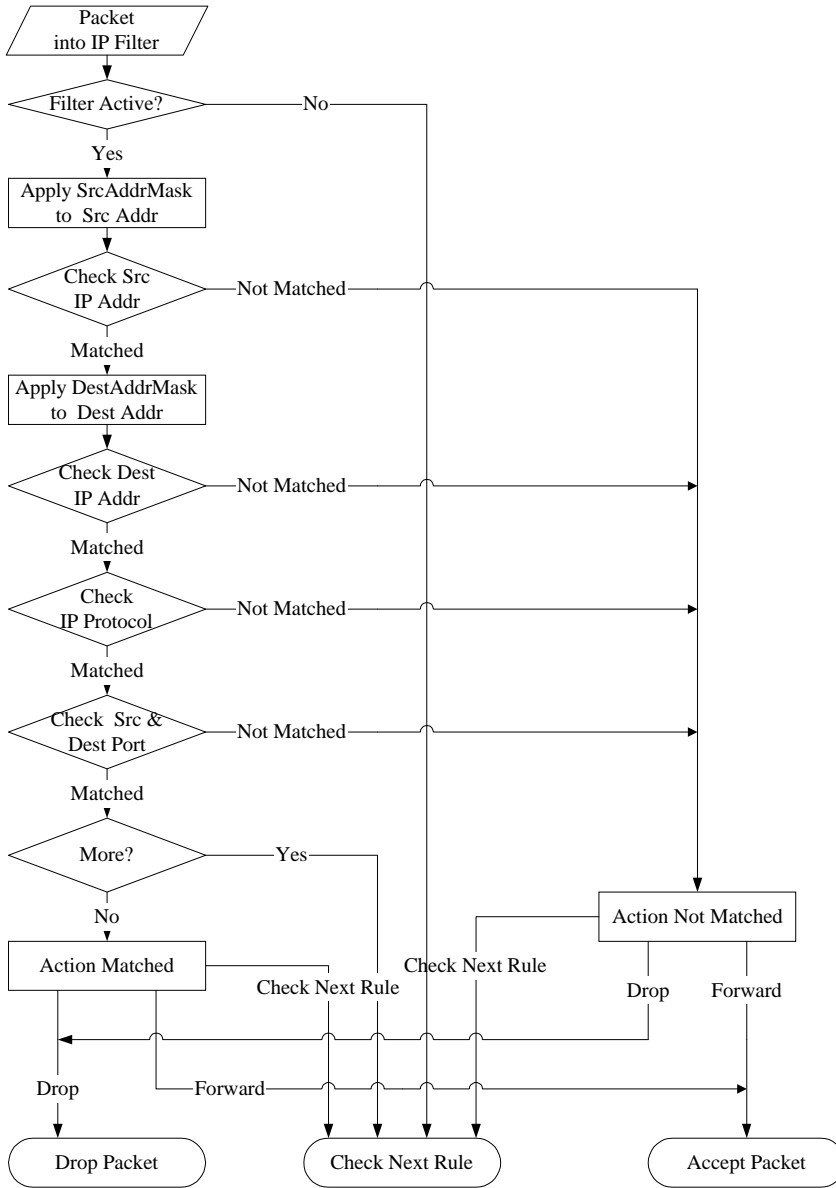
The following table describes how to configure your TCP/IP filter rule.

**Table 7-3 TCP/IP Filter Rule Menu Fields**

FIELD	DESCRIPTION	OPTIONS
Active	<b>Yes</b> activates the filter rule and <b>No</b> deactivates it.	<b>Yes/No</b>
IP Protocol	Protocol refers to the upper layer protocol, e.g., TCP is 6, UDP is 17 and ICMP is 1. This value must be between 0 and 255. A value of 0 matches ANY protocol.	0-255
IP Source Route	If <b>Yes</b> , the rule applies to packet with IP source route option; else the packet must not have source route option. The majority of IP packets do not have source route.	<b>Yes/No</b>
Destination		
IP Address	Enter the destination IP Address of the packet you wish to filter. This field is ignored if it is 0.0.0.0.	0.0.0.0
IP Mask	Enter the IP mask to apply to the <b>Destination: IP Addr.</b>	0.0.0.0
Port #	Enter the destination port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0.	0-65535
Port # Comp	Select the comparison to apply to the destination port in the packet against the value given in <b>Destination: Port #.</b>	<b>None/Less/Greater/Equal/Not Equal]</b>
Source		
IP Address	Enter the source IP Address of the packet you wish to filter. This field is ignored if it is 0.0.0.0.	0.0.0.0
IP Mask	Enter the IP mask to apply to the <b>Source: IP Addr.</b>	0.0.0.0
Port #	Enter the source port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0.	0-65535
Port # Comp	Select the comparison to apply to the source port in the packet against the value given in <b>Source: Port #.</b>	<b>None/Less/Greater/Equal/Not Equal</b>
TCP Estab	This field is applicable only when the IP Protocol field is 6, TCP. If <b>Yes</b> , the rule matches packets that want to establish a TCP connection (SYN=1 and ACK=0); if <b>No</b> , it is ignored.	<b>Yes/No</b>
More	If <b>Yes</b> , a matching packet is passed to the next filter rule before an action is taken; if <b>No</b> , the packet is disposed of	<b>Yes/No</b>

FIELD	DESCRIPTION	OPTIONS
	<p>according to the action fields.</p> <p>If <b>More</b> is <b>Yes</b>, then <b>Action Matched</b> and <b>Action Not Matched</b> will be <b>N/A</b>.</p>	
Log	<p>Select the logging option from the following:</p> <p><b>None</b> – No packets will be logged.</p> <p><b>Action Matched</b> - Only packets that match the rule parameters will be logged.</p> <p><b>Action Not Matched</b> - Only packets that do not match the rule parameters will be logged.</p> <p><b>Both</b> – All packets will be logged.</p>	<p><b>None</b></p> <p><b>Action Matched</b></p> <p><b>Action Not Matched</b></p> <p><b>Both</b></p>
Action Matched	<p>Select the action for a matching packet.</p>	<p><b>Check Next Rule</b></p> <p><b>Forward</b></p> <p><b>Drop</b></p>
Action Not Matched	<p>Select the action for a packet not matching the rule.</p>	<p><b>Check Next Rule</b></p> <p><b>Forward</b></p> <p><b>Drop</b></p>
<p>Press [SPACE BAR] to select properties for fields that do not need to be typed in. When you have <b>Menu 21.1.1.1 - TCP/IP Filter Rule</b> configured, press [ENTER] at the message "Press ENTER to Confirm" to save your configuration, or press [ESC] to cancel. This data will now be displayed on <b>Menu 21.1.1 - Filter Rules Summary</b>.</p>		

The following figure illustrates the logic flow of an IP filter.



**Figure 7-10 Executing an IP Filter**

## 7.2.4 Generic Filter Rule

This section shows you how to configure a generic filter rule. The purpose of generic rules is to allow you to filter non-IP packets. For IP, it is generally easier to use the IP rules directly.

For generic rules, the ZyWALL treats a packet as a byte stream as opposed to an IP or IPX packet. You specify the portion of the packet to check with the **Offset** (from 0) and the **Length** fields, both in bytes. The ZyWALL applies the Mask (bit-wise ANDing) to the data portion before comparing the result against the Value to determine a match. The **Mask** and **Value** are specified in hexadecimal numbers. Note that it takes two hexadecimal digits to represent a byte, so if the length is 4, the value in either field will take 8 digits, e.g., FFFFFFFF.

To configure a generic rule, select Generic Filter Rule in the Filter Type field in menu 21.4.1.1 and press [ENTER] to open Generic Filter Rule, as shown below.

```
Menu 21.4.1.1 - Generic Filter Rule

Filter #: 4,1
Filter Type= Generic Filter Rule
Active= No
Offset= 0
Length= 0
Mask= N/A
Value= N/A
More= No           Log= None
Action Matched= Check Next Rule
Action Not Matched= Check Next Rule

Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.
```

**Figure 7-11 Menu 21.4.1.1 — Generic Filter Rule**

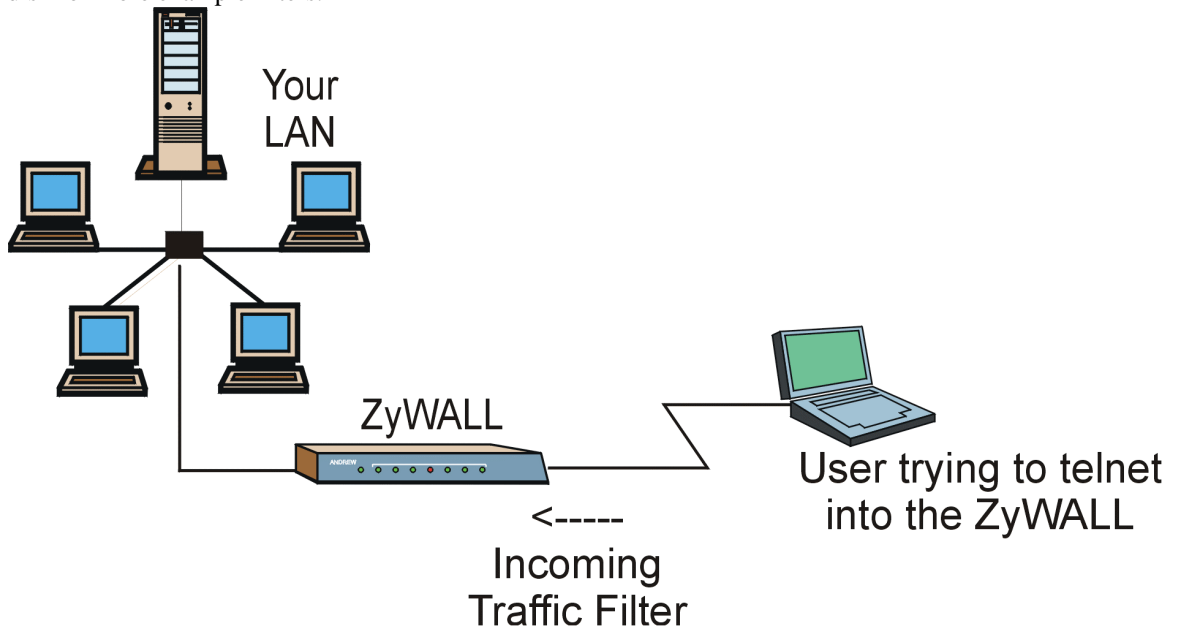
The following table describes the fields in the Generic Filter Rule Menu.

Table 7-4 Generic Filter Rule Menu Fields

FIELD	DESCRIPTION	OPTIONS
Filter #	This is the filter set, filter rule co-ordinates, i.e., 2,3 refers to the second filter set and the third rule of that set.	
Filter Type	Use the [SPACE BAR] to select a rule type. Parameters displayed below each type will be different. TCP/IP filter rules are used to filter IP packets while generic filter rules allow filtering of non-IP packets.	<b>Generic Filter Rule/ TCP/IP Filter Rule</b>
Active	Select <b>Yes</b> to turn on the filter rule or <b>No</b> to turn it off.	<b>Yes</b>
Offset	Enter the starting byte of the data portion in the packet that you wish to compare. The range for this field is from 0 to 255.	0 (Default)
Length	Enter the byte count of the data portion in the packet that you wish to compare. The range for this field is 0 to 8.	0 (Default)
Mask	Enter the mask (in Hexadecimal notation) to apply to the data portion before comparison.	
Value	Enter the value (in Hexadecimal notation) to compare with the data portion.	
More	If <b>Yes</b> , a matching packet is passed to the next filter rule before an action is taken; else the packet is disposed of according to the action fields.  If <b>More</b> is <b>Yes</b> , then Action Matched and Action Not Matched will be <b>No</b> .	<b>Yes/No</b>
Log	Select the logging option from the following:  <b>None</b> - No packets will be logged.  <b>Action Matched</b> - Only packets that match the rule parameters will be logged.  <b>Action Not Matched</b> - Only packets that do not match the rule parameters will be logged.  <b>Both</b> – All packets will be logged.	<b>None</b>  <b>Action Matched</b>  <b>Action Not Matched</b>  <b>Both</b>
Action Matched	Select the action for a packet matching the rule.	<b>Check Next Rule, Forward, Drop</b>
Action Not Matched	Select the action for a packet not matching the rule.	<b>Check Next Rule, Forward, Drop</b>
Once you have completed filling in <b>Menu 21.4.1.1 - Generic Filter Rule</b> , press [ENTER] at the message "Press ENTER to Confirm" to save your configuration, or press [ESC] to cancel. This data will now be displayed on <b>Menu 21.1.1 - Filter Rules Summary</b> .		

## 7.3 Example Filter

Let's look at an example to block outside users from telnetting into the ZyWALL. Please see our included disk for more example filters.



**Figure 7-12 Telnet Filter Example**

- Step 1.** Enter 21 from the main menu to open **Menu 21.1 - Filter Set Configuration**.
- Step 2.** Enter the index of the filter set you wish to configure (say 3) and press [ENTER].
- Step 3.** Enter a descriptive name or comment in the **Edit Comments** field and press [ENTER].
- Step 4.** Press [ENTER] at the message [Press ENTER to confirm] to open **Menu 21.1.1 - Filter Rules Summary**.
- Step 5.** Enter 1 to configure the first filter rule (the only filter rule of this set). Make the entries in this menu as shown in the following figure.



```
Menu 21.1.1 - TCP/IP Filter Rule
Filter #: 3,1
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 6      IP Source Route= No
Destination: IP Addr= 0.0.0.0
               IP Mask= 0.0.0.0
               Port # = 23
               Port # Comp= Equal
Source: IP Addr= 0.0.0.0
          IP Mask= 0.0.0.0
          Port # = 0
          Port # Comp= None
TCP Estab= No
More= No          Log= None
Action Matched= Drop
Action Not Matched= Forward
Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.
```

Press the [SPACE BAR] to choose this filter rule type. The first filter rule type determines all subsequent filter types within a set.

Select **Yes** to make the rule active.

**6** is the TCP protocol.

The port number for the telnet service (TCP protocol) is **23**. See *RFC 1060* for port numbers of well-known services.

There are no more rules to check.

Select **Equal** here as you are looking for packets going to port 23 only.

Select **Drop** here so that the packet will be dropped if its destination is the telnet port.

Select **Forward** here so that the packet will be forwarded if its destination is not the telnet port.

**Figure 7-13 Example Filter — Menu 21.1.1.1**

When you press [ENTER] to confirm, you will see the following screen. Note that there is only one filter rule in this set.

Menu 21.1.3 - Filter Rules Summary

#	A	Type	Filter Rules	M	m	n
1	Y	IP	Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=23			
2	N					
3	N					
4	N					
5	N					
6	N					

Enter Filter Rule Number (1-6) to Configure: 1

**M = N** means an action can be taken immediately. The action is to drop the packet (**m = D**) if the action is matched and to forward the packet immediately (**n = F**) if the action is not matched no matter whether there are more rules to be checked (there aren't in this example).

**Figure 7-14 Example Filter Rules Summary — Menu 21.1.3**

After you've created the filter set, you must apply it.

- Step 1.** Enter 11 from the main menu to go to menu 11.
- Step 2.** Go to the **Edit Filter Sets** field, press the [SPACE BAR] to select **Yes** and press [ENTER].
- Step 3.** This brings you to menu 11.5. Apply a filter set (our example filter set 3) as shown in *Figure 7-17*.
- Step 4.** Press [ENTER] to confirm after you enter the set numbers and to leave menu 11.5.

## 7.4 Filter Types and NAT

There are two classes of filter rules, **Generic Filter** (Device) rules and Protocol Filter (**TCP/IP**) rules. Generic Filter rules act on the raw data from/to LAN and WAN. Protocol Filter rules act on the IP packets. Generic and TCP/IP filter rules are discussed in more detail in the next section. When NAT (Network Address Translation) is enabled, the inside IP address and port number are replaced on a connection-by-connection basis, which makes it impossible to know the exact address and port on the wire. Therefore, the ZyWALL applies the protocol filters to the "native" IP address and port number before NAT for outgoing packets and after NAT for incoming packets. On the other hand, the generic, or device filters are applied to

the raw packets that appear on the wire. They are applied at the point when the ZyWALL is receiving and sending the packets; i.e. the interface. The interface can be an Ethernet port or any other hardware port. The following diagram illustrates this.

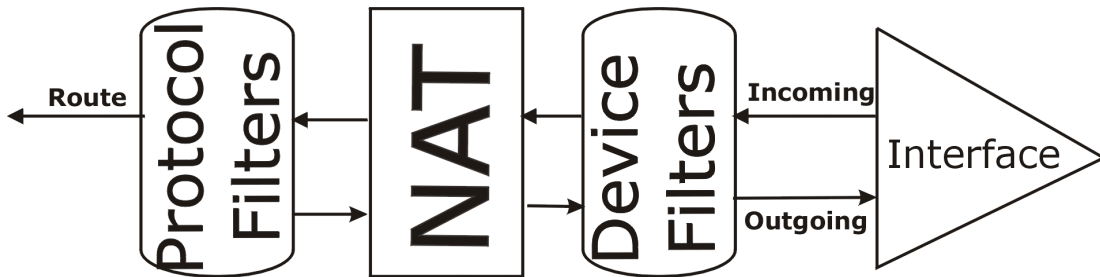


Figure 7-15 Protocol and Device Filter Sets

## 7.5 Firewall

Firewall configuration is discussed in *Part 4* of this manual. Further comparisons are also made there between filtering, NAT and the firewall.

## 7.6 Applying a Filter and Factory Defaults

This section shows you where to apply the filter(s) after you design it (them). Sets of factory default filter rules have been configured in menu 21 to prevent NetBIOS traffic from triggering calls, and block incoming telnet, FTP and HTTP connections.

---

If you do not activate the firewall, it is advisable to apply these default filters as shown next.

---

### 7.6.1 LAN traffic

LAN traffic filter sets may be useful to block certain packets, reduce traffic and prevent security breaches. Go to menu 3.1 (shown next) and enter the number(s) of the filter set(s) that you want to apply as appropriate. You can choose up to four filter sets (from twelve) by entering their numbers separated by commas, e.g., 3, 4, 6, 11. Input filter sets filter incoming traffic to the ZyWALL and output filter sets filter outgoing traffic from the ZyWALL. The factory default set, NetBIOS\_LAN, can be inserted in the **protocol filters** field under **Input Filter Sets** in menu 3.1 to block NetBIOS traffic to the ZyWALL from the LAN.

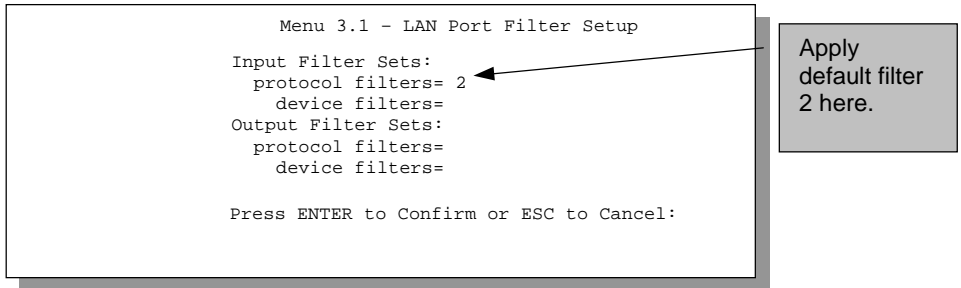


Figure 7-16 Filtering LAN Traffic

## 7.6.2 Remote Node Filters

Go to menu 11.5 (shown below – note that call filter sets are only present for PPPoE encapsulation) and enter the number(s) of the filter set(s) as appropriate. You can cascade up to four filter sets by entering their numbers separated by commas. The factory default filter set, NetBIOS\_WAN, can be applied in menu 11.5 to block local NetBIOS traffic from triggering calls to the ISP (when you are using PPPoE or PPTP encapsulation only). Enter 1 in **protocol filters** under **Output Filter Sets** when using Ethernet encapsulation, and in the **protocol filters** field under **Call Filter Sets** when using PPPoE or PPTP encapsulation. Apply them as shown in the following figure.

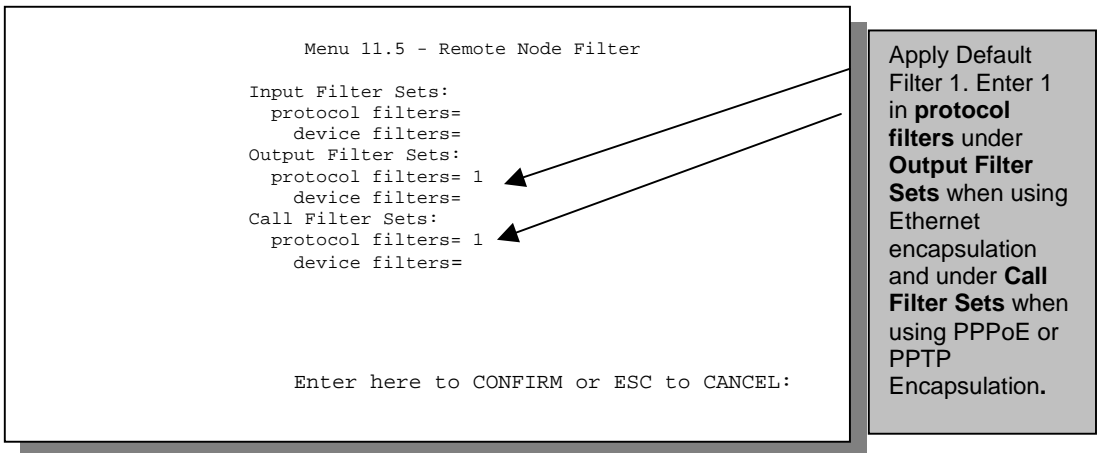


Figure 7-17 Filtering Remote Node Traffic



# Chapter 8

## SNMP Configuration

*This chapter discusses SNMP (Simple Network Management Protocol) for network management and monitoring.*

### 8.1 About SNMP

Your ZyWALL supports SNMP agent functionality, which allows a manager station to manage and monitor the ZyWALL through the network. Keep in mind that SNMP is only available if TCP/IP is configured on your ZyWALL.

### 8.2 Configuring SNMP

To configure SNMP, enter 22 from the main menu to open **Menu 22 - SNMP Configuration**, as shown in the figure below. The “community” for Get, Set and Trap fields is simply SNMP’s terminology for password.

```
Menu 22 - SNMP Configuration

SNMP:
  Get Community= public
  Set Community= public
  Trusted Host= 0.0.0.0
  Trap:
    Community= public
    Destination= 0.0.0.0

Press ENTER to Confirm or ESC to Cancel:
```

**Figure 8-1 Menu 22 — SNMP Configuration**

The following table describes the SNMP configuration parameters.

**Table 8-1 SNMP Configuration Menu Fields**

FIELD	DESCRIPTION	DEFAULT
Get Community	Enter the get community, which is the password for the incoming Get- and GetNext- requests from the management station.	public
Set Community	Enter the set community, which is the password for incoming Set- requests from the management station.	public
Trusted Host	If you enter a trusted host, your ZyWALL will only respond to SNMP messages from this address. If you leave the field blank (default), your ZyWALL will respond to all SNMP messages it receives, regardless of source.	blank
Trap Community	Enter the trap community, which is the password sent with each trap to the SNMP manager.	public
Trap Destination	Enter the IP address of the station to send your SNMP traps to.	0.0.0.0
Once you have completed filling in <b>Menu 22 - SNMP Configuration</b> , press [ENTER] at the message "Press ENTER to Confirm" to save your configuration, or press [ESC] to cancel.		

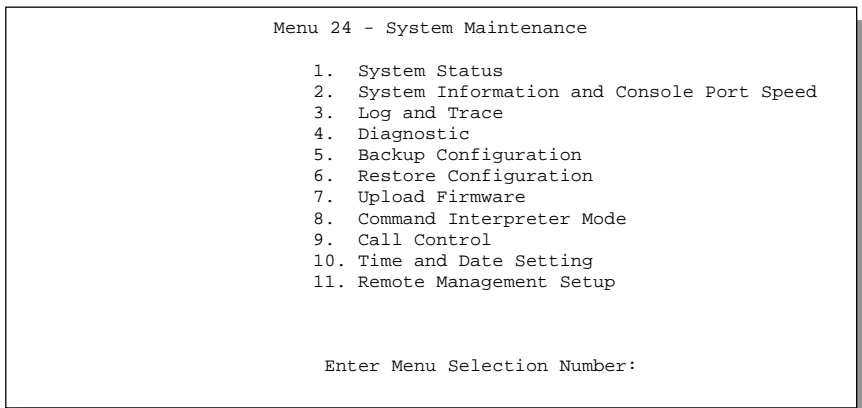
# Chapter 9

## System Information & Diagnosis

*This chapter covers SMT menus 24.1 to 24.4.*

This chapter covers the diagnostic tools that help you to maintain your ZyWALL. These tools include updates on system status, port status, log and trace capabilities and upgrades for the system software.

Select menu 24 in the main menu to open **Menu 24 - System Maintenance**, as shown below.



**Figure 9-1 Menu 24 — System Maintenance**

### 9.1 System Status

The first selection, System Status, gives you information on the version of your system firmware and the status and statistics of the ports, as shown in the next figure. System Status is a tool that can be used to monitor your ZyWALL. Specifically, it gives you information on your system firmware version, number of packets sent and number of packets received.

To get to the System Status:

- Step 1.** Enter number 24 to go to **Menu 24 - System Maintenance**.
- Step 2.** In this menu, enter 1 to open **System Maintenance - Status**.
- Step 3.** There are three commands in **Menu 24.1 - System Maintenance - Status**. Entering 1 drops the WAN connection, 9 resets the counters and [ESC] takes you back to the previous screen.



```

Menu 24.1 - System Maintenance - Status                               23:10:28
                                                                    Sat. Jan. 01, 2000
Port  Status      TxPkts    RxPkts    Cols    Tx B/s    Rx B/s    Up Time
WAN   10M/Half      67        289       0        74        64        2:20:56
LAN   10M/Half     299        220       0        74        64        2:20:54

Port:      Ethernet Address    IP Address          IP Mask            DHCP
WAN        00:a0:c5:21:8c:a3   x.y.155.97         255.255.255.0     Client
LAN        00:a0:c5:21:8c:a2   192.168.1.1       255.255.255.0     Server

System up Time: 22:11:43

Name: xxx.baboo.mickey.com
Routing: IP
ZyNOS F/W Version: V324WA0b06 | 3/14/2001

Press Command:

COMMANDS: 1-Drop WAN 9-Reset Counters  ESC-Exit
    
```

**Figure 9-2 Menu 24.1 — System Maintenance — Status**

The following table describes the fields present in **Menu 24.1 - System Maintenance - Status**. These fields are READ-ONLY and are meant to be used for diagnostic purposes. The upper right corner of the screen shows the time and date according to the format you set in menu 24.10.

**Table 9-1 System Maintenance — Status Menu Fields**

FIELD	DESCRIPTION
Port	The WAN or LAN port.
Status	Shows the port speed and duplex setting if you're using <b>Ethernet Encapsulation</b> and <b>Down</b> (line is down), <b>idle</b> (line (ppp) idle), <b>dial</b> (starting to trigger a call) and <b>drop</b> (dropping a call) if you're using <b>PPPoE Encapsulation</b> .
TxPkts	The number of transmitted packets on this port.
RxPkts	The number of received packets on this port.
Cols	The number of collisions on this port.
Tx B/s	Shows the transmission speed in Bytes per second on this port.
Rx B/s	Shows the reception speed in Bytes per second on this port.
Up Time	Total amount of time the line has been up.
LAN	
Ethernet Address	The LAN port Ethernet address.

FIELD	DESCRIPTION
IP Address	The LAN port IP address.
IP Mask	The LAN port IP mask.
DHCP	The LAN port DHCP role.
WAN	
Ethernet Address	The WAN port Ethernet address.
IP Address	The WAN port IP address.
IP Mask	The WAN port IP mask.
DHCP	The WAN port DHCP role.
System up Time	The total time the ZyWALL has been on.
Name	This is the ZyWALL's system name + domain name assigned in menu 1. e.g., System Name= xxx; Domain Name= baboo.mickey.com. Name= xxx.baboo.mickey.com
ZyNOS F/W Version	The ZyNOS Firmware version and the date created.
You may enter 1 to drop the WAN connection, 9 to reset the counters or [ESC] to return to menu 24.	

## 9.2 System Information and Console Port Speed

This section describes your system and allows you to choose different console port speeds. To get to the System Information and Console Port Speed:

**Step 1.** Enter 24 to go to **Menu 24 – System Maintenance**.

**Step 2.** Enter 2 to open **Menu 24.2 - System Information and Console Port Speed**.

**Step 3.** From this menu you have two choices as shown in the next figure:

```

Menu 24.2 - System Information and Console Port Speed
    1. System Information
    2. Console Port Speed

Please enter selection:

```

**Figure 9-3 Menu 24.2 — System Information and Console Port Speed**

## 9.2.1 System Information

System Information gives you information about your system as shown below. More specifically, it gives you information on your routing protocol, Ethernet address, IP address, etc.

```

Menu 24.2.1 - System Maintenance - Information
Name: xxx.baboo.mickey.com
Routing: IP
ZyNOS F/W Version: V324WA0b05 | 3/5/2001

LAN
Ethernet Address: 00:a0:c5:21:8c:a2
IP Address: 192.168.1.1
IP Mask: 255.255.255.0
DHCP: Server

Press ESC or RETURN to Exit

```

**Figure 9-4 Menu 24.2.1 — System Maintenance — Information**

**Table 9-2 Fields in System Maintenance — Information**

FIELD	DESCRIPTION
Name	This is the ZyWALL's system name + domain name assigned in Menu 1. E.G., System Name= xxx; Domain Name= baboo.mickey.com Name= xxx.baboo.mickey.com
Routing	Refers to the routing protocol used.
ZyNOS F/W Version	Refers to the version of ZyXEL's Network Operating System software.
Ethernet Address	Refers to the Ethernet MAC (Media Access Control) address of your ZyWALL.
IP Address	This is the IP address of the ZyWALL in dotted decimal notation.
IP Mask	This shows the IP mask of the ZyWALL.
DHCP	This field shows the DHCP setting of the ZyWALL.
When finished viewing, press [ESC] or [ENTER] to exit.	

## 9.2.2 Console Port Speed

You can change the speed of the console port through **Menu 24.2.2 – Console Port Speed**. Your ZyWALL supports 9600 (default), 19200, 38400, 57600, and 115200 bps for the console port. Use the [SPACE BAR] to select the desired speed in menu 24.2.2, as shown below.

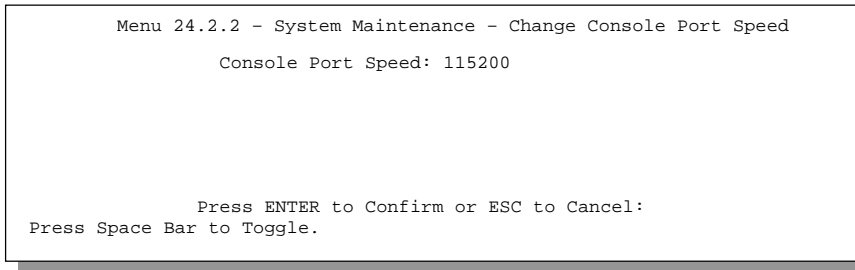


Figure 9-5 Menu 24.2.2 — System Maintenance — Change Console Port Speed

## 9.3 Log and Trace

There are two logging facilities in the ZyWALL. The first is the error logs and trace records that are stored locally. The second is the UNIX syslog facility for message logging.

### 9.3.1 Viewing Error Log

The first place you should look for clues when something goes wrong is the error/trace log. Follow the procedure below to view the local error/trace log:

- Step 1.** Select option 24 from the main menu to open **Menu 24 - System Maintenance**.
- Step 2.** From menu 24, select option 3 to open **Menu 24.3 - System Maintenance - Log and Trace**.
- Step 3.** Select the first option from **Menu 24.3 - System Maintenance - Log and Trace** to display the error log in the system.

After the ZyWALL finishes displaying, you will have the option to clear the error log.

```

Menu 24.3 - System Maintenance - Log and Trace

1. View Error Log
2. UNIX Syslog

4. Call-Triggering Packet

Please enter selection
    
```

**Figure 9-6 Menu 24.3 — System Maintenance — Log and Trace**

Examples of typical error and information messages are presented in the figure below.

```

59 Thu Jan 1 00:00:03 2000 PINI INFO SMT Session Begin
60 Thu Jan 1 00:05:11 2000 PINI INFO SMT Session End
61 Thu Jan 1 00:17:59 2000 PINI INFO SMT Session Begin
62 Thu Jan 1 00:24:40 2000 PINI INFO SMT Session End
63 Thu Jan 1 00:35:32 2000 PINI INFO SMT Session Begin
Clear Error Log (y/n):
    
```

**Figure 9-7 Examples of Error and Information Messages**

### 9.3.2 UNIX Syslog

The ZyWALL uses the UNIX syslog facility to log the CDR (Call Detail Record) and system messages to a syslog server. Syslog and accounting can be configured in **Menu 24.3.2 - System Maintenance - Syslog and Accounting**, as shown next.

```

Menu 24.3.2 - System Maintenance - UNIX Syslog and Accounting

UNIX Syslog:
Active= No
Syslog IP Address= ?
Log Facility= Local 1

Types:
CDR= No
Packet Triggered= No
Filter log= No
PPP log= No

Firewall log= No

Press ENTER to Confirm or ESC to Cancel
    
```

**Figure 9-8 Menu 24.3.2 — System Maintenance — UNIX Syslog**

You need to configure the UNIX syslog parameters described in the following table to activate syslog then choose what you want to log.

**Table 9-3 System Maintenance Menu Syslog Parameters**

PARAMETER	DESCRIPTION
UNIX Syslog:	
Active	Press [SPACE BAR] to turn syslog on or off.
Syslog IP Address	Enter the IP Address of the server that will log the CDR (Call Detail Record) and system messages i.e., the syslog server.
Log Facility	Press [SPACE BAR] to select a Local option. The log facility allows you to log the message to different files in the server. Please refer to your UNIX manual for more details.
Types:	
CDR	Call Detail Record (CDR) logs all data phone line activity if set to <b>Yes</b> .
Packet triggered	The first 48 bytes or octets and protocol type of the triggering packet is sent to the UNIX syslog server when this field is set to <b>Yes</b> .
Filter log	No filters are logged when this field is set to <b>No</b> . Filters with the individual filter Log Filter field set to <b>Yes</b> (Menu 21.x.x.) are logged when this field is set to <b>Yes</b> .
PPP log	PPP events are logged when this field is set to <b>Yes</b> .
Firewall log	When set to <b>Yes</b> , the ZyWALL sends the firewall log to a syslog server.
When finished configuring this screen, press [ENTER] to confirm or [ESC] to cancel.	

Your ZyWALL sends five types of syslog messages. Some examples (not all ZyWALL specific) of these syslog messages with their message formats are shown next:

## 1. CDR

### CDR Message Format

```
SdcmSyslogSend( SYSLOG_CDR, SYSLOG_INFO, String );  
String = board xx line xx channel xx, call xx, str  
board = the hardware board ID  
line = the WAN ID in a board  
Channel = channel ID within the WAN  
call = the call reference number which starts from 1 and increments by 1 for each new call  
str = C01 Outgoing Call dev xx ch xx (dev:device No. ch:channel No.)  
      L02 Tunnel Connected(L2TP)  
      C02 OutCall Connected xxxx (means connected speed) xxxxx (means Remote Call Number)  
      L02 Call Terminated  
      C02 Call Terminated
```

```
Jul 19 11:19:27 192.168.102.2 ZyXEL: board 0 line 0 channel 0, call 1, C01 Outgoing Call  
dev=2 ch=0 40002  
Jul 19 11:19:32 192.168.102.2 ZyXEL: board 0 line 0 channel 0, call 1, C02 OutCall  
Connected 64000 40002  
Jul 19 11:20:06 192.168.102.2 ZyXEL: board 0 line 0 channel 0, call 1, C02 Call Terminated
```

## 2. Packet triggered

### Packet triggered Message Format

```
sdcmdSyslogSend( SYSLOG_PKTTRI, SYSLOG_NOTICE, String );  
String = Packet trigger: Protocol=xx Data=xxxxxxxxx.....x  
Protocol: (1:IP 2:IPX 3:IPXHC 4:BPDU 5:ATALK 6:IPNG)  
Data: We will send forty-eight Hex characters to the server
```

```
Jul 19 11:28:39 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1,  
Data=4500003c100100001f010004c0a86614ca849a7b08004a5c020001006162636465666768696a6b6c6d6e6  
f7071727374  
Jul 19 11:28:56 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1,  
Data=4500002c1b0140001f06b50ec0a86614ca849a7b0427001700195b3e0000000600220008cd4000002040  
5b4  
Jul 19 11:29:06 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1,  
Data=45000028240140001f06ac12c0a86614ca849a7b0427001700195b451d1430135004000077600000
```

## 3. Filter log

### Filter log Message Format

```
SdcmSyslogSend(SYSLOG_FILLOG, SYSLOG_NOTICE, String );  
String = IP[Src=xx.xx.xx.xx Dst=xx.xx.xx.xx prot spo=xxxx dpo=xxxx] S04>R01mD  
  
IP[...] is the packet header and S04>R01mD means filter set 4 (S) and rule 1 (R), match (m) drop (D).  
Src: Source Address  
Dst: Destination Address  
prot: Protocol ("TCP", "UDP", "ICMP")  
spo: Source port  
dpo: Destination port
```

```

Mar 03 10:39:43 202.132.155.97 ZyXEL:
GEN[fffffffffnordff0080] }S05>R01mF
Mar 03 10:41:29 202.132.155.97 ZyXEL:
GEN[00a0c5f502fnord010080] }S05>R01mF
Mar 03 10:41:34 202.132.155.97 ZyXEL:
IP[Src=192.168.2.33 Dst=202.132.155.93 ICMP]}S04>R01mF
Mar 03 11:59:20 202.132.155.97 ZyXEL:
GEN[00a0c5f502fnord010080] }S05>R01mF
Mar 03 12:00:31 202.132.155.97 ZyXEL:
GEN[fffffffffnordff0080] }S05>R01mF
Mar 03 12:00:52 202.132.155.97 ZyXEL:
GEN[fffffffffff0080] }S05>R01mF
Mar 03 12:00:57 202.132.155.97 ZyXEL:
GEN[00a0c5f502010080] }S05>R01mF
Mar 03 12:01:01 202.132.155.97 ZyXEL:
IP[Src=192.168.2.33 Dst=202.132.155.93 TCP spo=01170 dpo=00021]}S04>R01mF
Mar 03 12:01:06 202.132.155.97 ZyXEL:
IP[Src=192.168.2.33 Dst=202.132.155.93 TCP spo=01170 dpo=00021]}S04>R01mF

```

#### 4. PPP log

**PPP Log Message Format**  
 sdcmdSyslogSend( SYSLOG\_PPLOG, SYSLOG\_NOTICE, String );  
 String = ppp:Proto Starting / ppp:Proto Opening / ppp:Proto Closing / ppp:Proto Shutdown  
 Proto = LCP / ATCP / BACP / BCP / CBCP / CCP / CHAP/ PAP / IPCP /  
 IPXCP

```

Jul 19 11:42:44 192.168.102.2 ZyXEL: ppp:LCP Closing
Jul 19 11:42:49 192.168.102.2 ZyXEL: ppp:IPCP Closing
Jul 19 11:42:54 192.168.102.2 ZyXEL: ppp:CCP Closing

```

#### 5. Firewall log

**Firewall Log Message Format**  
 sdcmdSyslogSend(SYSLOG\_FIREWALL, SYSLOG\_NOTICE, buf);  
 buf = IP[Src=xx.xx.xx.xx : spo=xxxx Dst=xx.xx.xx.xx : dpo=xxxx | prot | rule | action]  
 Src: Source Address  
 spo: Source port (empty means no source port information)  
 Dst: Destination Address  
 dpo: Destination port (empty means no destination port information)  
 prot: Protocol ("TCP", "UDP", "ICMP", "IGMP", "GRE", "ESP")  
 rule: <a,b> where a means "set" number; b means "rule" number.  
 action: nothing(N) block (B) forward (F)

```

08-01-2000      11:48:41      Local1.Notice  192.168.10.10  RAS: FW 172.21.1.80      :137
->172.21.1.80   :137 |UDP|default permit:<2,0>|B
08-01-2000      11:48:41      Local1.Notice  192.168.10.10  RAS: FW 192.168.77.88    :520
->192.168.77.88 :520 |UDP|default permit:<2,0>|B
08-01-2000      11:48:39      Local1.Notice  192.168.10.10  RAS: FW 172.21.1.50      -
>172.21.1.50   |IGMP<2>|default permit:<2,0>|B
08-01-2000      11:48:39      Local1.Notice  192.168.10.10  RAS: FW 172.21.1.25      -
>172.21.1.25   |IGMP<2>|default permit:<2,0>|B

```



### 9.3.3 Call-Triggering Packet

Call-Triggering Packet displays information about the packet that triggered a dial-out call in an easy readable format. Equivalent information is available in menu 24.1 in hex format. An example is shown next.

```
IP Frame: ENET0-RCV Size: 44/ 44   Time: 17:02:44.262
Frame Type:

IP Header:
  IP Version           = 4
  Header Length       = 20
  Type of Service     = 0x00 (0)
  Total Length        = 0x002C (44)
  Identification      = 0x0002 (2)
  Flags               = 0x00
  Fragment Offset     = 0x00
  Time to Live        = 0xFE (254)
  Protocol            = 0x06 (TCP)
  Header Checksum     = 0xFB20 (64288)
  Source IP           = 0xC0A80101 (192.168.1.1)
  Destination IP     = 0x00000000 (0.0.0.0)

TCP Header:
  Source Port         = 0x0401 (1025)
  Destination Port    = 0x000D (13)
  Sequence Number     = 0x05B8D000 (95997952)
  Ack Number          = 0x00000000 (0)
  Header Length       = 24
  Flags               = 0x02 (...S.)
  Window Size         = 0x2000 (8192)
  Checksum            = 0xE06A (57450)
  Urgent Ptr          = 0x0000 (0)
  Options             =
    0000: 02 04 02 00

RAW DATA:
  0000: 45 00 00 2C 00 02 00 00-FE 06 FB 20 C0 A8 01 01  E.....
  0010: 00 00 00 00 04 01 00 0D-05 B8 D0 00 00 00 00  .....
  0020: 60 02 20 00 E0 6A 00 00-02 04 02 00

Press any key to continue...
```

**Figure 9-9 Call-Triggering Packet Example**

## 9.4 Diagnostic

The diagnostic facility allows you to test the different aspects of your ZyWALL to determine if it is working properly. Menu 24.4 allows you to choose among various types of diagnostic tests to evaluate your system, as shown next.

```
Menu 24.4 - System Maintenance - Diagnostic

TCP/IP
1. Ping Host
2. WAN DHCP Release
3. WAN DHCP Renewal
4. Internet Setup Test

System
11. Reboot System

Enter Menu Selection Number:

Host IP Address= N/A
```

**Figure 9-10 Menu 24.4 — System Maintenance — Diagnostic**

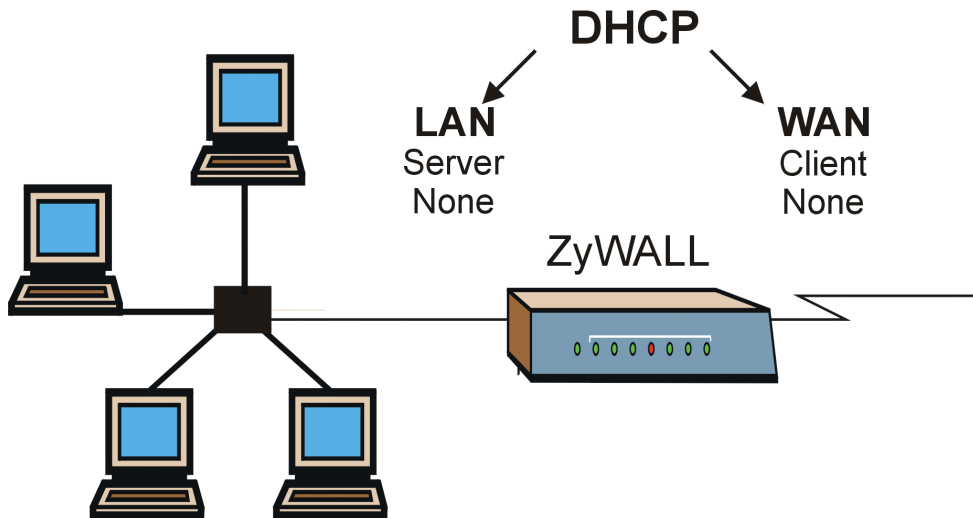
Follow the procedure below to get to **Menu 24.4 - System Maintenance – Diagnostic**.

**Step 1.** From the main menu, select option 24 to open **Menu 24 - System Maintenance**.

**Step 2.** From this menu, select option 4. Diagnostic. This will open **Menu 24.4 - System Maintenance - Diagnostic**.

### 9.4.1 WAN DHCP

DHCP functionality can be enabled on the LAN or WAN as shown in *Figure 9-11*. LAN DHCP has already been discussed. The ZyWALL can act either as a WAN DHCP client (**IP Address Assignment** field in menu 4 or menu 11.3 is **Dynamic** and the **Encapsulation** field in menu 4 or menu 11 is **Ethernet**) or **None**, i.e., you have a static IP. The **WAN Release** and **Renewal** fields in menu 24.4 conveniently allow you to release and/or renew the assigned WAN IP address, subnet mask and default gateway in a fashion similar to winipcfg.



**Figure 9-11 WAN & LAN DHCP**

The following table describes the diagnostic tests available in menu 24.4 for your ZyWALL and associated connections.

**Table 9-4 System Maintenance Menu Diagnostic**

FIELD	DESCRIPTION
Ping Host	Enter 1 to ping any machine (with an IP address) on your LAN or WAN. Enter its IP address in the Host IP Address= field below.
WAN DHCP Release	Enter 2 to release your WAN DHCP settings.
WAN DHCP Renewal	Enter 3 to renew your WAN DHCP settings.
Internet Setup Test	Enter 4 to test the Internet Setup. You can also test the Internet Setup in <b>Menu 4 - Internet Access</b> . Please refer to the <i>Internet Access</i> chapter for more details. This feature is only available for dial-up connections using PPPoE or PPTP encapsulation.
Reboot System	Enter 11 to reboot the ZyWALL.
Host IP Address=	If you entered 1 above, then enter the IP address of the machine you want to ping in this field.
Enter the number of the selection you would like to perform or press [ESC] to cancel.	

# Chapter 10

## 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.*

### 10.1 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 name of `zywall.rom` or similar. Once you have customized the ZyWALL's setting, they can be saved back to your computer under a filename of your choosing. Choose something meaningful, e.g., "`zywall.cfg`".

The ZyNOS firmware file (sometimes referred to as the ras file) is the file that contains the ZyXEL Network Operating System firmware and usually is the router model name with a `*.bin` extension, e.g., `zywall.bin`.

With serial (XMODEM) transfer, the filenames on the computer are your choice. With many ftp and tftp clients, they are similar to those seen next.

```
ftp>put zywall.bin ras
```

This is a sample ftp session showing the transfer of the computer file "`zywall.bin`" to the ZyWALL.

```
ftp>get rom-0 zywall.cfg
```

This is a sample ftp session saving the current configuration to the computer file `zywall.cfg`.

If your [t]ftp client does not allow you have a destination filename different than the source, you will need to rename them as the ZyWALL only recognizes `rom-0` and `ras`. Be sure you keep unaltered copies of both files for later use.

The following table is a summary. Please note that the internal filename refers to the filename on the ZyWALL and the external filename refers to the filename not on the ZyWALL, i.e., on your workstation, local network or ftp site and so the name (but not the extension) will vary. The AT command is the command you enter after you press `y` when prompted in the SMT menu to go into debug mode. After uploading new firmware see the **ZyNOS F/W Version** field in Menu 24.2.1 — System Maintenance — Information to confirm that you have uploaded the correct firmware version.

**Table 10-1 Filename Conventions**

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION	AT COMMAND
Configuration File	Rom-0	*.rom	This is the router 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 console port speed and default password), the error log and the trace log.	ATLC
Firmware	Ras	*.bin	This is the generic name for the ZYNOS firmware on the ZyWALL.	ATUR

### 10.1.1 Firmware Development

It is important to upgrade your firmware regularly, especially if there are problems. If you discover an unexpected behavior, or bug, see if your problem is mentioned in the release notes. Load it according to instructions (e.g., see if the default configuration file is needed also). If the problem still exists, e-mail or call technical support.

## 10.2 Backup Configuration

Option 5 from **Menu 24 - System Maintenance** allows you to backup the current ZyWALL configuration to your workstation. Backup is highly recommended once your ZyWALL is functioning properly. FTP and TFTP are the preferred methods for backing up your current workstation configuration to your computer since FTP and TFTP are faster. You can also perform backup and restore using menu 24 through the console port. Any serial communications program should work fine; however, you must use XMODEM protocol to perform the download/upload and you don't have to rename the files (see *section 10.1*). Please note that terms "download" and "upload" are relative to the workstation. Download means to transfer from the ZyWALL to the workstation, while upload means from your workstation to the ZyWALL.

```
Ready to backup Configuration via Xmodem.
Do you want to continue (y/n):
```

**Figure 10-1 System Maintenance — Backup Configuration**

## 10.2.1 Example: Backup Configuration Using HyperTerminal

This section contains examples of backup configuration, restore configuration and upload firmware using the HyperTerminal program. Other serial communications programs should be similar.

In menu 24.5 enter `y`.

Run the HyperTerminal program. Click **Transfer**, then **Receive File** to display the following screen.

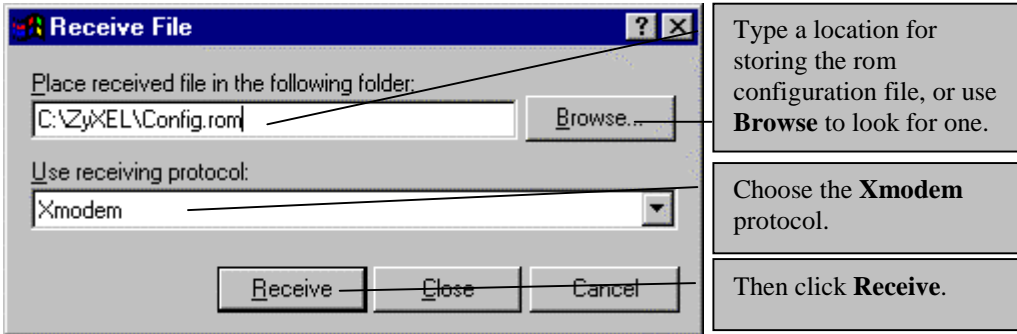


Figure 10-2 Example: Backup Configuration

## 10.2.2 Backup Configuration Using Telnet

Telnetting into the ZyWall produces this Backup Configuration screen.

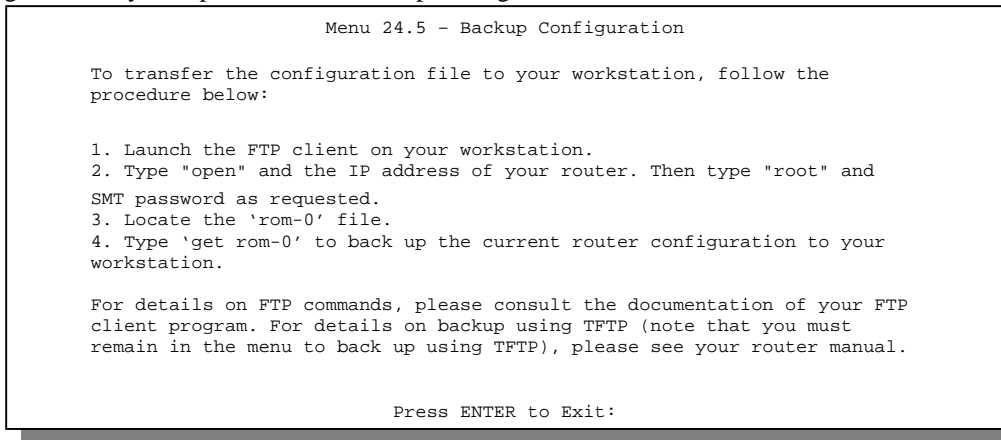


Figure 10-4 Telnet into Menu 24.5 — Backup Configuration

## 10.3 Restore Configuration

**Menu 24.6 -- System Maintenance - Restore Configuration** allows you to restore the configuration via the console port.

FTP and TFTP are the preferred methods for restoring your current workstation configuration to your ZyWALL since FTP and TFTP are faster. Please note that the system reboots automatically after the file transfer is complete.

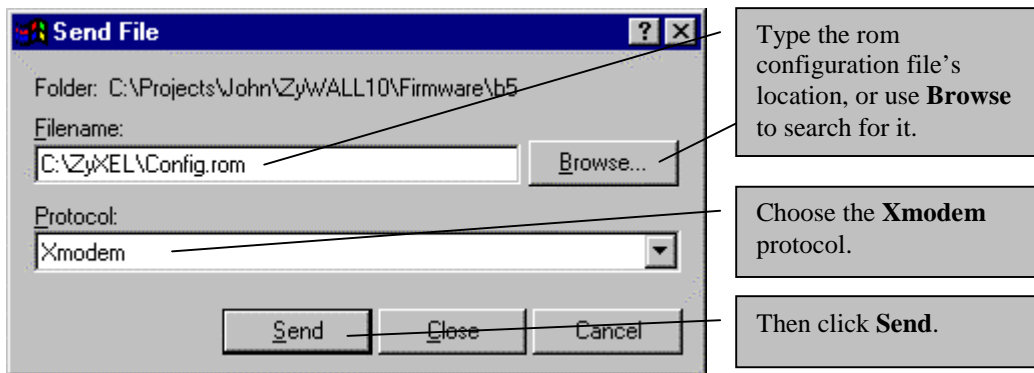
```
Ready to restore Configuration via Xmodem.
Do you want to continue (y/n):
```

**Figure 10-5 System Maintenance — Restore Configuration**

### 10.3.1 Example: Restore Configuration Using HyperTerminal

In menu 24.6 press **y** to continue.

Run the HyperTerminal program. Click **Transfer**, then **Send File** to display the following screen.



**Figure 10-6 Example: Restore Configuration**

```

Menu 24.6 - Restore Configuration

To transfer the firmware and the configuration file, follow the procedure
below:

1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your router. Then type "root" and
SMT password as requested.
3. Type "put backupfilename rom-0" where backupfilename is the name of
your backup configuration file on your workstation and rom-spt is the
remote file name on the router. This restores the configuration to your
router.
4. The system reboots automatically after a successful file transfer.

For details on FTP commands, please consult the documentation of your FTP
client program. For details on restoring using TFTP (note that you must
remain in the menu to back up using TFTP), please see your router manual.

```

**Figure 10-8 Telnet into Menu 24.6 Restore Configuration**

## 10.4 Upload Firmware

**Menu 24.7 -- System Maintenance - Upload Firmware** allows you to upgrade the firmware and the configuration file via the console port. There are two components in the system: the router firmware and the configuration file, as shown below.

```

Menu 24.7 - System Maintenance - Upload Firmware

1. Upload Router Firmware
2. Upload Router Configuration File

Enter Menu Selection Number:

```

**Figure 10-9 Menu 24.7 — System Maintenance — Upload Firmware**

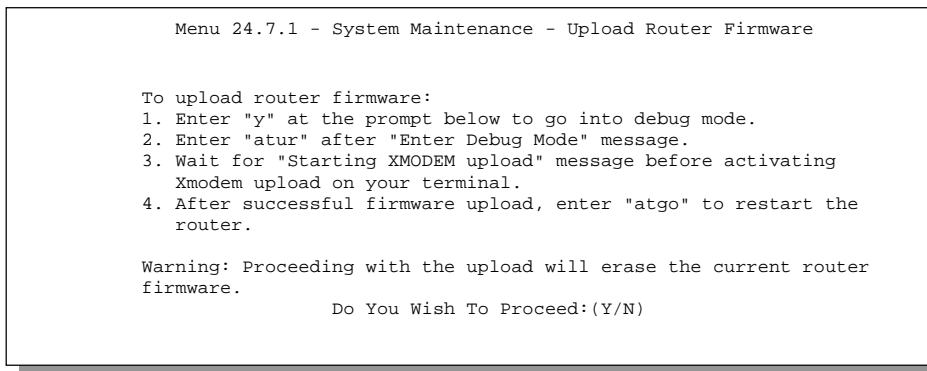
### 10.4.1 Uploading the Router Firmware

Menu 24.7.1 shows you the instructions for uploading the router firmware. Follow the procedure below to upload the file:

- Step 1.** Enter `y` at the prompt to go into debug mode.
- Step 2.** Enter `atur` after the `Enter Debug Mode` message.
- Step 3.** Wait for the `Starting XMODEM upload` message before activating Xmodem upload on your terminal.



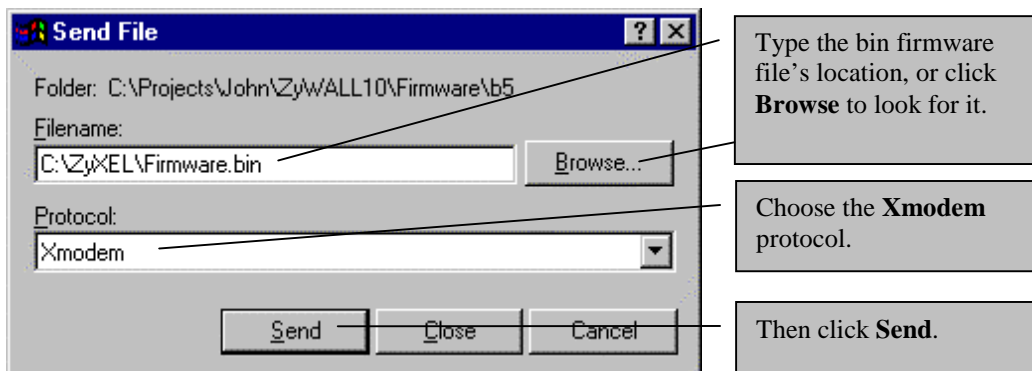
**Step 4.** After successful firmware upload, enter `atgo` to restart the ZyWALL.



**Figure 10-10 Menu 24.7.1 — System Maintenance — Upload Router Firmware**

### 10.4.2 Example: Xmodem Upload Using HyperTerminal

Click **Transfer**, then **Send File** to display the following screen.



**Figure 10-11 Example: Xmodem Upload**

### 10.4.3 Uploading Router Configuration File

The configuration data, system-related data, the error log and the trace log are all stored in the configuration file. Please be aware that uploading the configuration file replaces everything contained within.

---

Menu 24.6 replaces the current configuration with your customized configuration you backed up previously. Menu 24.7.2 shows you the instructions for uploading the Router Configuration file that replaces the current configuration file with the default configuration file, i.e., `zywall.rom`. You will lose all configurations that you had before and the speed of the console port will be reset to the default of 9600 bps with 8 data bit, no parity and 1 stop bit (8n1). You will need to change your serial communications software to the default before you can connect to the ZyWALL again. The password will be reset to the default of 1234, also.

---

Follow the procedure below to upload the configuration file:

- Step 1.** Enter `y` at the prompt to go into debug mode.
- Step 2.** Enter `atlc` after the Enter Debug Mode message.
- Step 3.** Wait for the Starting XMODEM upload message before activating Xmodem upload on your terminal (Xmodem upload will be similar to the previous example for uploading firmware).
- Step 4.** After successful firmware upload, enter `atgo` to restart the ZyWALL.

```

Menu 24.7.2 - System Maintenance - Upload Router Configuration File

To upload router configuration file:
1. Enter "y" at the prompt below to go into debug mode.
2. Enter "atlc" after "Enter Debug Mode" message.
3. Wait for "Starting XMODEM upload" message before activating
   Xmodem upload on your terminal.
4. After successful configuration file upload, enter "atgo" to restart the
   router.

Warning:
1. Proceeding with the upload will erase the current
   configuration file.
2. The router's console port speed (Menu 24.2.2) may change
   when it is restarted; please adjust your terminal's speed
   accordingly. The password may change (menu 23), also.
3. When uploading the DEFAULT configuration file, the console
   port speed will be reset to 9600 bps and the password to
   "1234".

Do You Which To Proceed:(Y/N)

```

**Figure 10-12 Menu 24.7.2 — System Maintenance — Upload Router Configuration File**

## 10.5 TFTP File Transfer

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

To use TFTP, your workstation must have both telnet and TFTP clients. To transfer the firmware and the configuration file, follow the procedure shown next:

- Step 1.** Use telnet from your workstation to connect to the ZyWALL and log in. Because TFTP does not have any security checks, the ZyWALL records the IP address of the telnet client and accepts TFTP requests only from this address.
- Step 2.** Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.
- Step 3.** Enter command `sys stdio 0` to disable the SMT timeout, so the TFTP transfer will not be interrupted. Enter command `sys stdio 5` to restore the five-minute SMT timeout (default) when the file transfer is complete.
- Step 4.** Launch the TFTP client on your workstation and connect to the ZyWALL. Set the transfer mode to binary before starting data transfer.
- Step 5.** Use the TFTP client (see the example below) to transfer files between the ZyWALL and the workstation. The file name for the firmware is `ras` and the configuration file is `rom-0` (rom-zero, not capital o).

---

If you upload the firmware to the ZyWALL, it will reboot automatically when the file transfer is completed (the SYS LED will flash).

---

Note that the telnet connection must be active and the SMT in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use “get” to transfer from the ZyWALL to the workstation, “put” the other way around, and “binary” to set binary transfer mode.

### 10.5.1 Example: TFTP Command

The following is an example tftp command:

```
TFTP [-i] host put zywll.bin ras
```

where “i” specifies binary image transfer mode (use this mode when transferring binary files), “host” is the ZyWALL IP address, “put” transfers the file source on the workstation (zywall.bin – name of the firmware on the workstation) to the file destination on the remote host (ras - name of the firmware on the ZyWALL). The following table describes some of the fields that you may see in third party TFTP clients.

**Table 10-2 Third Party TFTP Clients — General commands**

COMMAND	DESCRIPTION
Host	Enter the IP address of the ZyWALL. 192.168.1.1 is the ZyWALL default IP address when shipped.
Send/Fetch	Press “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.

COMMAND	DESCRIPTION
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.

TFTP over WAN will not work if:

1. You have disabled Telnet service in menu 24.11.
2. You have applied a filter in menu 3.1 (LAN) or in menu 11.5 (WAN) to block Telnet service.
3. The IP you entered in **the Secured Client IP** field in menu 24.11 does not match the client IP. If it does not match, the ZyWALL will disconnect the Telnet session immediately.
4. You have an SMT console session running.
5. The firewall is active. The default firewall policies block all traffic from the WAN, so to enable TFTP over the WAN, you must turn the firewall off (menu 21.2) or create a firewall rule to allow TFTP from the WAN.

## 10.6 FTP File Transfer

In addition to uploading the firmware and configuration via the console port and TFTP client, you can also upload the ZyWALL firmware and configuration files using FTP. To use this feature, your workstation must have an FTP client.

When you telnet into the ZyWALL, you will see the following screens for uploading firmware and the configuration file using FTP.

### Menu 24.7.1 - System Maintenance - Upload Router Firmware

To upload the router firmware, follow the procedure below:

1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your router. Then type "root" and SMT password as requested.
3. Type "put firmwarefilename ras" where "firmwarefilename" is the name of your firmware upgrade file on your workstation and "ras" is the remote file name on the router.
4. The system reboots automatically after a successful firmware upload.

For details on FTP commands, please consult the documentation of your FTP client program. For details on uploading router firmware using TFTP (note that you must remain on this menu to upload router firmware using TFTP), please see your router manual.

Press ENTER to Exit:

**Figure 10-13 Telnet into Menu 24.7.1**

You see the following screen when you telnet into menu 24.7.2.

Menu 24.7.2 - System Maintenance - Upload Router Configuration File  
To upload the router configuration file, follow the procedure below:

1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your router. Then type "root" and SMT password as requested.
3. Type "put configurationfilename rom-0" where "configurationfilename" is the name of your router configuration file on your workstation, which will be transferred to the "rom-0" file on the router.
4. The system reboots automatically after the upload router configuration file process is complete.

For details on FTP commands, please consult the documentation of your FTP client program. For details on uploading router firmware using TFTP (note that you must remain on this menu to upload router firmware using TFTP), please see your router manual.

Press ENTER to Exit:

**Figure 10-14 Telnet into Menu 24.7.2 — System Maintenance**

To transfer the firmware and the configuration file, follow these examples:

## 10.6.1 Using the FTP command from the DOS Prompt

- Step 1.** Launch the FTP client on your workstation.
- Step 2.** Type `open` and the IP address of your ZyWALL.
- Step 3.** Press [ENTER] when prompted for a username.
- Step 4.** Type `root` and your SMT password as requested. The default is 1234.
- Step 5.** Type `bin` to set transfer mode to binary.
- Step 6.** Use “put” to transfer files from the workstation to the ZyWALL, e.g., `put zywall.bin ras` transfers the firmware on your computer (`zywall.bin`) to the ZyWALL and renames it “ras”. Similarly `put zywall.rom rom-0` transfers the configuration file on your computer (`zywall.rom`) to the ZyWALL and renames it “rom-0”. Likewise `get rom-0 zywall.rom` transfers the configuration file on the ZyWALL to your computer and renames it `zywall.rom`. See *section 10.1* for more information on filename conventions.
- Step 7.** Type `quit` to exit the ftp prompt.

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> put zywall.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 327680 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

**Figure 10-15 FTP Session Example**

---

The system reboots after a successful upload.

---

The following table describes some of the fields that you may see in third party FTP clients.

**Table 10-3 Third Party FTP Clients — General Fields**

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	Anonymous.  This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option.  Normal.  The server requires a unique User ID and Password to login.
Transfer Type	Transfer files in either ASCII (plain text format) or in binary mode.
Initial Remote Directory.	Specify the default remote directory (path).
Initial Local Directory.	Specify the default local directory (path).

FTP over WAN will not work if:

1. You have disabled Telnet service in menu 24.11.
2. You have applied a filter in menu 3.1 (LAN) or in menu 11.5 (WAN) to block Telnet service.
3. The IP you entered in **the Secured Client IP** field in menu 24.11 does not match the client IP. If it does not match, the ZyWALL will disconnect the Telnet session immediately.
4. You have an SMT console session running.
5. The firewall is active. The default firewall policies block all traffic from the WAN, so to enable FTP over the WAN, you must turn the firewall off (menu 21.2) or create a firewall rule to allow FTP from the WAN.

# Chapter 11

## System Maintenance & Information

*This chapter leads you through SMT menus 24.8 to 24.11.*

### 11.1 Command Interpreter Mode

The Command Interpreter (CI) is a part of the main router firmware. The CI provides much of the same functionality as the SMT, while adding some low-level setup and diagnostic functions. The CI can be entered from the SMT by selecting menu 24.8. Access can be either by Telnet or by a serial connection to the console port, although some commands are only available with a serial connection. See the included disk or the [zyxel.com](http://zyxel.com) web site for more detailed information on CI commands. Enter 8 from **Menu 24 - System Maintenance**. A list of valid commands can be found by typing `help` or `?` at the command prompt. Type “exit” to return to the SMT main menu when finished.

```
Menu 24 - System Maintenance

1. System Status
2. System Information and Console Port Speed
3. Log and Trace
4. Diagnostic
5. Backup Configuration
6. Restore Configuration
7. Firmware Update
8. Command Interpreter Mode
9. Call Control
10. Time and Date Setting
11. Remote Management Setup

Enter Menu Selection Number:
```

**Figure 11-1 Command Mode in Menu 24**

```
Copyright (c) 1994 - 2001 ZyXEL Communications Corp.
ras> ?
Valid commands are:
sys                exit                device            ether
poe                config              ip                ppp
hdap
ras>
```

**Figure 11-2 Valid Commands**



## 11.2 Call Control Support

The ZyWALL provides two call control functions: budget management and call history. Please note that this menu is only applicable when **Encapsulation** is set to **PPPoE** or **PPTP** in menu 4 or menu 11.1. The budget management function allows you to set a limit on the total outgoing call time of the ZyWALL within certain times. When the total outgoing call time exceeds the limit, the current call will be dropped and any future outgoing calls will be blocked.

Call history chronicles preceding incoming and outgoing calls.

To access the call control menu, select option 9 in menu 24 to go to **Menu 24.9 - System Maintenance - Call Control**, as shown in the next table.

```
Menu 24.9 - System Maintenance - Call Control

1. Budget Management
2. Call History

Enter Menu Selection Number:
```

**Figure 11-3 Call Control**

### 11.2.1 Budget Management

Menu 24.9.1 shows the budget management statistics for outgoing calls. Enter 1 from **Menu 24.9 - System Maintenance - Call Control** to bring up the following menu.

```
Menu 24.9.1 - Budget Management

Remote Node      Connection Time/Total Budget    Elapsed Time/Total Period
1. ChangeMe      No Budget                       No Budget

Reset Node (0 to update screen):
```

**Figure 11-4 Budget Management**

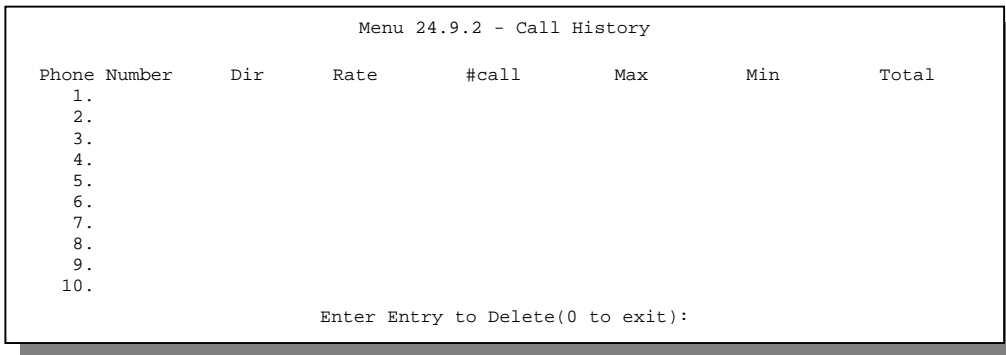
The total budget is the time limit on the accumulated time for outgoing calls to a remote node. When this limit is reached, the call will be dropped and further outgoing calls to that remote node will be blocked. After each period, the total budget is reset. The default for the total budget is 0 minutes and the period is 0 hours, meaning no budget control. You can reset the accumulated connection time in this menu by entering the index of a remote node. Enter 0 to update the screen. The budget and the reset period can be configured in menu 11.1 for the remote node.

**Table 11-1 Budget Management**

FIELD	DESCRIPTION	EXAMPLE
Remote Node	Enter the index number of the remote node you want to reset (just one in this case)	1
Connection Time/Total Budget	This is the total connection time that has gone by (within the allocated budget that you set in menu 11.1.	5/10 means that 5 minutes out of a total allocation of 10 minutes have lapsed.
Elapsed Time/Total Period	The period is the time cycle in hours that the allocation budget is reset (see menu 11.1.) The elapsed time is the time used up within this period.	0.5/1 means that 30 minutes out of the 1 hour time period has lapsed.
Enter "0" to update the screen or press [ESC] to return to the previous screen.		

### 11.2.2 Call History

This is the second option in **Menu 24.9 - System Maintenance - Call Control**. It displays information about past incoming and outgoing calls. Enter 2 from **Menu 24.9 - System Maintenance - Call Control** to bring up the following menu.



**Figure 11-5 Call History**

**Table 11-2 Call History Fields**

FIELD	DESCRIPTION
Phone Number	The PPPoE service names are shown here.
Dir	This shows whether the call was incoming or outgoing.
Rate	This is the transfer rate of the call.
#call	This is the number of calls made to or received from that telephone number.
Max	This is the length of time of the longest telephone call.
Min	This is the length of time of the shortest telephone call.
Total	This is the total length of time of all the telephone calls to/from that telephone number.
You may enter an entry number to delete it or "0" to exit.	

## 11.3 Time and Date Setting

There is no Real Time Chip (RTC) in the ZyWALL, so there is a software mechanism to set the time manually or get the current time and date from an external server when you turn on your ZyWALL. Menu 24.10 allows you to update the time and date settings of your ZyWALL. The real time is then displayed in the ZyWALL error logs and firewall logs. If you do not choose a time service protocol that your timeserver will send when you turn on the ZyWALL, then you can enter the time manually but each time the system is booted, the time and date will be reset to 2000/01/01 00:00:00.

Select menu 24 in the main menu to open **Menu 24 - System Maintenance**, as shown next.

```
Menu 24 - System Maintenance

1. System Status
2. System Information and Console Port Speed
3. Log and Trace
4. Diagnostic
5. Backup Configuration
6. Restore Configuration
7. Upload Firmware
8. Command Interpreter Mode
9. Call Control
10. Time and Date Setting
11. Remote Management Setup

Enter Menu Selection Number:
```

**Figure 11-6 Menu 24 — System Maintenance**

Then enter 10 to go to **Menu 24.10 - System Maintenance - Time and Date Setting** to update the time and date settings of your ZyWALL as shown in the following screen.

```
Menu 24.10 - System Maintenance - Time and Date Setting

Use Time Server when Bootup= None
Time Server IP Address= N/A

Current Time:                00 : 00 : 00
New Time (hh:mm:ss):        11 : 23 : 16

Current Date:                2000 - 01 - 01
New Date (yyyy-mm-dd):      2001 - 03 - 01

Time Zone= GMT+0800

Daylight Saving= No
Start Date (mm-dd):          01 - 00
End Date (mm_dd):            01 - 00

Press ENTER to Confirm or ESC to Cancel:
```

**Figure 11-7 Menu 24.10 System Maintenance — Time and Date Setting**

**Table 11-3 Time and Date Setting Fields**

FIELD	DESCRIPTION
Use Time Server when Bootup	<p>Enter the time service protocol that your time server sends when you turn on the ZyWALL. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main differences between them are the format.</p> <p><b>Daytime (RFC 867)</b> format is day/month/year/time zone of the server.</p> <p><b>Time (RFC-868)</b> format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0.</p> <p><b>NTP (RFC-1305)</b> is similar to <b>Time (RFC-868)</b>.</p> <p><b>None</b> is the default value. Enter the time manually. Each time you turn on the ZyWALL, the time and date will be reset to 2000-1-1 0:0:0.</p>
Time Server IP Address	Enter the IP address of your time server. Check with your ISP/network administrator if you are unsure of this information.
Current Time New Time	<p>This field displays an updated time only when you reenter this menu.</p> <p>Enter the new time in hour, minute and second format.</p>
Current Date New Date	<p>This field displays an updated date only when you reenter this menu.</p> <p>Enter the new date in year, month and day format.</p>
Time Zone	Press [SPACE BAR] to set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Saving Start Date End Date	<p>If you use daylight savings time, then choose <b>Yes</b>.</p> <p>If using daylight savings time, enter the month and day that it starts on.</p> <p>If using daylight savings time, enter the month and day that it ends on</p>
Once you have filled in this menu, press [ENTER] at the message "Press ENTER to Confirm or ESC to Cancel" to save your configuration, or press [ESC] to cancel.	

## How often does the ZyWALL update the time?

The ZyWALL updates the time in three instances:

- i. On leaving menu 24.10 after making changes.
- ii. When the ZyWALL boots up and there is a time server configured in menu 24.10.
- iii. 24-hour intervals after booting.

## 11.4 Remote Management Setup

Telnet and FTP do not support encryption, so for very strong security both services should be shut down. This is done in **Menu 24.11 - Remote Management Control**. Enter 11 from menu 24 to bring up this menu. All Telnet and FTP activity, both LAN and WAN may be disabled by selecting **No** (press the [SPACE BAR] to select **No**) in the two fields in this menu. If you just wish to block certain users from using these activities, then please use filtering – see *menu 21.1*.

```

Menu 24.11 - Remote Management Control

FTP service active = Yes
Telnet service active = Yes
Secured Client IP= 0.0.0.0

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.

```

**Figure 11-8 Menu 24.11 — Remote Management Control**

---

Remote management is only allowed from one single IP host.

---

**Table 11-4 Menu 24.11 — Remote Management Control**

FIELD	DESCRIPTION	EXAMPLE
FTP service active	Press [SPACE BAR] to select <b>No</b> and press [ENTER] to disable all FTP activity (both LAN and WAN).	<b>No</b>
Telnet service active	Press [SPACE BAR] to select <b>No</b> and press [ENTER] to disable all Telnet activity (both LAN and WAN).	<b>No</b>
Secured Client IP	The default value for <b>Secured Client IP</b> is 0.0.0.0, which means you don't care which host is trying to telnet. If you enter an IP in this field, the ZyWALL will check if the client IP matches the value here when a Telnet session is up. If it does not match, the ZyWALL will disconnect the session immediately. If the Telnet service active field is disabled ( <b>No</b> ) then this field is not applicable ( <b>N/A</b> ).	0.0.0.0

## 11.5 Boot Commands

The BootModule AT commands execute from within the router's bootup software, when debug mode is selected before the main router firmware (ZyNOS) is started. When you start up your ZyWALL, you are given a choice to go into debug mode by pressing a key at the prompt shown in the following screen. In debug mode you have access to a series of boot module commands, for example ATUR (for uploading firmware) and ATLC (for uploading the configuration file). These are already discussed in the *Transferring Files* chapter.

```
Bootbase Version: V2.02 | 10/11/2000 13:58:03
RAM: Size = 8192 Kbytes
DRAM Post: Testing: 8192K OK
FLASH: Intel 16M

ZyNOS Version: V324\wa0b05 | 3/5/2001 18:00:34

Press any key to enter debug mode within 3 seconds.
```

**Figure 11-9 Option to Enter Debug Mode**

Enter ATHE to view all available ZyWALL boot module commands as shown in the next screen. ATBAx allows you to change the console port speed. The x denotes the number preceding the colon to give the console port speed following the colon in the list of numbers that follows; e.g., ATBA3 will give a console port speed of 9.6 Kbps. ATSE displays the seed that is used to generate a password to turn on the debug flag in the firmware. The ATSH command shows product related information such as boot module version, vendor name, product model, RAS code revision, etc. ATGO allows you to continue booting the system. Most other commands aid in advanced troubleshooting and should only be used by qualified engineers.

```

===== Debug Command Listing =====
AT          just answer OK
ATHE       print help
ATBAX      change baudrate. 1:38.4k, 2:19.2k, 3:9.6k 4:57.6k 5:115.2k
ATENx,(y)  set BootExtension Debug Flag (y=password)
ATSE       show the seed of password generator
ATTI(h,m,s) change system time to hour:min:sec or show current time
ATDA(y,m,d) change system date to year/month/day or show current date
ATDS       dump RAS stack
ATDT       dump Boot Module Common Area
ATDUX,y    dump memory contents from address x for length y
ATWBx,y    write address x with 8-bit value y
ATWwx,y    write address x with 16-bit value y
ATWLx,y    write address x with 32-bit value y
ATRBx     display the 8-bit value of address x
ATRWx     display the 16-bit value of address x
ATRLx     display the 32-bit value of address x
ATGO(x)   run program at addr x or boot router
ATGR       boot router
ATGT       run Hardware Test Program
AT%Tx     Enable Hardware Test Program at boot up
ATBTx     block0 write enable (1=enable, other=disable)
ATRTw,x,y,(z) RAM test level w, from address x to y (z iterations)
ATWEa(b,c,d) write MAC addr, Country code, EngDbgFlag, FeatureBit to flash ROM
ATCUX     write Country code to flash ROM
ATCB       copy from FLASH ROM to working buffer
ATCL       clear working buffer
ATSB       save working buffer to FLASH ROM
ATBU       dump manufacturer related data in working buffer
ATSH       dump manufacturer related data in ROM
ATWMx     set MAC address in working buffer
ATCOx     set country code in working buffer
ATFLx     set EngDebugFlag in working buffer
ATSTx     set ROMRAS address in working buffer
ATSYx     set system type in working buffer
ATVDx     set vendor name in working buffer
ATPNx     set product name in working buffer
ATFEx,y,... set feature bits in working buffer
ATMP       check & dump memMapTab
ATDOx,y    download from address x for length y to PC via XMODEM
ATTD       download router configuration to PC via XMODEM
ATUPx,y    upload to RAM address x for length y from PC via XMODEM
ATUR       upload router firmware to flash ROM
ATLC       upload router configuration file to flash ROM
ATUXx(,y)  xmodem upload from flash block x to y
ATERx,y    erase flash rom from block x to y
ATWFx,y,z  copy data from addr x to flash addr y, length z
ATXSx     xmodem select: x=0: CRC mode(default); x=1: checksum mode
ATLOa,b,c,d Int/Trap Log Cmd

```

**Figure 11-10 Boot Module Commands**





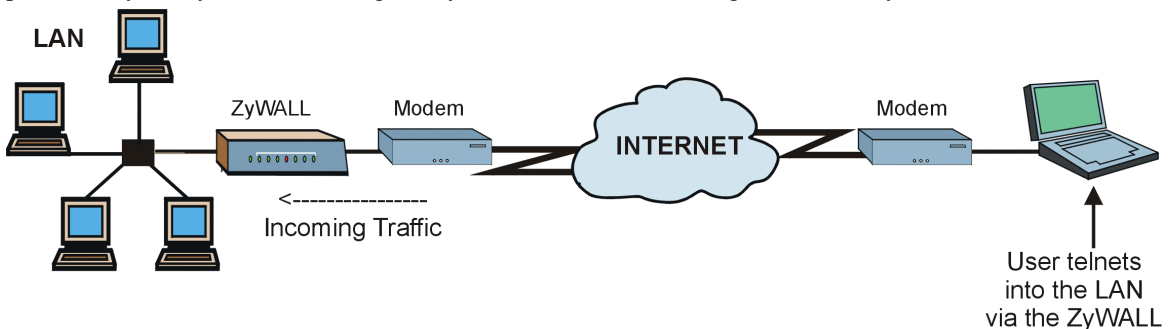
# Chapter 12

## Telnet Configuration and Capabilities

*This chapter covers the Telnet Configuration and Capabilities of the ZyWALL.*

### 12.1 About Telnet Configuration

Before the ZyWALL is properly setup for TCP/IP, the only option for configuring it is through the console port. Once your ZyWALL is configured, you can use telnet to configure it remotely as shown below.



**Figure 12-1 Telnet Configuration on a TCP/IP Network**

### 12.2 Telnet Under NAT

When Network Address Translation (NAT) is enabled and an inside server is specified, telnet connections from the outside will be forwarded to the inside server. So to configure the ZyWALL via telnet from the outside, you must first telnet to the inside server, and then telnet from the server to the ZyWALL using its inside LAN IP address. If no inside server is specified, telnetting to the NAT's IP address will connect to the ZyWALL directly.

### 12.3 Telnet Capabilities

#### 12.3.1 Single Administrator

To prevent confusion and discrepancy on the configuration, your ZyWALL only allows one administrator to log in at any time. Your ZyWALL also gives priority to the console port over telnet. If you have already connected to your ZyWALL via telnet, you will be logged out if another user logs in to the ZyWALL via the console port.

### 12.3.2 System Timeout

There is a system timeout of 5 minutes (300 seconds) for either the console port or telnet. Your ZyWALL will automatically log you out if you do nothing in this timeout period, except when it is continuously updating the status in menu 24.1 or when `sys studio` has been changed on the command line.

### 12.4 Telnet Behind the Firewall

Telnet over the WAN will not work if the firewall is active because the default firewall policies block all traffic from the WAN to the LAN. To enable Telnet over the WAN, you must turn the firewall off (menu 21.2) or create a firewall rule to allow Telnet from the WAN. Telnet will also not work when

1. You have disabled Telnet service in menu 24.11.
2. You have applied a filter in menu 3.1 (LAN) or in menu 11.5 (WAN) to block Telnet service.
3. The IP you entered in the **Secured Client IP** field in menu 24.11 does not match the client IP. If it does not match, the ZyWALL will disconnect the Telnet session immediately.
4. You have an SMT console session running.
5. The firewall is active. The default firewall policies block all traffic from the WAN, so to enable FTP over the WAN, you must turn the firewall off (menu 21.2) or create a firewall rule to allow FTP from the WAN.

---

# Part IV:

---

## Firewall and Content Filters

---

Chapters 13 — 20 define the term “Firewall”, introduce the ZyWALL Firewall and ZyWALL Web Configurator, describe how to create Custom Rules and configure customized ports, explain Logs and provide Example Firewall Rules. Chapter 20 explains Content Filtering and how to use the ZyWALL to restrict web features such as ActiveX controls and Java applets, etc.



# Chapter 13

## What is a Firewall?

*This chapter gives some background information on Firewalls.*

Originally, the term *firewall* referred to a construction technique designed to prevent the spread of fire from one room to another. The network term firewall is typically defined as 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.

### 13.1 Types of Firewalls

There are three main types of firewalls:

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

#### 13.1.1 Packet Filtering Firewalls

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

#### 13.1.2 Application-level Firewalls

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

- i. Information hiding prevents the names of internal systems from being made known via DNS to outside systems, since the application gateway is the only host whose name must be made known to outside systems.

- ii. Robust authentication and logging pre-authenticates application traffic before it reaches internal hosts and causes it to be logged more effectively than if it were logged with standard host logging. Filtering rules at the packet filtering router can be less complex than they would be if the router needed to filter application traffic and direct it to a number of specific systems. The router need only allow application traffic destined for the application gateway and reject the rest.

### 13.1.3 Stateful Inspection Firewalls

Stateful inspection firewalls restrict access by screening data packets against defined access rules. They make access control decisions based on IP address and protocol. They also "inspect" the session data to assure the integrity of the connection and to adapt to dynamic protocols. These firewalls generally provide the best speed and transparency, however, they may lack the granular application level access control or caching that some proxies support. See *section 13.4* for more information on Stateful Inspection.

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

## 13.2 Introduction to ZyXEL's Firewall

The ZyWALL firewall is a stateful inspection firewall and is designed to protect against Denial of Service attacks when activated (in SMT menu 21.2 or in the ZyWALL Web Configurator). The ZyWALL's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The ZyWALL can be used to prevent theft, destruction and modification of data, as well as log events, which may be important to the security of your network. The ZyWALL also has packet filtering capabilities.

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

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

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

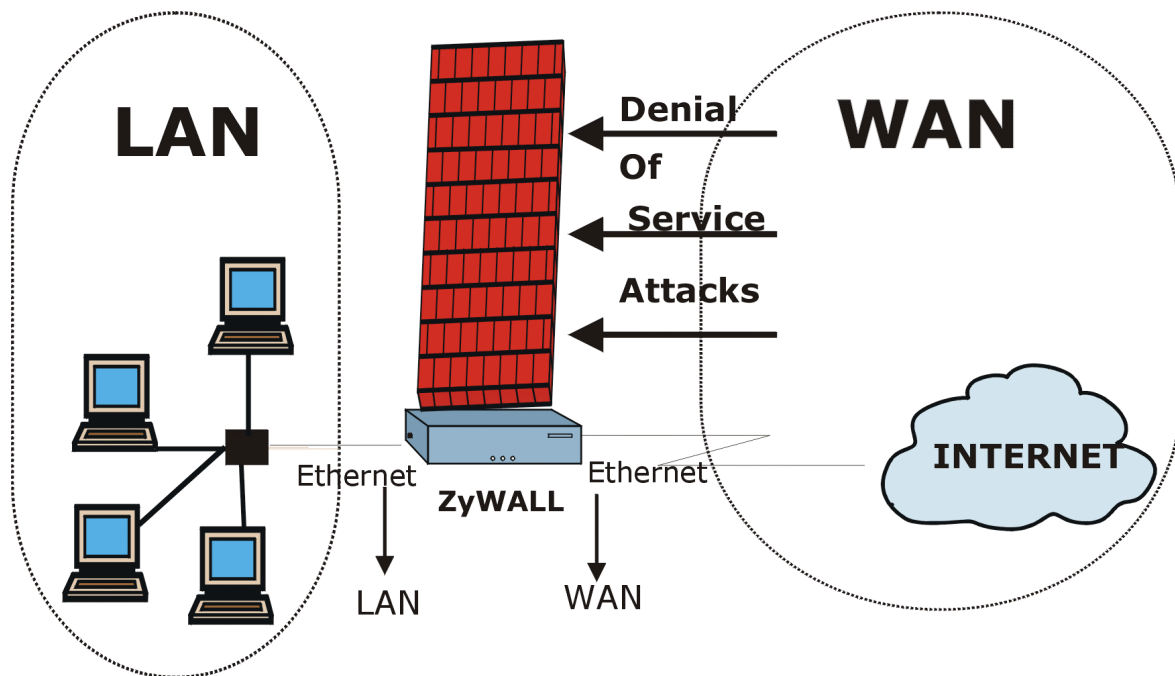


Figure 13-1 ZyWALL Firewall Application

## 13.3 Denial of Service

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

### 13.3.1 Basics

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

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



Some of the most common IP ports are:

**Table 13-1 Common IP Ports**

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

### 13.3.2 Types of DoS attacks

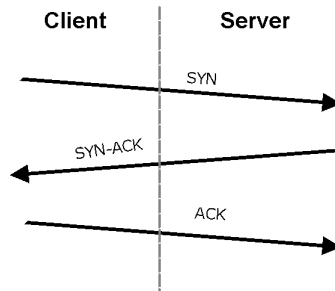
There are four types of DoS attacks:

1. Those that exploit bugs in a TCP/IP implementation.
2. Those that exploit weaknesses in the TCP/IP specification.
3. Brute-force attacks that flood a network with useless data.
4. IP Spoofing.
1. "**Ping of Death**" and "**Teardrop**" attacks exploit bugs in the TCP/IP implementations of various computer and host systems.

1-a Ping of Death uses a "ping" utility to create an IP packet that exceeds the maximum 65,536 bytes of data allowed by the IP specification. The oversize packet is then sent to an unsuspecting system. Systems may crash, hang or reboot.

1-b Teardrop attack exploits weaknesses in the reassembly of IP packet fragments. As data is transmitted through a network, IP packets are often broken up into smaller chunks. Each fragment looks like the original IP packet except that it contains an offset field that says, for instance, "This fragment is carrying bytes 200 through 400 of the original (non fragmented) IP packet." The Teardrop program creates a series of IP fragments with overlapping offset fields. When these fragments are reassembled at the destination, some systems will crash, hang, or reboot.

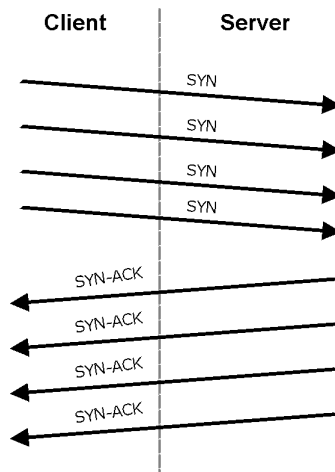
2. Weaknesses in the TCP/IP specification leave it open to "**SYN Flood**" and "**LAND**" attacks. These attacks are executed during the handshake that initiates a communication session between two applications.



**Figure 13-2 Three-Way Handshake**

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

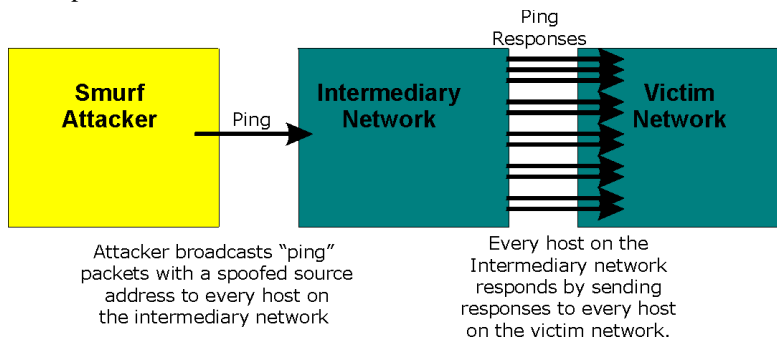
**2-a SYN Attack** floods a targeted system with a series of SYN packets. Each packet causes the targeted system to issue a SYN-ACK response. While the targeted system waits for the ACK that follows the SYN-ACK, it queues up all outstanding SYN-ACK responses on what is known as a backlog queue. SYN-ACKs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



**Figure 13-3 SYN Flood**

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

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



**Figure 13-4 Smurf Attack**

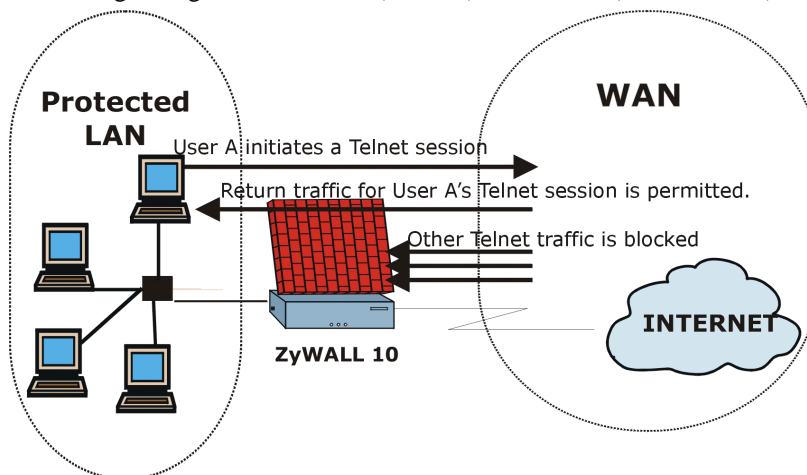
4. Often, many DoS attacks also employ a technique known as "**IP Spoofing**" as part of their attack. IP Spoofing may be used to break into systems, to hide the hacker's identity, or to magnify the effect of the DoS attack. IP Spoofing is a technique used to gain unauthorized access to computers by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

## 13.4 Stateful Inspection

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

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

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



**Figure 13-5 Stateful Inspection**

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

### 13.4.1 Stateful Inspection Process

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

1. The packet travels from the firewall's LAN to the WAN.
2. The packet is evaluated against the interface's existing outbound access list, and the packet is permitted (a denied packet would simply be dropped at this point).
3. The packet is inspected by a firewall rule to determine and record information about the state of the packet's connection. This information is recorded in a new state table entry created for the new connection. If there is not a firewall rule for this packet and it is not an attack, then **The default action for packets not matching following rules** field (see *Figure 16-3*) determines the action for this packet.
4. Based on the obtained state information, a firewall rule creates a temporary access list entry that is inserted at the beginning of the WAN interface's inbound extended access list. This temporary access list entry is designed to permit inbound packets of the same connection as the outbound packet just inspected.
5. The outbound packet is forwarded out the interface.

6. Later, an inbound packet reaches the interface. This packet is part of the connection previously established with the outbound packet. The inbound packet is evaluated against the inbound access list, and is permitted because of the temporary access list entry previously created.
7. The packet is inspected by a firewall rule, and the connection's state table entry is updated as necessary. Based on the updated state information, the inbound extended access list temporary entries might be modified, in order to permit only packets that are valid for the current state of the connection.
8. Any additional inbound or outbound packets that belong to the connection are inspected to update the state table entry and to modify the temporary inbound access list entries as required, and are forwarded through the interface.
9. When the connection terminates or times out, the connection's state table entry is deleted and the connection's temporary inbound access list entries are deleted.

### 13.4.2 Stateful Inspection & the ZyWALL

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

- i. Block all traffic of a certain type, such as IRC (Internet Relay Chat), from the LAN to the Internet.
- ii. Allow certain types of traffic from the Internet to specific hosts on the LAN.
- iii. Allow access to a Web server to everyone but competitors.
- iv. Restrict use of certain protocols, such as Telnet, to authorized users on the LAN.

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

---

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

---

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

### 13.4.3 TCP Security

The ZyWALL use state information embedded in TCP packets. The first packet of any new connection has its SYN flag set and its ACK flag cleared; these are "initiation" packets. All packets that do not have this flag structure are called "subsequent" packets, since they represent data that occurs later in the TCP stream. If an initiation packet originates on the WAN, this means that someone is trying to make a connection from the Internet into the LAN. Except in a few special cases (see "Upper Layer Protocols" shown next), these packets are dropped and logged.

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

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

### **13.4.4 UDP/ICMP Security**

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

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

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

### **13.4.5 Upper Layer Protocols**

Some higher layer protocols (such as FTP and RealAudio) utilize multiple network connections simultaneously. In general terms, they usually have a "control connection" which is used for sending commands between endpoints, and then "data connections" which are used for transmitting bulk information. Consider the FTP protocol. A user on the LAN opens a control connection to a server on the Internet and requests a file. At this point, the remote server will open a data connection from the Internet. For FTP to work properly, this connection must be allowed to pass through even though a connection from the Internet would normally be rejected.

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

Any protocol that operates in this way must be supported on a case-by-case basis. You can use the ZyWALL Web Configurator's Custom Ports feature to do this.

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

1. Change the default password on the SMT and Web Configurator.

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

### 13.5.1 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.
7. 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.

8. 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 #.
9. 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.
10. If you use “chat rooms” or IRC sessions, be careful with any information you reveal to strangers.
11. 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.
12. 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.





# Chapter 14

## Introducing the ZyWALL Firewall

*This chapter shows you how to get started with the ZyWALL Firewall. Please see Chapter 13 for some background information on firewalls.*

### 14.1 SMT Menus

From the main menu (see below) enter 21 to go to **Menu 21 - Filter Set and Firewall Configuration**.

```
Copyright (c) 1994 - 2000 ZyXEL Communications Corp.

ZyWALL 10 Main Menu

Getting Started
1. General Setup
2. WAN Setup
3. LAN Setup
4. Internet Access Setup

Advanced Applications
11. Remote Node Setup
12. Static Routing Setup
15. NAT Setup

Advanced Management
21. Filter and Firewall Setup
22. SNMP Configuration
23. System Password
24. System Maintenance

26. Schedule Setup

99. Exit

Enter Menu Selection Number:
```

**Figure 14-1 SMT Main Menu**

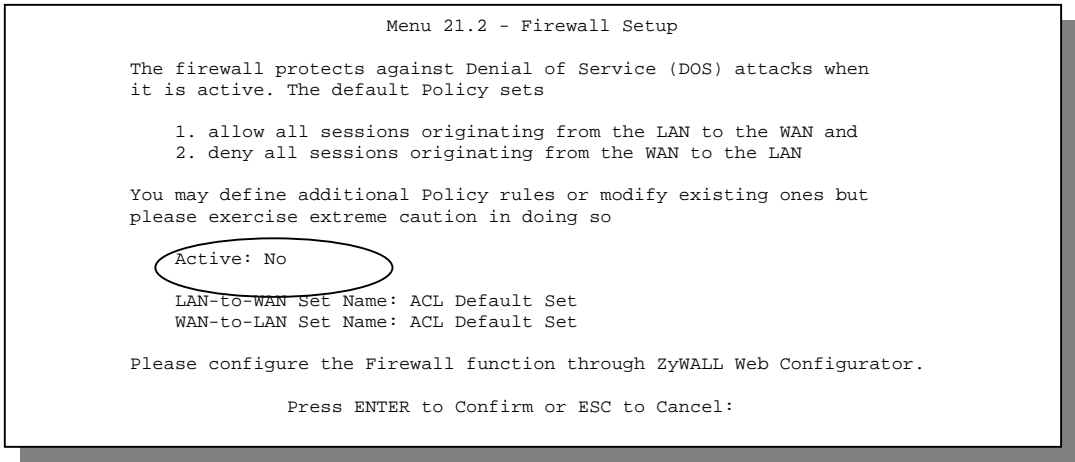
This is menu 21.

```
Menu 21 - Filter and Firewall Setup

1. Filter Setup
2. Firewall Setup
3. View Firewall Log
```

**Figure 14-2 Menu 21 — Filter and Firewall Setup**

Enter option 2 in this menu to bring up the following screen. Press the [SPACE BAR] to select **Yes** in the **Active** field to activate the firewall. The firewall must be active to protect against Denial of Service (DoS) attacks. Additional rules may be configured using the ZyWALL Web Configurator.



**Figure 14-3 Menu 21.2 — Firewall Setup**

---

Configure the firewall rules using the ZyWALL Web Configurator or CLI commands.

---

### 14.1.1 View Firewall Log

Enter option 3 from menu 21 to view the firewall log. Firewall logs may also be viewed from the ZyWALL Web Configurator or may be sent to a syslog server using SMT **Menu 24.3.2 - System Maintenance - UNIX Syslog** and setting the **Firewall log** field to **Yes**. Attack types that may be displayed in the “Reason” column of the firewall log are briefly described in *Table 14-4 View Firewall Log*.

### 14.1.2 Attack Types

#### Land

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

#### IP Spoofing

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

## ICMP Echo

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

## ICMP Vulnerability

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

**Table 14-1 ICMP Commands That Trigger Alerts**

5	REDIRECT
13	TIMESTAMP_REQUEST
14	TIMESTAMP_REPLY
17	ADDRESS_MASK_REQUEST
18	ADDRESS_MASK_REPLY

## Illegal Commands (NetBIOS and SMTP)

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

**Table 14-2 Legal NetBIOS Commands**

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

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

**Table 14-3 Legal SMTP Commands**

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

**Traceroute**

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

**Teardrop**

Teardrop attacks exploit weaknesses in the reassembly of IP packet fragments. As data is transmitted through a network, IP packets are often broken up into smaller chunks. Each fragment looks like the original IP packet except that it contains an offset field that says, for instance, "This fragment is carrying bytes 200 through 400 of the original (non fragmented) IP packet." The Teardrop program creates a series of IP fragments with overlapping offset fields. When these fragments are reassembled at the destination, some systems will crash, hang, or reboot.

**SYN Flood**

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

Attack types and some background are described in more detail in *Chapter 13*.

#	Time	Packet Information	Reason	Action
124	Jan 1 00 00:01:30	From:192.168.1.2 To: 10.100.6.45 TCP src port:01060 dest port:00119	not match <2,01>protocol	none
125	Jan 1 00 22:10:10	From:192.168.1.2 To: 10.100.6.66 UDP src port:01053 dest port:00053	match <1,02>	block
126	Jan 1 00 23:10:30	From:192.168.1.2 To: 10.100.6.66 UDP src port:01054 dest port:00053	not match <1,02>dest port	none
127	Jan 1 00 23:20:30	From:192.168.1.2 To: 10.100.6.45 ICMP type:00008 code:00000	attack land	block
Clear Firewall Log (y/n):				

**Figure 14-4 View Firewall Log**

Each log consists of two lines, showing the information described in the following table.

Table 14-4 View Firewall Log

FIELD	DESCRIPTION	EXAMPLES
#	This is the index number of the firewall log. 128 entries are available numbered from 0 to 127. Once they are all used, the log will wrap around and the old logs will be lost.	23
Time	This is the time the log was recorded in this format. You must configure menu 24.10 for real time; otherwise the clock will start at 2000/01/01 00:00:00 the last time the ZyWALL 10 was reset.	mm:dd:yy e.g., Jan 1 00
		hh:mm:ss e.g., 00:00:00
Packet Information	This field lists packet information such as protocol and src/dest port numbers (TCP, UDP), or protocol, type and code (ICMP).	From and To IP addresses
		Protocol and port numbers
Reason	This field states the reason for the log; i.e., was the rule matched, not matched or was there an attack. The set and rule coordinates (<X, Y> where X=1,2; Y=00~10) follow with a simple explanation. There are two policy sets; set 1 (X = 1) is for LAN to WAN rules and set 2 (X = 2) for WAN to LAN rules. Y represents the rule in the set. You can configure up to 10 rules in any set (Y = 01 to 10). Rule number 00 is the default rule.  This is a log for a DoS attack.	not match  <1,01> dest IP  This means this packet does not match the destination IP address in set 1, rule 1. Other reasons (instead of dest IP) are src IP, dest port, src port and protocol.
		attack  land, ip spoofing, icmp echo, icmp vulnerability, NetBIOS, smtp illegal command, traceroute, teardrop or syn flood
Action	This field displays whether the packet was blocked, forwarded or neither. None means that no action is dictated by this rule.	block, forward  or none
After viewing the firewall log, ENTER "y" to clear the log or "n" to retain it. With either option you will be returned to <b>Menu 21-Filter and Firewall Setup</b> .		

## 14.2 The Big Picture - Filtering, Firewall and NAT

The following figure illustrates the path a packet takes as it passes through the filtering, firewall and NAT processes. An earlier chapter covers NAT; what follows is a brief comparison of the firewall and filtering.

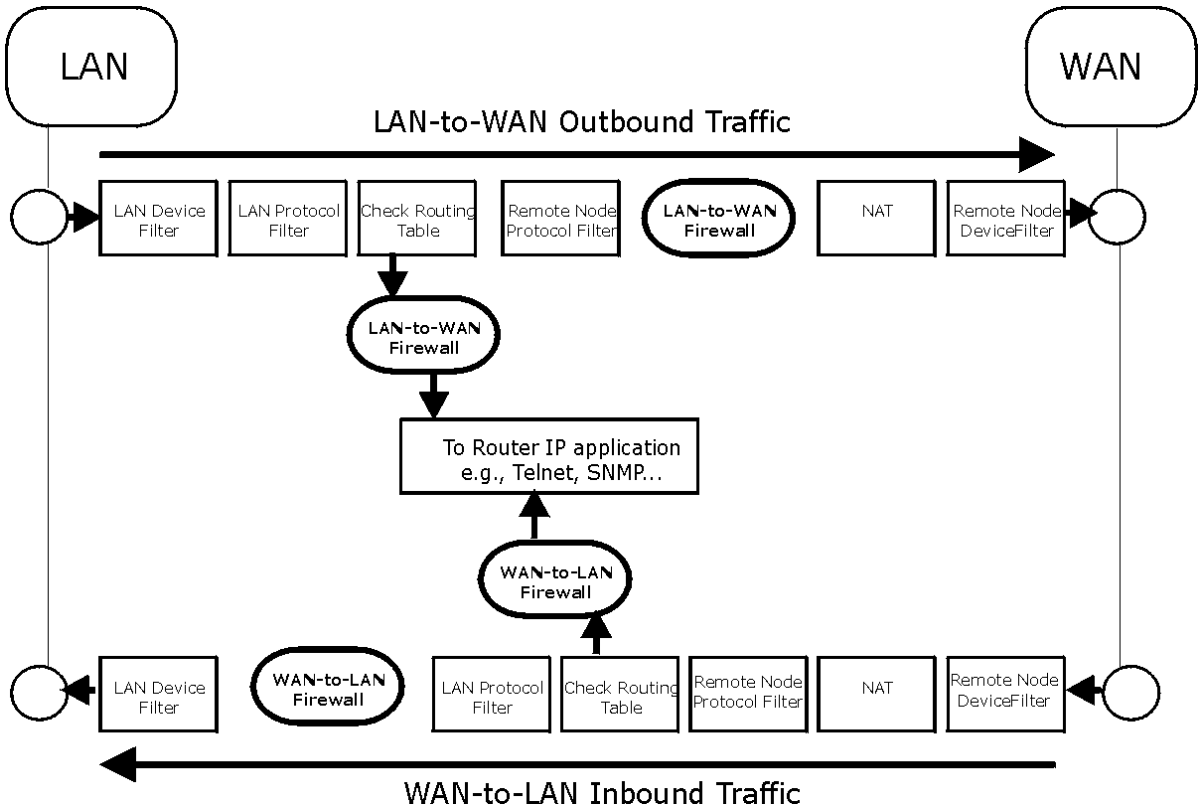


Figure 14-5 Big Picture — Filtering, Firewall and NAT

## 14.3 Packet Filtering Vs Firewall

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

### 14.3.1 Packet Filtering:

- ❑ The router filters packets as they pass through the router's interface according to the filter rules you designed.
- ❑ Packet filtering is a powerful tool, yet can be complex to configure and maintain, especially if you need a chain of rules to filter a service.
- ❑ Packet filtering only checks the header portion of an IP packet.

### **When To Use Filtering**

1. To block/allow LAN packets by their MAC address.
2. To block/allow special IP packets which are neither TCP, UDP, nor ICMP packets.
3. To block/allow both inbound (WAN to LAN) and outbound (LAN to WAN) traffic between the specific inside host/network "A" and outside host/network "B". If the filter blocks the traffic from A to B, it also blocks the traffic from B to A. Filters can not distinguish traffic originating from an inside host or an outside host by IP address.
4. To block/allow IP trace route.

### **14.3.2 Firewall**

- ❑ The firewall inspects packet contents as well as their source and destination addresses. Firewalls of this type employ an inspection module, applicable to all protocols, that understands data in the packet is intended for other layers, from the network layer (IP headers) up to the application layer.
- ❑ The firewall performs stateful inspection. It takes into account the state of connections it handles so that, for example, a legitimate incoming packet can be matched with the outbound request for that packet and allowed in. Conversely, an incoming packet masquerading as a response to a nonexistent outbound request can be blocked.
- ❑ The firewall uses session filtering, i.e., smart rules, that enhance the filtering process and control the network session rather than control individual packets in a session.
- ❑ The firewall provides e-mail service to notify you of routine reports and when alerts occur.

### **When To Use The Firewall**

1. To prevent DoS attacks and prevent hackers cracking your network.
2. A range of source and destination IP addresses as well as port numbers can be specified within one firewall rule making the firewall a better choice when complex rules are required.
3. To selectively block/allow inbound or outbound traffic between inside host/networks and outside host/networks. Remember that filters can not distinguish traffic originating from an inside host or an outside host by IP address.
4. The firewall performs better than filtering if you need to check many rules.
5. Use the firewall if you need routine e-mail reports about your system or need to be alerted when attacks occur.
6. The firewall can block specific URL traffic that might occur in the future. The URL can be saved in an Access Control List (ACL) database.





# Chapter 15

## Introducing the ZyWALL Web Configurator

*This chapter shows you how to configure your firewall with the Web Configurator.*

### 15.1 Web Configurator Login and Welcome Screens

Launch your web browser and enter 192.168.1.1 as the URL. This is the factory default IP address of the ZyWALL when shipped. You will see the following **Login** screen.



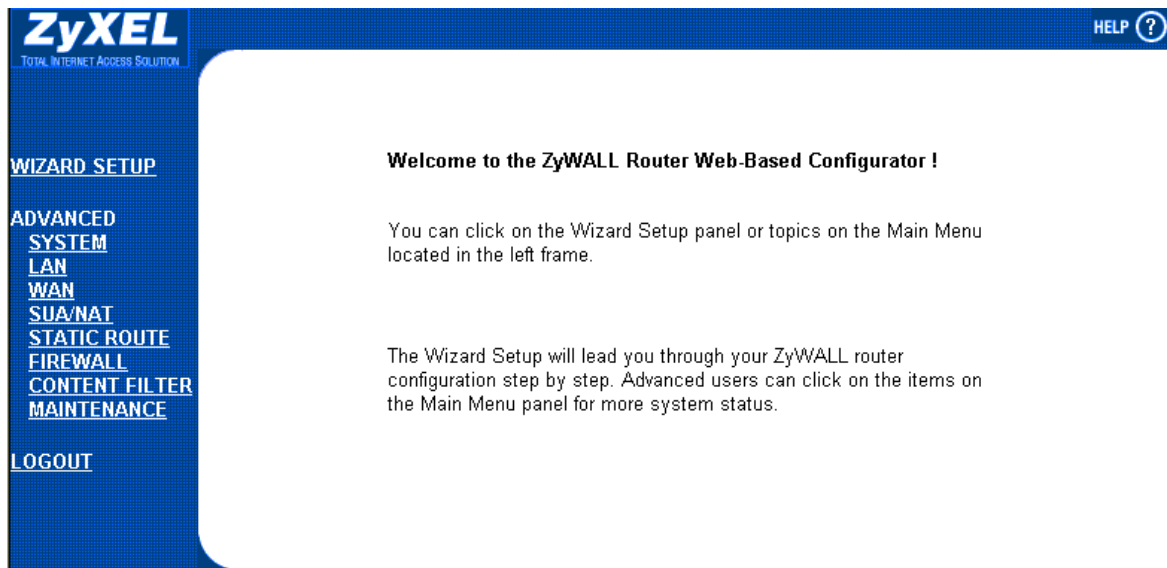
**Figure 15-1 Login screen as seen in Netscape**

1. The default Username and Password is "admin" and "1234" respectively.
2. The Password is configurable, but the Username is not.
3. The Password is case sensitive.
4. The Web Configurator times out after five minutes of inactivity. The time out is not configurable.
5. Please make sure that your web browser is Java and JavaScript enabled.

You can **ONLY** configure the firewall via ZyWALL Web Configurator or CLI command. You will not be able to access the ZyWALL Web Configurator from the WAN if:

1. The firewall is activated, as the firewall by default, blocks all WAN to LAN traffic. To access the ZyWALL Web Configurator from the WAN when the firewall is activated, you will need to create a firewall rule (see the *Example Firewall Rules* chapter ahead) to allow web traffic initiated from the WAN.
2. You have applied a filter in menu 3.1 (LAN) or in menu 11.5 (WAN) to block Web service.
3. You have an SMT console session running.

After a successful login, you will see the **Welcome** screen shown next.



**Figure 15-2 ZyWALL Web Configurator Welcome Screen**

## 15.2 Enabling the Firewall

Click **Firewall**, then **Configuration**, then the **Rule Config** tab to enable the firewall as seen in the following screen.

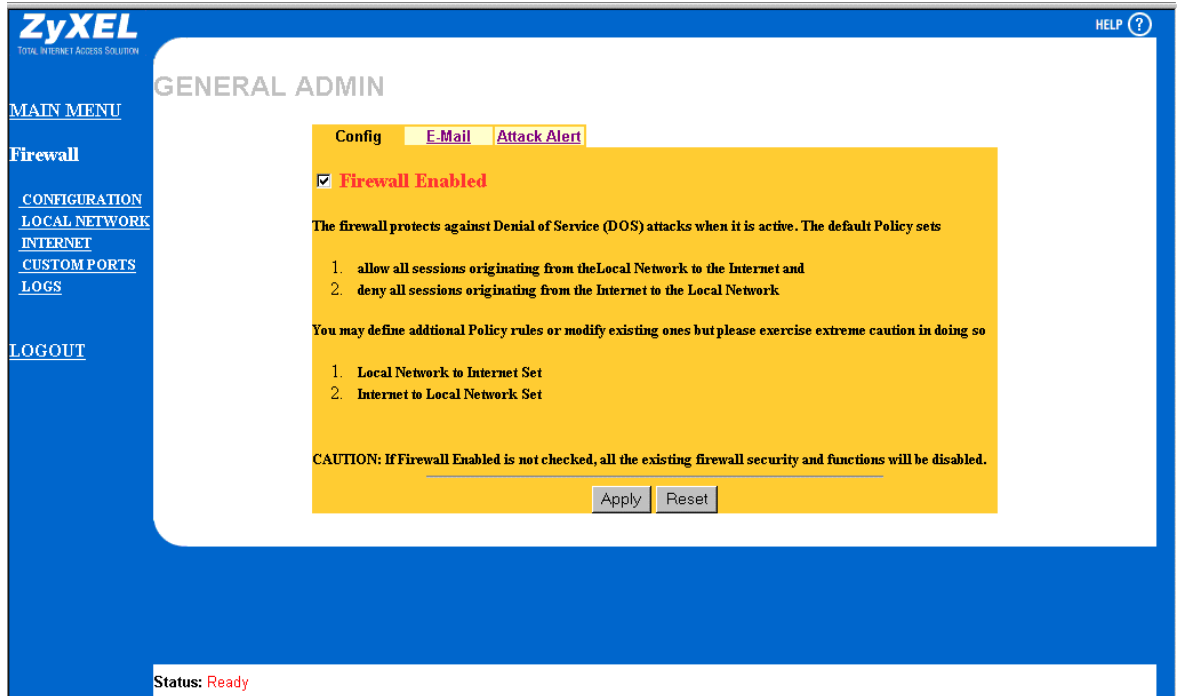


Figure 15-3 Enabling the Firewall

## 15.3 E-mail

This screen allows you to specify your mail server, where e-mail alerts should be sent as well as when and how often they should be sent.

### 15.3.1 What are Alerts?

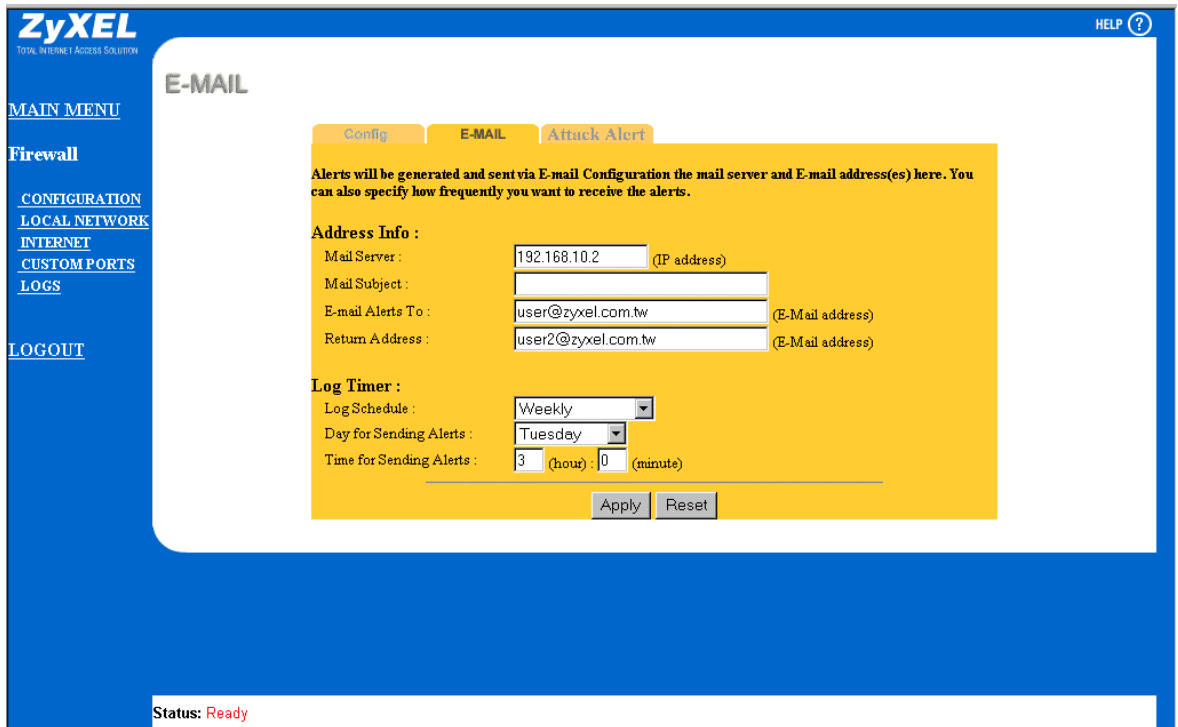
Alerts are reports on events such as attacks, which you may want to know about right away. You can choose to generate an alert when an attack is detected in the **Attack Alert** screen (*Figure 15-6* - check the **Generate an alert when attack detected** checkbox) or when a rule is matched in the creating/editing a firewall rule screen (see *Figure 16-4*). When an event generates a report (an alert), a message is immediately sent to an e-

mail account. Enter the complete e-mail address to which alert messages will be sent in the **E-mail Alerts To** field and schedule times for sending alerts in the **Alert Timer** fields in the **E-mail** screen (following screen).

### 15.3.2 What are Logs?

A log is a detailed record that you create for packets that either match a rule, don't match a rule or both when you are creating/editing a firewall rule (see *Figure 16-4*). You can also choose not to create a log for a rule in this screen. An attack automatically generates a log.

Click **Firewall** then **Configuration**, then the **E-mail** tab to bring up the following screen.



**Figure 15-4 E-mail Screen**

The following table describes the fields in this screen.

Table 15-1 E-mail

FIELD	DESCRIPTION	OPTIONS
<p>Address Information</p> <p>Mail Server</p> <p>Mail Subject</p> <p>E-mail Alerts To</p> <p>Return address</p>	<p>Enter the IP address of your mail server in dotted decimal format. Your Internet Service Provider (ISP) should be able to provide this information. If this field is left blank, log and alert messages will not be sent via e-mail.</p> <p>Enter a subject that you want to appear in the subject field of your e-mail here (see <i>Figure 15-5</i>). If you leave this field blank then the default "Firewall Alert From ZyWALL" displays as your e-mail subject.</p> <p>Enter the e-mail address (username@mydomain.com) of whoever is responsible for maintaining the firewall, e.g., your system administrator. If this field is left blank, alert messages will not be sent via E-mail.</p> <p>Enter an e-mail address to identify the ZyWALL as the sender of the e-mail messages i.e., a "return-to-sender" address for backup purposes.</p>	
<p>Log Timer</p> <p>Alert Schedule</p> <p>Day for Sending Alerts</p> <p>Time for Sending Alerts</p>	<p>This pop-up menu is used to configure the frequency of log messages being sent as e-mail: daily, weekly, hourly, only when the log is full or none. If the <b>Weekly</b> or the <b>Daily</b> option is selected, specify a time of day when the e-mail should be sent. If the <b>Weekly</b> option is selected, then also specify which day of the week the e-mail should be sent. If the <b>When Log is Full</b> option is selected, an alert is sent when the log fills up. If you select <b>None</b>, no log messages are e-mailed.</p> <p>Click which day of the week you want to send the alert from the drop down list box.</p> <p>Click the up or down arrows to the right of the list box to choose a time to send the alerts.</p>	<p><b>When Log is Full</b></p> <p><b>Hourly</b></p> <p><b>Daily</b></p> <p><b>Weekly</b></p> <p><b>None</b></p> <p><b>Sunday through Saturday</b></p>
<p>When you have finished, click <b>Apply</b> to save your customized settings and exit this screen, <b>Cancel</b> to exit this screen without saving, or <b>Help</b> for online HTML help on fields in this screen.</p>		

### 15.3.3 SMTP Error Messages

If there are difficulties in sending e-mail the following error messages appear. Please see the Support Notes on the included disk for information on other types of error messages.

E-mail error messages appear in menu 24.3.1 as "SMTP action request failed. ret= ??". "??" is described in the following table.

**Table 15-2 SMTP Error Messages**

-1 means ZyWALL out of socket
-2 means tcp SYN fail
-3 means smtp server OK fail
-4 means HELO fail
-5 means MAIL FROM fail
-6 means RCPT TO fail
-7 means DATA fail
-8 means mail data send fail

### 15.3.4 Example E-mail Log

An "End of Log" message displays for each mail in which a complete log has been sent. The following is an example of a log sent by e-mail.

The screenshot shows an email log with several callouts:

- Subject:** Firewall Alert From ZyWALL (circled)
- Date:** Fri, 07 Apr 2000 10:05:42 (circled)
- From:** user@zyxel.com
- To:** user@zyxel.com
- Log Entries:**
  - 1|Apr 7 00|From:192.168.1.1 To:192.168.1.255 |default permit
  - |forward
  - |09:54:03|UDP src port:00520 dest port:00520 |<1,00>|
  - 2|Apr 7 00|From:192.168.1.131 To:192.168.1.255 |default permit
  - |forward
  - |09:54:17|UDP src port:00520 dest port:00520 |<1,00>|
  - 3|Apr 7 00|From:192.168.1.6 To:10.10.10.10 |match |forward
  - |09:54:19|UDP src port:03516 dest port:00053 |<1,01>|
  - .....{snip}.....
  - .....{snip}.....
  - 126|Apr 7 00|From:192.168.1.1 To:192.168.1.255 |match
  - |forward
  - |10:05:00|UDP src port:00520 dest port:00520 |<1,02>|
  - 127|Apr 7 00|From:192.168.1.131 To:192.168.1.255 |match
  - |forward
  - |10:05:17|UDP src port:00520 dest port:00520 |<1,02>|
  - 128|Apr 7 00|From:192.168.1.1 To:192.168.1.255 |match
  - |forward
  - |10:05:30|UDP src port:00520 dest port:00520 |<1,02>|
- End of Firewall Log** (circled)

Callout boxes provide additional information:

- "The date format here is Day-Month-Year." (points to the date field)
- "You may edit the subject title" (points to the subject field)
- "The date format here is Month-Day-Year. The time format is Hour-Minute-Second." (points to the log entry date and time)
- "End of Log" message shows that a complete log has been sent." (points to the "End of Firewall Log" text)

Figure 15-5 E-mail Log

## 15.4 Attack Alert

The first defense against DOS attacks. In this screen you may choose to generate an alert whenever an attack is detected. For DoS attacks, the ZyWALL uses thresholds to determine when to drop sessions that do not become fully established. These thresholds apply globally to all sessions.

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

### 15.4.1 Threshold Values:

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

1. The maximum number of opened sessions.
2. The minimum capacity of server backlog in your LAN network.
3. The CPU power of servers in your LAN network.
4. Network bandwidth.



5. Type of traffic for certain servers.

If your network is slower than average for any of these factors (especially if you have servers that are slow or handle many tasks and are often busy), then the default values should be reduced.

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

## 15.4.2 Half-Open Sessions

An unusually high number of half-open sessions (either an absolute number or measured as the arrival rate) could indicate that a Denial of Service attack is occurring. For TCP, "half-open" means that the session has not reached the established state-the TCP three-way handshake has not yet been completed (see *Figure 13-2*). For UDP, "half-open" means that the firewall has detected no return traffic.

The ZyWALL measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are counted in the total number and rate measurements. Measurements are made once a minute.

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

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

### TCP Maximum Incomplete and Blocking Time

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

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

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

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

**ZyXEL**  
TOTAL INTERNET ACCESS SOLUTION

HELP ?

**ATTACK ALERT**

Config E-Mail **ATTACK ALERT**

The firewall is set by default to prevent attacks on your network. Any detected attacks will automatically generate a log entry. You can also choose to generate an alert whenever such an attack is detected.

Generate alert when attack detected

**Denial of Service Thresholds :**

One Minute Low : 80

One Minute High : 100

Maximum Incomplete Low : 80

Maximum Incomplete High : 100

TCP Maximum Incomplete : 10

Blocking Time 0 (min)

Apply Reset

Status: Ready

**Figure 15-6 Attack Alert**

The following table describes the fields in this screen.

**Table 15-3 Attack Alert**

FIELD	DESCRIPTION	DEFAULT VALUES
Generate alert when attack detected	A detected attack automatically generates a log entry. Check this box to generate an alert (as well as a log) whenever an attack is detected. See the <i>Logs Chapter</i> for more information on logs and alerts.	
Denial of Service Thresholds		
One Minute Low	This is the rate of new half-open sessions that causes the firewall to stop deleting half-open sessions. The ZyWALL continues to delete half-open sessions as necessary, until the rate of new connection attempts drops below this number.	80 existing half-open sessions.
One Minute High	This is the rate of new half-open sessions that causes the firewall to start deleting half-open sessions. When the rate of new connection attempts rises above this number, the ZyWALL deletes half-open sessions as required to accommodate new connection attempts.	100 half-open sessions per minute. The above numbers cause the ZyWALL to start deleting half-open sessions when more than 100 session establishment attempts have been detected in the last minute, and to stop deleting half-open sessions when fewer than 80 session establishment attempts have been detected in the last minute.
Maximum Incomplete Low	This is the number of existing half-open sessions that causes the firewall to stop deleting half-open sessions. The ZyWALL continues to delete half-open requests as necessary, until the number of existing half-open sessions drops below this number.	80 existing half-open sessions.
Maximum Incomplete High	This is the number of existing half-open sessions that causes the firewall to start deleting half-open sessions. When the number of existing half-open sessions	100 half-open sessions per minute. The above values causes the ZyWALL to start deleting

FIELD	DESCRIPTION	DEFAULT VALUES
	rises above this number, the ZyWALL deletes half-open sessions as required to accommodate new connection requests. Do not set <b>Maximum Incomplete High</b> to lower than the current <b>Maximum Incomplete Low</b> number.	half-open sessions when the number of existing half-open sessions rises above 100, and to stop deleting half-open sessions with the number of existing half-open sessions drops below 80.
TCP Maximum Incomplete	This is the number of existing half-open TCP sessions with the same destination host IP address that causes the firewall to start dropping half-open sessions to that same destination host IP address. Enter a number between 1 and 250. As a general rule, you should choose a smaller number for a smaller network, a slower system or limited bandwidth.	10 existing half-open TCP sessions.
Blocking Time	When <b>TCP Maximum Incomplete</b> is reached you can choose if the next session should be allowed or blocked. If you check <b>Blocking Time</b> any new sessions will be blocked for the length of time you specify in the next field (min) and all old incomplete sessions will be cleared during this period. If you want strong security, it is better to block the traffic for a short time, as it will give the server some time to digest the loading.	Check this checkbox to specify a number in minutes (min) text box.
(min)	Enter the length of Blocking Time in minutes.	10
When you have finished, click <b>Apply</b> to save your customized settings and exit this screen, <b>Cancel</b> to exit this screen without saving, or <b>Help</b> for online HTML help on fields in this screen.		



# Chapter 16

## Creating Custom Rules

*This chapter contains instructions for defining both Local Network and Internet rules.*

### 16.1 Rules Overview

Firewall rules are subdivided into “Local Network” and “Internet”. By default, the ZyWALL’s stateful packet inspection allows all communications to the Internet that originate from the local network, and blocks all traffic to the LAN that originates from the Internet. You may define additional rules and sets or modify existing ones but please exercise extreme caution in doing so.

---

**If you try to configure rules but do not have a good understanding of how rules work, you might inadvertently introduce security risks to the firewall and to the protected network. You should be sure you test your rules after you configure them.**

---

For example, you may create rules to:

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

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

### 16.2 Rule Logic Overview

---

**Study these points carefully before beginning to configure rules.**

---

#### 16.2.1 Rule Checklist

1. State the intent of the rule. For example, “This restricts all IRC access from the LAN to the Internet.” Or, “This allows a remote Lotus Notes server to synchronize over the Internet to an inside Notes server.”
2. Is the intent of the rule to forward or block traffic?
3. What is the direction connection: from the LAN to the Internet, or from the Internet to the LAN?
4. What IP services will be affected?

5. What computers on the LAN are to be affected (if any)?
6. What computers on the Internet will be affected? The more specific, the better. For example, if traffic is being allowed from the Internet to the LAN, it is better to allow only certain machines on the Internet to access the LAN.

## 16.2.2 Security Ramifications

Once the logic of the rule has been defined, it is critical to consider the security ramifications created by the rule:

1. Does this rule stop LAN users from accessing critical resources on the Internet? For example, if IRC is blocked, are there users that require this service?
2. Is it possible to modify the rule to be more specific? For example, if IRC is blocked for all users, will a rule that blocks just certain users be more effective?
3. Does a rule that allows Internet users access to resources on the LAN create a security vulnerability? For example, if FTP ports (TCP 20, 21) are allowed from the Internet to the LAN, Internet users may be able to connect to computers with running FTP servers.
4. Does this rule conflict with any existing rules?

Once these questions have been answered, adding rules is simply a matter of plugging the information into the correct fields in the **Rules** screen in the ZyWALL Web Configurator.

## 16.2.3 Key Fields For Configuring Rules

### Action

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

---

“Block” means the firewall silently discards the packet.

---

### Service

Select the service from the **Service** scrolling list box. If the service is not listed, it is necessary to first define it. See *section 16.5* for more information on services.

### Source Address

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

### Destination Address

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

## 16.3 Connection Direction

This section talks about configuring firewall rules for connections going from LAN to WAN and WAN to LAN in your firewall.

### 16.3.1 LAN to WAN Rules

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

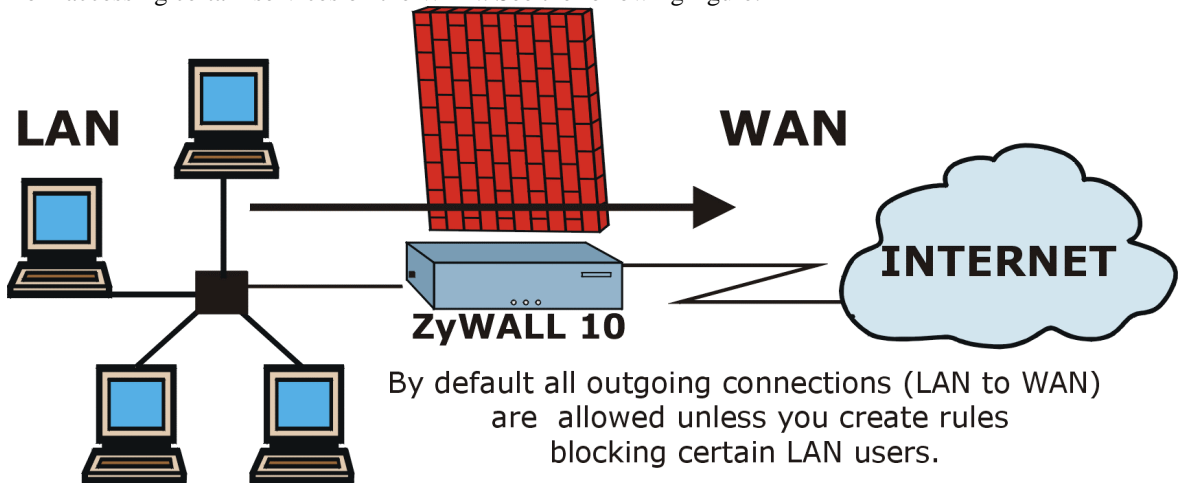


Figure 16-1 LAN to WAN Traffic

### 16.3.2 WAN to LAN Rules

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



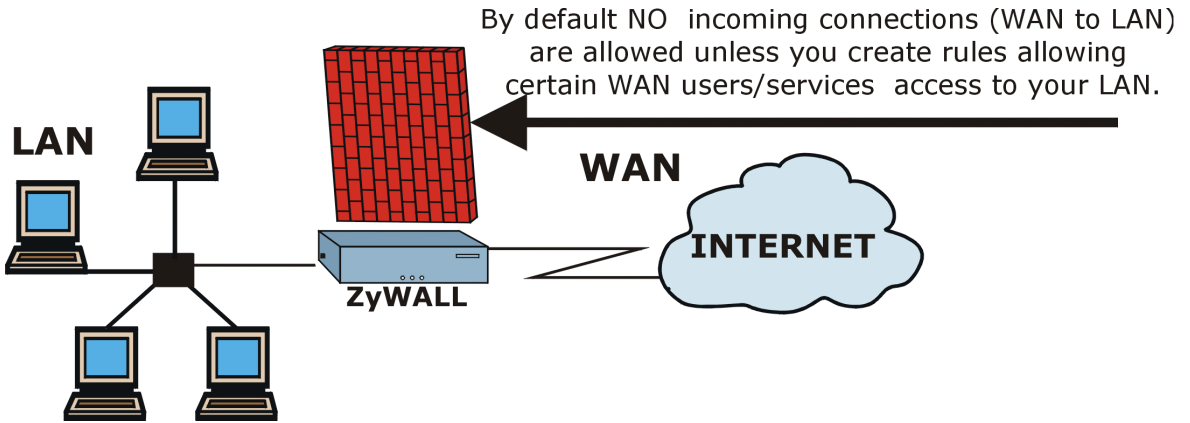


Figure 16-2 WAN to LAN Traffic

## 16.4 Rule Summary

---

The fields in the Rule Summary screens are the same for Local Network and Internet, so the discussion below refers to both.

---

Click on **Firewall**, then **Local Network** to bring up the following screen. This screen is a summary of the existing rules. Note the order in which the rules are listed.

---

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

---

**ZyXEL**  
TOTAL INTERNET ACCESS SOLUTION

LOCAL NETWORK

Local Network to Internet

**RULE SUMMARY** Time Out

**General :**

Name :

The default action for packets not matching following rules :   Default Permit Log

No.	Status	Source IP	Destination IP	Service	Action	Log
1	Configured	192.168.10.2	Any	*POP(TCP:110)	Forward	None
2	Configured	192.168.10.5	Any	HTTP(TCP:80)	Forward	None
3	Empty					
4	Empty					
5	Empty					
6	Empty					
7	Empty					
8	Empty					
9	Empty					
10	Empty					

Move Rule : To Rule Number

Status: Ready

**Figure 16-3 Firewall Rules Summary — First Screen**

The following table describes the fields in this screen.

**Table 16-1 Firewall Rules Summary — First Screen**

FIELD	DESCRIPTION	OPTIONS
<p>General</p> <p style="text-align: right;">Name</p> <p>The default action for packets not matching following rules.</p> <p style="text-align: right;">Default Permit Log</p>	<p>This is the name of the firewall rule set. Type a name to distinguish the LAN-to-WAN filter set from the WAN-to-LAN filter set.</p> <p>Should packets that do not match the following rules be blocked or forwarded? Make your choice from the drop down list box. Note that “block” means the firewall silently discards the packet.</p> <p>Check this box to log all matched rules in the ACL default set.</p>	<p>Name</p> <p><b>Block</b> <b>Forward</b></p>
<p>Firewall Rule Summary</p> <p style="text-align: right;">No</p> <p style="text-align: right;">Source IP</p> <p style="text-align: right;">Destination IP</p> <p style="text-align: right;">Service</p> <p style="text-align: right;">Action</p> <p style="text-align: right;">Log</p>	<p>The following fields summarize the rules you have created. Note that these fields are read only. Click the tab at the top of the box to order the rules according to that tab.</p> <p>This is your firewall rule number. The ordering of your rules is important as rules are applied in turn. The <b>Move</b> field below allows you to reorder your rules.</p> <p>This is the source address of the packet.</p> <p>This is the destination address of the packet.</p> <p>This is the service to which the rule applies. See <i>Table 16-2</i> for more information.</p> <p>This is the specified action for that rule. Note that <b>Block</b> means the firewall silently discards the packet.</p> <p>This field shows you if a log is created for packets that match the rule, don't match the rule, both or no log is created.</p>	<p><b>Block</b> <b>Forward</b> <b>Match</b> <b>Not Match</b> <b>Both</b> <b>None</b></p>
<p>Move Rule</p> <p style="text-align: right;">To Rule Number</p> <p style="text-align: right;">Move</p>	<p>You may reorder your rules using this function. Select by clicking on the rule you want to move. The ordering of your rules is important as rules are applied in turn.</p> <p>In this box, type the number you want to move the rule to.</p> <p>Click this command button to move the rule.</p>	

FIELD	DESCRIPTION	OPTIONS
Click <b>Apply</b> to create a new firewall rule. New firewall rules are added at the end after existing firewall rules. Click <b>Edit</b> to edit an existing filter rule. See <i>section 16.5</i> for more details. Click <b>Delete</b> to delete an existing firewall rule. Note that subsequent firewall rules move up by one when you take this action. Click <b>Help</b> for online HTML help on fields in this screen		

## 16.5 Predefined Services

The **Available Services** list box in the **Rule Config(uration)** screen (see *Figure 16-4*) displays all predefined services that the ZyWALL already supports. Next to the name of the service, two fields appear in brackets. The first field indicates the IP protocol type (TCP, UDP, or ICMP). The second field indicates the IP port number that defines the service. (Note that there may be more than one IP protocol type. For example, look at the default configuration labeled “(DNS)”. **(UDP/TCP:53)** means UDP port 53 and TCP port 53. Up to 128 entries are supported. Custom services may also be configured using the **Custom Ports** function discussed later.

**Table 16-2 Predefined Services**

SERVICE	DESCRIPTION
BGP(TCP:179)	Border Gateway Protocol.
BOOTP_CLIENT(UDP:68)	DHCP Client.
BOOTP_SERVER(UDP:67)	DHCP Server.
CU-SEEME(TCP/UDP:7648, 24032)	A popular videoconferencing solution from White Pines Software.
DNS(UDP/TCP:53)	Domain Name Server, a service that matches web names (e.g. <a href="http://www.zyxel.com">www.zyxel.com</a> ) to IP numbers.
FINGER(TCP:79)	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP(TCP:20.21)	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
HTTP(TCP:80)	Hyper Text Transfer Protocol - a client/server protocol for the world wide web
HTTPS	HTTPS is a secured http session often used in e-commerce.
ICMP	ICMP service allows normal ICMP packets to go through.
ICQ(UDP:4000)	This is a popular Internet chat program.
IRC(TCP/UDP:6667)	This is another popular Internet chat program.
NEWS(TCP:144)	A protocol for news groups.
NFS(UDP:2049)	Network File System - NFS is a client/server distributed file service that provides transparent file-sharing for network environments.
NNTP(TCP:119)	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
RCMD(TCP:512)	Remote Command Service.
REAL_AUDIO(TCP:7070)	A streaming audio service that enables real time sound over the web.
REXEC(TCP:514)	Remote Execution Daemon.
RLOGIN(TCP:513)	Remote Login.
RTELNET(TCP:107)	Remote Telnet.
RTSP(TCP/UDP:554)	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.

SERVICE	DESCRIPTION
SFTP(TCP:115)	Simple File Transfer Protocol.
SMTP(TCP:25)	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP(TCP/UDP:161)	Simple Network Management Program.
SNMP-TRAPS(TCP/UDP:162)	Traps for use with the SNMP(RFC:1215).
SQL-NET(TCP:1521)	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH(TCP/UDP:22)	Secure Shell Remote Login Program.
STRM WORKS(UDP:1558)	Stream Works Protocol.
TACACS(UDP:49)	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET(TCP:23)	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP(UDP:69)	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE(TCP:7000)	Another videoconferencing solution.

### 16.5.1 Creating/Editing Firewall Rules

To create a new rule, click a number (No.) then click **Edit** in the last screen shown to display the following screen.

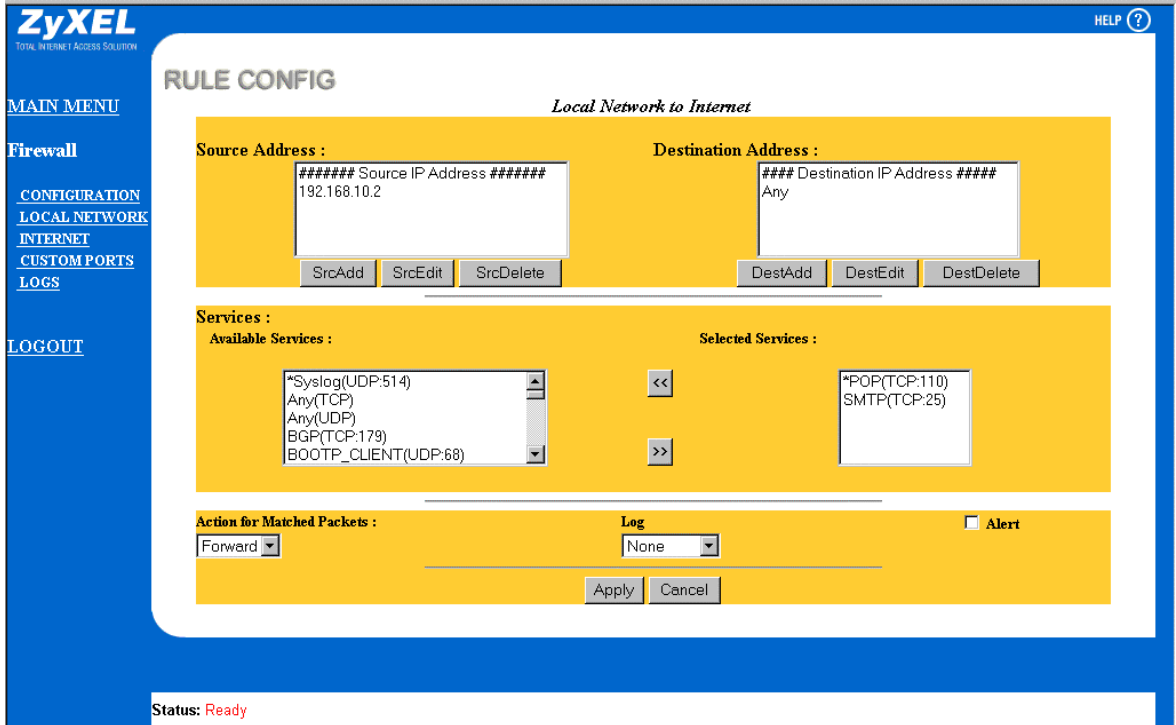


Figure 16-4 Creating/Editing A Firewall Rule

Table 16-3 Creating/Editing A Firewall Rule

FIELD	DESCRIPTION	OPTIONS
Source Address	Press <b>SrcAdd</b> to add a new address, <b>SrcEdit</b> to edit an existing one or <b>SrcDelete</b> to delete one. Please see the next section for more information on adding and editing source addresses.	<b>SrcAdd</b> <b>SrcEdit</b> <b>SrcDelete</b>
Destination Address	Press <b>DestAdd</b> to add a new address, <b>DestEdit</b> to edit an existing one or <b>DestDelete</b> to delete one. Please see the next information on adding and editing destination addresses.	<b>DestAdd</b> <b>DestEdit</b> <b>DestDelete</b>
Services Available/Selected	Please see <i>Table 16-2</i> for more information on services available. Highlight a service from the <b>Available Services</b> box on the left, then press <b>&gt;&gt;</b> to add it to the <b>Selected Services</b> box on the right. To remove a service, highlight it in the <b>Selected Services</b> box on the right, then press <b>&lt;&lt;</b> .	<b>&gt;&gt;</b> <b>&lt;&lt;</b>
Action for Matched Packets	Should packets that match this rule be blocked or forwarded? Make your choice from the drop down list box. Note that <b>Block</b> means the firewall silently discards the packet.	<b>Block</b> <b>Forward</b>
Log	This field determines if a log is created for packets that match the rule, don't match the rule, both or no log is created.	<b>Match</b> <b>Not Match</b> <b>Both</b> <b>None</b>
Alert	Check the <b>Alert</b> check box to determine that this rule generates an alert when the rule is matched.	
When you have finished, click <b>Apply</b> to save your customized settings and exit this screen, <b>Cancel</b> to exit this screen without saving, or <b>Help</b> for online HTML help on fields in this screen.		



## 16.5.2 Source and Destination Addresses

To add a new source or destination address, click **SrcAdd** or **DestAdd** from the screen above. To edit an existing source or destination address, select it from the box and click **SrcEdit** or **DestEdit** from the screen above. Either action displays the following screen.

The screenshot displays the ZyXEL web interface for configuring IP rules. The main content area is titled "RULE IP CONFIG" and shows a configuration window for "Local Network to Internet". The window has a yellow background and contains the following fields:

- Address Type :** A dropdown menu set to "Single Address".
- Start IP Address :** A text input field containing "192.168.10.2".
- End IP Address :** A text input field containing "0.0.0.0".
- Subnet Mask :** A text input field containing "0.0.0.0".

At the bottom of the configuration window are "Apply" and "Cancel" buttons. The status bar at the bottom of the page shows "Status: Ready".

Figure 16-5 Adding/Editing Source and Destination Addresses

**Table 16-4 Adding/Editing Source and Destination Addresses**

FIELD	DESCRIPTION	OPTIONS
Address Type	Do you want your rule to apply to packets with a particular (single) IP address, a range of IP addresses (e.g., 192.168.1.10 to 192.169.1.50), a subnet or any IP address? Select an option from the drop down list box	<b>Single Address</b> <b>Range Address</b> <b>Subnet Address</b> <b>Any Address</b>
Start IP Address	Enter the single IP address or the starting IP address in a range here.	
End IP Address	Enter the ending IP address in a range here.	
Subnet Mask	Enter the Subnet Mask here, if applicable.	
When you have finished, click <b>Apply</b> to save your customized settings and exit this screen, <b>Cancel</b> to exit this screen without saving, or <b>Help</b> for online HTML help on fields in this screen.		

## 16.6 Timeout

The fields in the Timeout screens are the same for Local and Internet networks, so the discussion below refers to both.

### 16.6.1 Factors Influencing Choices for Timeout Values

The factors influencing choices for timeout values are the same as the factors influencing choices for threshold values – see *section 15.4.1*. Click on either **Local Network** or **Internet**, then select the **Timeout** tab.

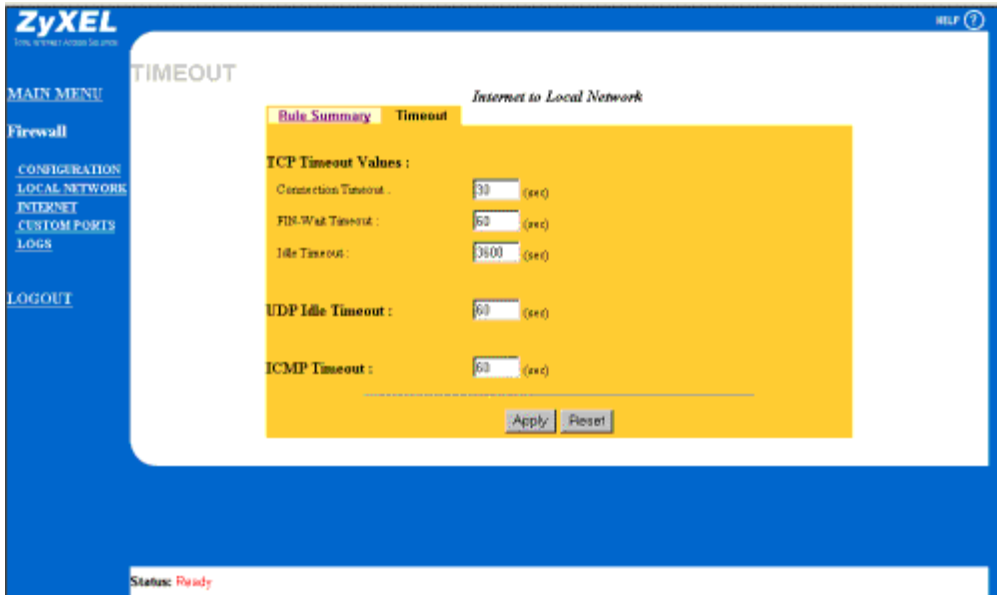


Figure 16-6 Timeout Screen

**Table 16-5 Timeout Menu**

FIELD	DESCRIPTION	DEFAULT VALUE
TCP Timeout Values Connection Timeout  FIN-Wait Timeout  Idle Timeout	This is the length of time the ZyWALL waits for a TCP session to reach the established state before dropping the session.  This is the length of time a TCP session remains open after the firewall detects a FIN-exchange (indicating the end of the TCP session).  This is the length of time of inactivity a TCP connection remains open before the ZyWALL considers the connection closed.	30 seconds  60 seconds  3600 seconds (1 hour)
UDP Idle Timeout	This is the length of time of inactivity a UDP connection remains open before the ZyWALL considers the connection closed.	60 seconds
ICMP Timeout	This is the length of time an ICMP session waits for the ICMP response.	60 seconds
When you have finished, click on <b>Apply</b> to apply your changes or <b>Reset</b> to go back to the original settings. Click <b>Help</b> for online HTML help on fields in this screen.		



# Chapter 17

## Custom Ports

*This chapter covers creating, viewing and editing custom ports.*

### 17.1 Introduction

Configure customized ports for services not predefined by the ZyWALL (see *Figure 16-4*). For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) website. For further information on these services, please read *section 16.5*. To configure a custom port, click **Custom Ports** to bring up the following screen.

The screenshot shows the ZyWALL 10 Internet Security Gateway interface. The top left features the ZyXEL logo and the tagline 'TOTAL INTERNET ACCESS SOLUTION'. The top right has a 'HELP ?' icon. A blue sidebar on the left contains a 'MAIN MENU' with links for 'Firewall', 'CONFIGURATION', 'LOCAL NETWORK', 'INTERNET', 'CUSTOM PORTS', 'LOGS', and 'LOGOUT'. The main content area is titled 'CUSTOM PORTS' and contains a table of 'Customized Services'. The table has five columns: 'No.', 'Status', 'Name', 'Protocol', and 'Port'. The first two rows are filled with data: row 1 has '1.', 'configured', 'POP', 'TCP', and '110'; row 2 has '2.', 'configured', 'Syslog', 'UDP', and '514'. Rows 3 through 10 are empty, with 'Status' set to 'empty'. Below the table are 'Edit' and 'Delete' buttons. At the bottom left of the screen, a status bar indicates 'Status: Ready'.

No.	Status	Name	Protocol	Port
1.	configured	POP	TCP	110
2.	configured	Syslog	UDP	514
3.	empty			
4.	empty			
5.	empty			
6.	empty			
7.	empty			
8.	empty			
9.	empty			
10.	empty			

**Figure 17-1 Custom Ports**

The next table describes the fields in this screen.

**Table 17-1 Custom Ports**

FIELD	DESCRIPTION
Customized Services	
No.	This is the number of your customized port.
Status	Indicates whether ports have already been configured or are still empty.
Name	This is the name of your customized port.
Protocol	This shows the IP protocol (TCP, UDP or Both) that defines your customized port.
Port	This is the port number or range that defines your customized port.
Add a New Entry	Click this button to create a new service (custom port).
Click a custom port number option box (No.) and then click <b>Edit</b> to edit an existing service (custom port) or <b>Delete</b> to delete that service (custom port). Click <b>Help</b> for online HTML help on fields in this screen. When you have finished viewing this screen, click another link to exit.	

## 17.2 Creating/Editing A Custom Port

Click **Edit** to create a new custom port or edit an existing one. This displays the following screen.

**ZyXEL**  
TOTAL INTERNET ACCESS SOLUTION

HELP ?

### PORT CONFIG

Service Name :

Service Type :

Port Configuration :

Type :  Single  Range

Port Number :  -

Status: Ready

**Figure 17-2 Creating/Editing A Custom Port**

The next table describes the fields in this screen.



**Table 17-2 Creating/Editing A Custom Port**

FIELD	DESCRIPTION	OPTIONS
Service Name	Enter a unique name for your custom port.	
Service Type	Choose the IP port ( <b>TCP</b> , <b>UDP</b> or <b>Both</b> ) that defines your customized port from the drop down list box.	<b>TCP</b> <b>UDP</b> <b>Both</b>
Port Configuration Type  Port Number	Click the <b>Single</b> button to specify one port only or <b>Range radio</b> button to specify a span of ports that define your customized service.  Enter a single port number or the range of port numbers that define your customized service.	<b>Single</b> <b>Range</b>
When you have finished, click <b>Apply</b> to save your customized settings and exit this screen, <b>Cancel</b> to exit this screen without saving, or <b>Help</b> for online HTML help on fields in this screen.		

# Chapter 18

## Logs

This chapter contains information about using the log screen to view the results of the rules you have configured.

### 18.1 Log Screen

When you configure a new rule you also have the option to log events that match, don't match (or both) this rule (see *Figure 16-4*). Click on the **Logs** to bring up the next screen. Firewall logs may also be viewed in SMT Menu 21.3 (see *section 14.1.1*) or via syslog (SMT Menu 24.3.2 - System Maintenance - UNIX Syslog). Syslog is an industry standard protocol used for capturing log information for devices on a network. 128 entries are available numbered from 0 to 127. Once they are all used, the log wraps around and the old logs are lost.

The screenshot shows the ZyXEL ZyWALL 10 Internet Security Gateway interface. The main menu on the left includes: MAIN MENU, Firewall, CONFIGURATION, LOCAL NETWORK, INTERNET, CUSTOM PORTS, LOGS, and LOGOUT. The LOGS screen displays a table titled "Firewall Log (Page 3/4)".

No	Time	Packet Information	Reason	Action
120	Jan 1 0	From:192.168.1.33 To:192.168.1.1	[default permit	forward
	00:12:37	TCP src port:01051 dest port:00000	<1,00>	
121	Jan 1 0	From:192.168.1.33 To:224.0.1.22	[default permit	forward
	00:13:04	IGMP src port:00000 dest port:00000	<1,00>	
122	Jan 1 0	From:192.168.1.33 To:224.0.1.22	[default permit	forward
	00:15:16	IGMP src port:00000 dest port:00000	<1,00>	
123	Jan 1 0	From:192.168.1.33 To:192.168.1.1	[default permit	forward
	00:16:12	TCP src port:01052 dest port:00000	<1,00>	
124	Jan 1 0	From:192.168.1.33 To:192.168.1.1	[default permit	forward
	00:16:12	TCP src port:01053 dest port:00000	<1,00>	
125	Jan 1 0	From:192.168.1.33 To:192.168.1.255	[default permit	forward
	00:16:51	UDP src port:00138 dest port:00138	<1,00>	
126	Jan 1 0	From:192.168.1.33 To:224.0.1.22	[default permit	forward
	00:17:19	IGMP src port:00000 dest port:00000	<1,00>	

Navigation buttons: Previous Page, Refresh, Clear, Next Page

Status: Ready

Figure 18-1 Log Screen

**Table 18-1 Log Screen**

FIELD	DESCRIPTION	EXAMPLES
No.	This is the index number of the firewall log. 128 entries are available numbered from 0 to 127. Once they are all used, the log will wrap around and the old logs will be lost.	
Time	This is the time the log was recorded in this format. You must configure menu 24.10 for real-time; otherwise the time shown in these examples is displayed.	dd:mm:yy e.g., Jan 1 0
		hh:mm:ss e.g., 00:00:00
Packet Information	This field lists packet information such as:	From and To IP addresses ----- protocol and port numbers.
Reason	<p>This field states the reason for the log; i.e., was the rule matched, not matched, or was there an attack. The set and rule coordinates (&lt;X, Y&gt; where X=1,2; Y=00~10) follow with a simple explanation. There are two policy sets; set 1 (X = 1) is for LAN to WAN rules and set 2 (X = 2) for WAN to LAN rules. Y represents the rule in the set. You can configure up to 10 rules in any set (Y = 01 to 10). Rule number 00 is the default rule.</p> <p>This is a log is for a DoS attack</p>	<p>not match</p> <p>&lt;1,01&gt; dest IP</p> <p>This means this packet does not match the destination IP address in set 1, rule 1. Other reasons (instead of dest IP) are src IP, dest port, src port and protocol.</p> <p>attack</p> <p>land, ip spoofing, icmp echo, icmp vulnerability, NetBIOS, smtp illegal command, traceroute, teardrop, or syn flood.</p> <p>Section 14.1.2 and Chapter 13 have more detailed discussion of what these attacks mean.</p>
Action	This field displays whether the packet was blocked (i.e., silently discarded), forwarded or neither (Block, Forward or None). "None" means that no action is dictated by this rule.	Block, Forward  or None
<p>Click <b>Previous Page</b> or <b>Next Page</b> to view other pages in your log. Click <b>Refresh</b> to renew the log screen or <b>Clear</b> to clear all the logs. Click <b>Help</b> for online HTML help on fields in this screen. When you have finished viewing this screen, click another link to exit.</p>		

# Chapter 19

## Example Firewall Rules

*This chapter gives examples for configuring various rules for WAN to LAN and LAN to WAN.*

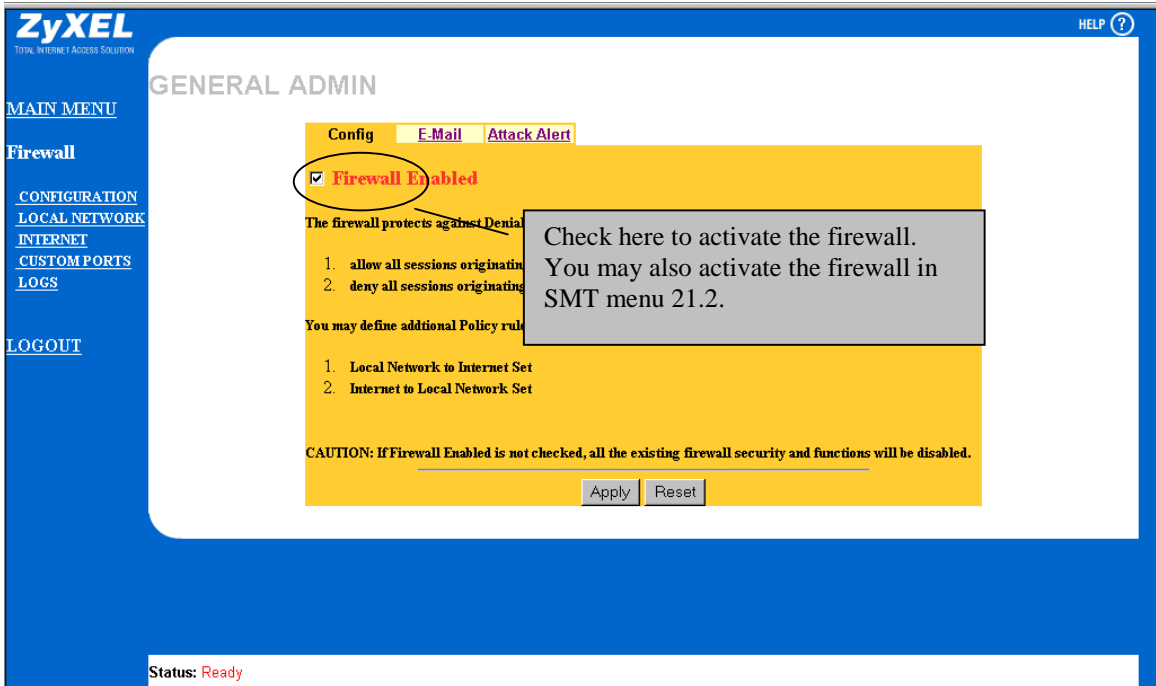
### 19.1 Examples

Whenever you open a hole in the firewall to forward a service from the Internet to the local network, and NAT is also enabled, you may have to also configure a server behind NAT using SMT menu 15.2. Please see the *NAT chapter* for more detailed information and also see *Figure 14-5* for a view of how filtering, the firewall and NAT interact.

#### 19.1.1 Example 1: Firewall Rule To Allow Web Service From The Internet

Let's say you have one server on the local network, with an IP of 10.100.1.2, supporting FTP, HTTP, Telnet and mail services. The only traffic allowed from the Internet is web service. You want to be able to forward all traffic initiated from the local network. You want to know who accesses your server and send e-mail alerts when this happens. Assume, for example, your mail account is [user@zyxel.com](mailto:user@zyxel.com). Another network administrator has an e-mail address of [user2@zyxel.com](mailto:user2@zyxel.com). Here are the steps you would follow.

**Step 1.** Activate the firewall. You may activate the firewall through the ZyWALL Web Configurator as shown next (click **Configuration**, the **Config** tab, then check the **Firewall Enabled** box) or through SMT menu 21.2. You can only configure the firewall using the ZyWALL Web Configurator or CI commands (see *Appendices*). When the firewall is active, the default rules allow all traffic from the local network to the WAN (Internet) and block all traffic from the Internet to the local network.



**Figure 19-1 Activate The Firewall**

**Step 2.** Configure your **E-mail** screen as follows. Click the **E-mail** tab to bring up the next screen.

**ZyXEL**  
TOTAL INTERNET ACCESS SOLUTION

HELP ?

**E-MAIL**

Config E-MAIL Attack Alert

Alerts will be generated and sent via E-mail Configuration it can also specify how frequently you want to receive the alert

**Address Info :**

Mail Server :  (IP address)

Mail Subject :

E-mail Alerts To :  (E-Mail address)

Return Address :  (E-Mail address)

**Log Timer :**

Log Schedule :

Day for Sending Alerts :

Time for Sending Alerts :  (hour)  (minute)

Status: Ready

**Figure 19-2 Example 1: E-mail Screen**

**Step 3.** Configure your firewall rule as shown in the following screen. The default firewall blocks all Internet traffic entering our local network, but you want to create a hole for web service from the Internet. Click **Internet** and go to the **Rule Summary**. Configure this screen as shown.

**Internet to Local Network**

**Source Address :** ##### Source IP Address #####  
Any

**Destination Address :** ### Destination IP Ad  
10.100.1.2

**Services :**

**Available Services :**

- \*POP(TCP:110)
- \*Syslog(UDP:514)
- Any(TCP)
- Any(UDP)
- BGP(TCP:179)

**Selected Services :**

- HTTP(TCP:80)

**Action for Matched Packets :**

Log: Match

Alert

Apply Cancel

**Callout 1:** This is an Internet to Local Network rule.

**Callout 2:** Click **DestAdd** to configure the destination address as the IP of the server on the LAN. See the next screen.

**Callout 3:** Select this service (web service) from the **Available Services** list box and click >>.

**Callout 4:** Forward the packet when it matches this rule (remember the default is to block all packets from the Internet), log packets that match this rule and to send alerts when this happens.

**Callout 5:** Click this button when you have finished editing screens.

**Figure 19-3 Example 1: Configuring a Rule**

**Step 4.** Click **DestAdd** to configure the destination address as the IP of your server on the LAN.

The screenshot shows the ZyXEL configuration interface for a firewall rule. The page title is 'RULE IP CONFIG' and the rule name is 'Internet to Local Network'. The 'Address Type' is set to 'Single Address'. The 'Start IP Address' is '10.100.1.2', 'End IP Address' is '0.0.0.0', and 'Subnet Mask' is '0.0.0.0'. A callout box explains that 10.100.1.2 is the IP of a server on the LAN. The status at the bottom is 'Ready'.

**ZyXEL**  
TOTAL INTERNET ACCESS SOLUTION

HELP ?

**MAIN MENU**

**Firewall**

[CONFIGURATION](#)

[LOCAL NETWORK](#)

[INTERNET](#)

[CUSTOM PORTS](#)

[LOGS](#)

[LOGOUT](#)

**RULE IP CONFIG**

*Internet to Local Network*

Address Type :

Start IP Address :

End IP Address :

Subnet Mask :

10.100.1.2 is the IP of our server on the LAN (supporting FTP, HTTP, Telnet and mail services) to which we wish to forward traffic originating from the Internet.

Status: Ready

**Figure 19-4 Example 1: Destination Address for Traffic Originating from the Internet**



**Step 5.** When you have finished configuring your rules, the Rule Summary screen should look like this. Click **Apply** in this screen to save your configuration back to the ZyWALL.

The screenshot shows the ZyWALL 10 web interface. The left sidebar contains navigation links: MAIN MENU, Firewall, CONFIGURATION, LOCAL NETWORK, INTERNET, CUSTOM PORTS, LOGS, and LOGOUT. The main content area is titled "Internet to Local Network" and shows a "General" section with "ACL Default Set" set to "Block" and "Default Permit Log" checked. Below this is a table of rules:

No.	Status	Source IP	Destination IP	Service	Action	Log
1	Configured	Any	Any	BOOTP_CLIENT(UDP:68)	Forward	None
2	Configured	Any	10.100.1.2	HTTP(TCP:80)	Forward	Match
3	Empty					
4	Empty					
5	Empty					
6	Empty					
7	Empty					
8	Empty					
9	Empty					
10	Empty					

Below the table are buttons for "Apply", "Edit", and "Delete", and a "Number 1" dropdown with a "Move" button.

Callouts in the image provide the following information:

- A box pointing to the "General" section states: "Block packets that don't match the rules specified below." (Note: This text is slightly contradictory to the "Block" action shown in the screenshot).
- A box pointing to the first rule (No. 1) states: "The first rule is a default rule to allow DHCP negotiation between the ISP and the ZyWALL 10. The second rule is what we configured in the last 2 screens. See Table 16-1".
- A box pointing to the second rule (No. 2) states: "Log of packets should match this rule in the ACL Default Set." (Note: The screenshot shows "Match" in the Log column for rule 2).
- A box at the bottom states: "Click **Apply** in this screen when you have finished configuring to save your configuration back to the ZyWALL."

**Figure 19-5 Example 1: Rule Summary Screen**

### 19.1.2 Example 2: Small Office With Mail, FTP and Web Servers

A small office has:

- i. A mail server with an IP of 192.168.10.2.
- ii. Two FTP servers. You want FTP server One (IP of 192.168.10.3) to be accessible from the Internet, but FTP server Two (192.168.10.4) may only be accessed by internal users, i.e., from the local network.
- iii. HTTP proxy server at 192.168.10.5.

You want:

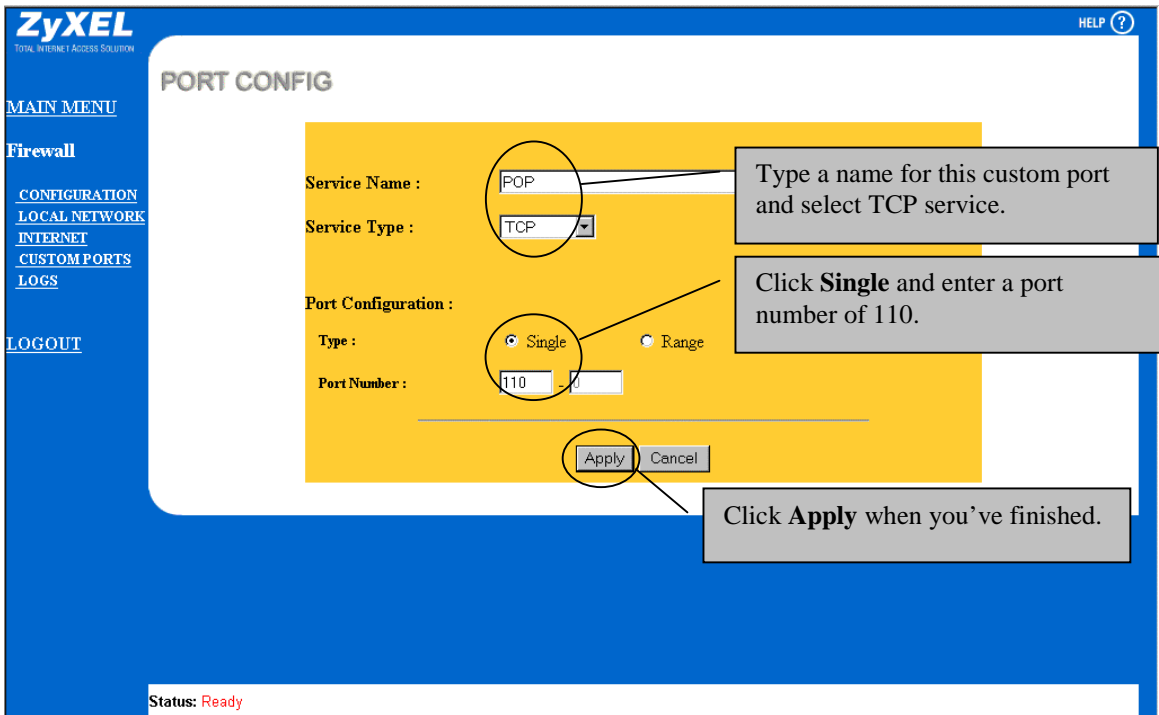
- i. To send alerts when there is an attack.
- ii. To only allow access to the Internet from the HTTP proxy server and your mail server.
- iii. To only allow FTP server One to be accessible from the Internet.

**Step 1.** First you want to send alerts when there is an attack. Go to the **Attack Alert** screen (click **Configuration**, then the **Attack Alert** tab) shown next.

**Figure 19-6 Send Alerts When Attacked**

**Step 2.** Configure the **E-mail** screen as shown in example 1: your mail server's IP is 192.168.10.2.

**Step 3.** Now you want to restrict access to the Internet except for the HTTP proxy server and your mail server. First you need to create a custom port for POP3. POP (Post Office Protocol) is an Internet mail server protocol that provides an incoming message storage system. It works in conjunction with the SMTP (Simple Mail Transfer Protocol), which provides the message transport services required to move mail from one system to another. The current version is called POP3. Click **Custom Ports** and configure the screen as follows.



**Figure 19-7 Configuring A POP Custom Port**

- Step 4.** Now, you will create rules to block all outgoing traffic (from the local network to the Internet) except for traffic originating from the HTTP proxy server and our mail server. Click **Internet** to see the **Rule Summary** screen. Now click an available **No.** (rule number) button, then click **Edit** to bring up the next screen.

**Step 5.** Click **SrcAdd** under the **Source Address** box and enter the IP address of the mail server (192.168.10.2) in the same fashion as in *Figure 19-4*.

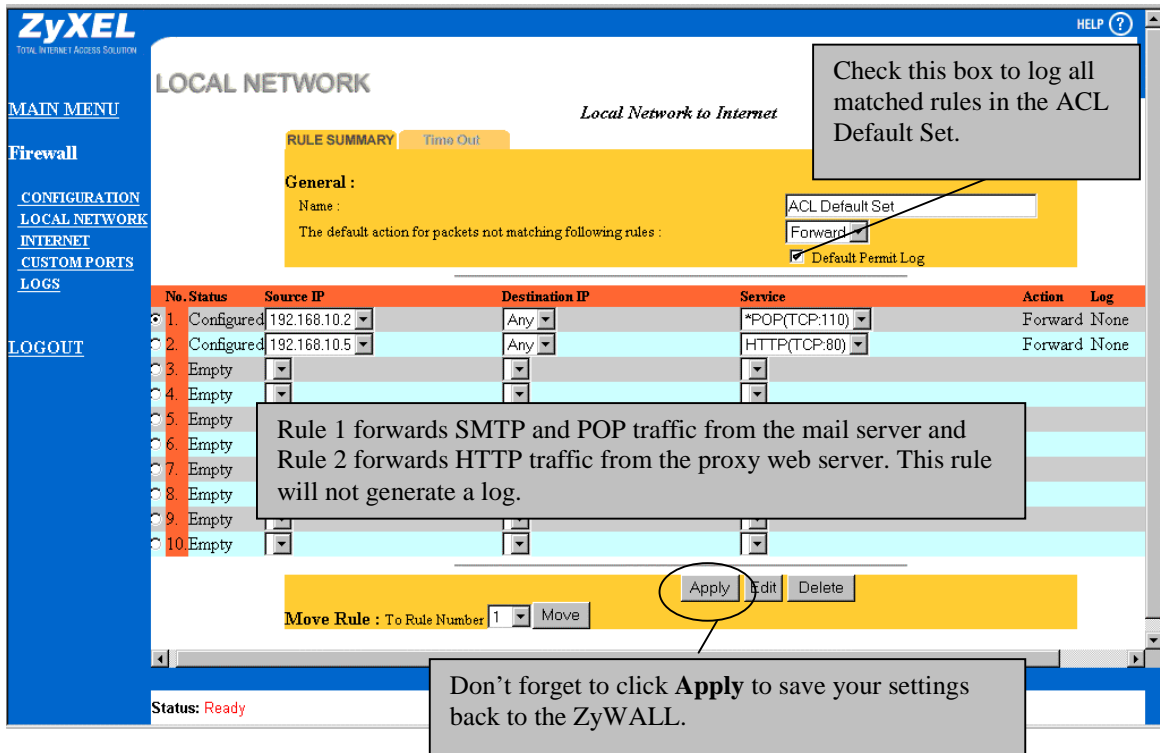
The screenshot displays the ZyXEL ZyWALL 10 Internet Security Gateway configuration interface. The main title is "RULE CONFIG" for a rule named "Local Network to Internet". The interface is divided into several sections:

- Source Address:** A text box containing "##### Source IP Address #####" with "192.168.10.2" entered below it. A callout box points to this field with the text "This is the IP address of your mail server." Below the text box are buttons for "SrcAdd", "SrcEdit", and "SrcDelete".
- Destination Address:** A text box containing "#####" with a callout box pointing to it.
- Services:**
  - Available Services:** A list box containing "\*Syslog(UDP:514)", "Any(TCP)", "Any(UDP)", "BGP(TCP:179)", and "BOOTP\_CLIENT(UDP:68)".
  - Selected Services:** A list box containing "\*POP(TCP:110)" and "SMTP(TCP:25)". A callout box points to this list with the text "You select these mail services. Note that the customized service has an '\*' before the name to distinguish it as such."
- Action for Matched Packets:** A dropdown menu set to "Forward". A callout box points to it with the text "You want to forward packets that match these rules."
- Log:** A dropdown menu set to "None".
- Buttons:** "Apply" and "Cancel" buttons are located at the bottom of the configuration area. A callout box points to the "Apply" button with the text "Click Apply when finished."

**Figure 19-8 Example 2: Local Network Rule 1 Configuration**

**Step 6.** Similarly configure another local network to Internet rule allowing traffic from our web (HTTP) proxy server.

**Step 7.** The **Rule Summary** screen should look like *Figure 19-9*. Don't forget to click **Apply** when you have finished configuring your rule(s) to save your settings back to the ZyWALL.



**Figure 19-9 Example 2: Local Network Rule Summary**

**Step 8.** Now you want an FTP server (IP of 192.168.10.3) to be accessible from the Internet. Remember the default Internet to Local Network ACL Set blocks all traffic from the Internet, so you want to create a hole for this server. Click the **Internet** link to see its **Rule Summary** screen. Now click an available **No.** (rule number) radio button, then click **Edit** to bring up the **Rule Config(uration)** screen. Now click on the **DestAdd** button under the **Destination Address** box and enter the IP of FTP server One (192.168.10.3). Follow the same procedure as shown in *Figure 19-3* and *Figure 19-4*.

**Step 9.** On completing the procedure the **Rule Summary** for this Internet firewall rules should look like the following screen. Don't forget to click **Apply** when you have finished configuring your rule(s) to save your settings back to the ZyWALL.

**ZyXEL**  
TOTAL INTERNET ACCESS SOLUTION

MAIN MENU  
Firewall  
CONFIGURATION  
LOCAL NETWORK  
INTERNET  
CUSTOM PORTS  
LOGS  
LOGOUT

Internet to Local Network

General :

Name : ACL\_Default Set

The default action for packets not matching following rules : Block

Default Permit Log

No.	Status	Source IP	Destination IP	Service	Action	Log
1	Configured	Any	Any	BOOTP_CLIENT(UDP:68)	Forward	None
2	Configured	Any	192.168.10.3	FTP(TCP:20,21)	Forward	None
3	Empty					
4	Empty					
5	Empty					
6	Empty					
7	Empty					
8	Empty					
9	Empty					
10	Empty					

Move Rule : To Rule Number 1 Move

Apply Edit Delete

Status: Ready

**Figure 19-10 Example: Internet to Local Network Rule Summary**

### 19.1.3 Example 3: DHCP Negotiation and Syslog Connection from the Internet

The following are some Internet firewall rule examples that allow DHCP negotiation between the ISP and the ZyWALL 10 and allow a syslog connection from the Internet.

**Step 1.** Follow the procedure shown next to first configure a custom port.

The screenshot shows the ZyXEL web interface for configuring a custom port. The page title is "PORT CONFIG". The left sidebar contains navigation links: MAIN MENU, Firewall, CONFIGURATION, LOCAL NETWORK, INTERNET, CUSTOM PORTS, LOGS, and LOGOUT. The main content area is yellow and contains the following fields:

- Service Name : Syslog
- Service Type : UDP
- Port Configuration :
  - Type :  Single  Range
  - Port Number : 514 - 0

At the bottom of the form are "Apply" and "Cancel" buttons. A grey callout box on the right contains the text: "Custom ports show up with an “\*” before their names in the Services list box and the Rule Summary list box. Click Apply after you’ve created your custom port." The status bar at the bottom left shows "Status: Ready".

Figure 19-11 Custom Port for Syslog

**Step 2.** Follow the procedures outlined in the previous examples to configure all your rules. When finished, your rule summary screen should look like the following.

The screenshot displays the ZyXEL Firewall Rule Configuration interface. The title is "RULE CONFIG" and the rule name is "Internet to Local Network".

- Source Address:** A text box contains "10.0.0.10 - 10.0.0.15". A callout box points to this field with the text: "This is the address range of the syslog servers."
- Destination Address:** A text box contains "Any".
- Services:**
  - Available Services:** A list box contains "\*POP(TCP:110)", "Any(TCP)", "Any(UDP)", "BGP(TCP:179)", and "BOOTP\_CLIENT(UDP:68)".
  - Selected Services:** A list box contains "\*Syslog(UDP:514)". A callout box points to this field with the text: "This is your Syslog custom port."
- Action for Matched Packets:** A dropdown menu is set to "Forward".
- Log:** A dropdown menu is set to "None".
- Alert:** An unchecked checkbox.
- Buttons:** "Apply" and "Cancel" buttons are visible at the bottom of the configuration area.
- Status:** A "Status: Ready" indicator is located at the bottom left of the interface.

A callout box at the bottom center of the interface says: "Click Apply when finished."

**Figure 19-12 Syslog Rule Configuration**



**Step 3.** On completing the procedure the **Rule Summary** for this Internet firewall rules should look like the following screen. Don't forget to click **Apply** when you have finished configuring your rule(s) to save your settings back to the ZyWALL.

**ZyXEL**  
TOTAL INTERNET ACCESS SOLUTION

MAIN MENU  
Firewall  
CONFIGURATION  
LOCAL NETWORK  
INTERNET  
CUSTOM PORTS  
LOGS  
LOGOUT

Rule 1: Allow DHCP negotiation between the ISP and the ZyWALL 10.  
Rule 2: Allow a syslog connection from the WAN.

Name : ACL Default Set  
The default action for packets not matching following rules : Block  
 Default Permit Log

No.	Status	Source IP	Destination IP	Service	Action	Log
1	Configured	Any	Any	BOOTP_CLIENT(UDP:68)	Forward	None
2	Configured	10.0.0.10 - 10.0.0.15	Any	*Syslog(UDP:514)	Forward	None
3	Empty					
4	Empty					
5	Empty					
6	Empty					
7	Empty					
8	Empty					
9	Empty					
10	Empty					

Move Rule : To Rule Number 1 Move

Apply Edit Delete

Click **Apply** to save your settings back to the ZyWALL.

Status: Ready

**Figure 19-13 Example 3: Rule Summary**

# Chapter 20

## Content Filtering

*This chapter provides a brief overview of content filtering using the Web Configurator. For more detailed information, consult the HTML help section of the included disk.*

Internet content filtering allows schools and businesses to create and enforce Internet access policies tailored to their needs. Content filtering gives the ability to block certain web features or specific URLs and should not be confused with packet filtering via SMT menu 21.1. To access these functions, Click on **Main Menu**, then **Content Filter** to expand the content filter menus.

### 20.1 Categories

#### 20.1.1 Restrict Web Features

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

#### 20.1.2 Filter List

The administrator can block categories, such as pornography or racial intolerance, or monitor visitation from a pre-defined list. Upon registration of the ZyWALL, the use of the list is free for a trial period. After this period, you must subscribe to the list periodically.

#### 20.1.3 Days and Times

The ZyWALL also allows the administrator to define time periods and days during which content filtering is enabled.

**ZyXEL**  
TOTAL INTERNET ACCESS SOLUTION

HELP ?

**CATEGORIES**

MAIN MENU

**Content Filter**

REGISTRY

Free  
iCard

CATEGORIES

LIST UPDATE

EXEMPT ZONE

CUSTOMIZE

URL KEYWORD

LOGS

LOGOUT

**Restrict Web Server Data :**

ActiveX  Java Applet  Cookies  Web Proxy

**Filter List Setup :**

The Filter List has not been loaded

Log and Block Access  Log Only

Block all categories

Violence/Profanity  Partial Nudity  Full Nudity  Sexual Acts

Gross Depictions  Intolerance  Satanic/Cult  Drug Culture

Militant/Extremist  Sex Education  Alcohol/Tobacco

Gambling/Questionable/Illegal  Sports/Entertainment

**Time of Day(Filter List/Customize/Keyword) :**

Always block

Block from 08 : 00 to 17 : 30 (24-Hour Format)

Apply Reset

Status: Ready

Figure 20-1 Categories Screen

## 20.2 Update List

Content on the Internet is constantly changing, so the content filter list should be updated on a weekly basis.

**ZyXEL**  
TOTAL INTERNET ACCESS SOLUTION

HELP ?

MAIN MENU

Content Filter

REGISTRY

Free

iCard

CATEGORIES

LIST UPDATE

EXEMPT ZONE

CUSTOMIZE

URL KEYWORD

LOGS

LOGOUT

**LIST UPDATE**

Filter List Status :  
The Filter List has not been loaded

Filter List Updates :

Download Now

Automatic Download :

Update Schedule Day : Wednesday

At : 12 : 30 (24-Hour Format)

Apply Reset

Status: Ready

Figure 20-2 List Update Screen

## 20.3 Exempting Computers

This screen allows the administrator to include or exclude a range of users on the LAN from content filtering.

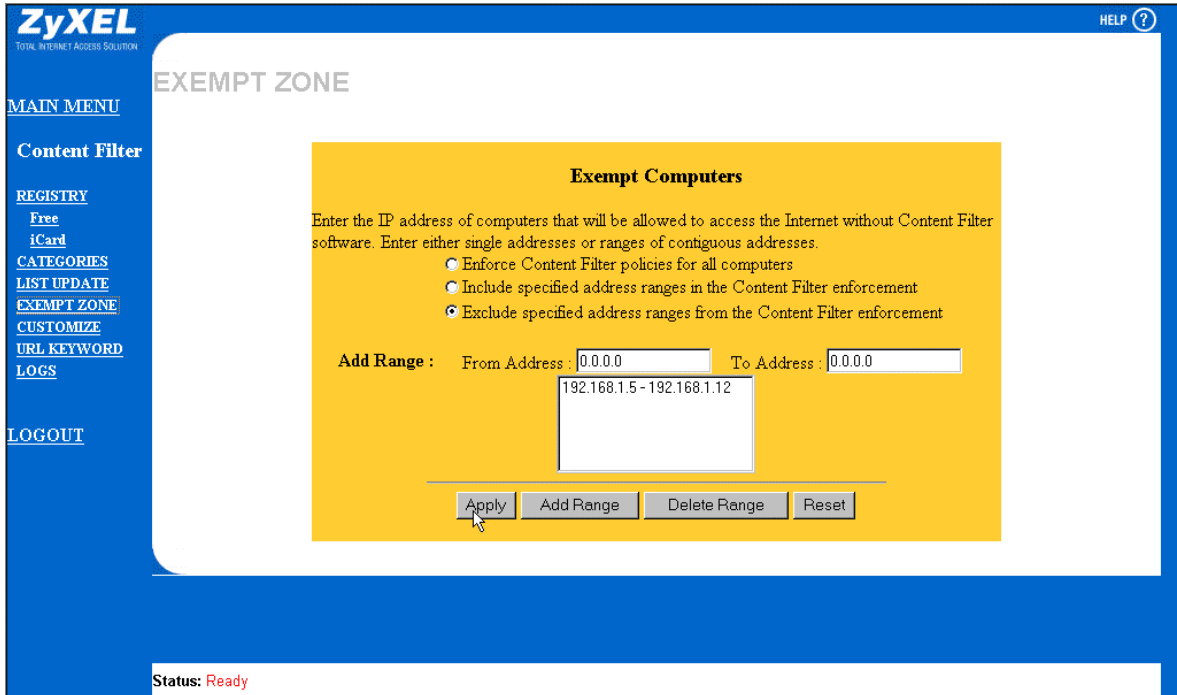


Figure 20-3 Exempt Zone Screen

## 20.4 Customizing

Customize the content filter list by adding or removing specific sites from the filter list.

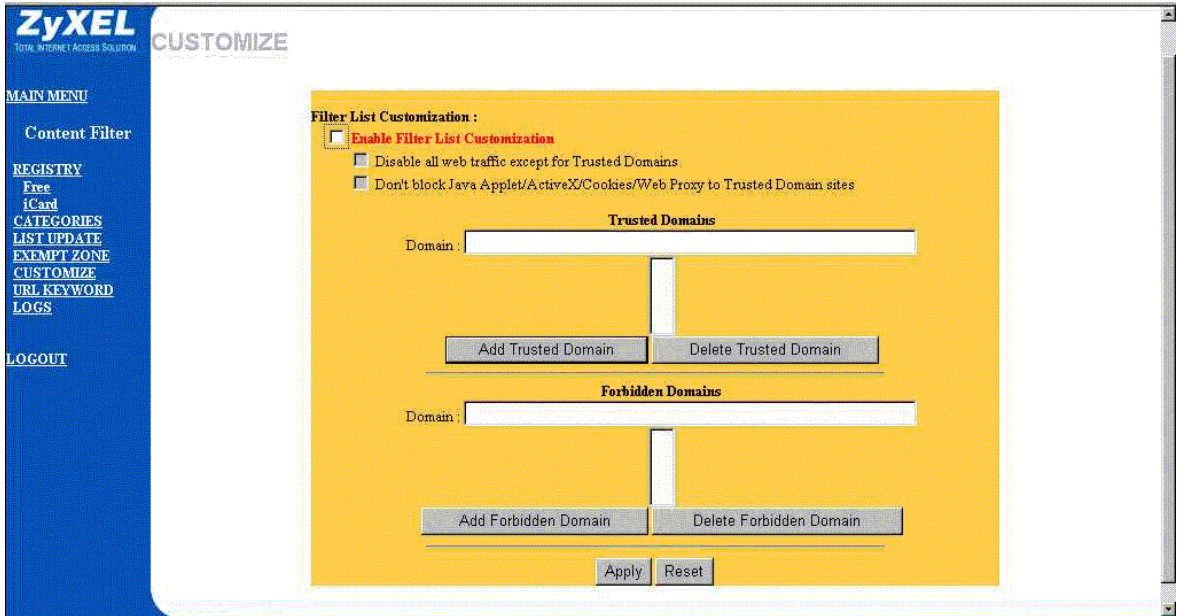


Figure 20-4 Customize Screen

## 20.5 Keywords

The ZyWALL can also be configured to block certain web sites by using URL keywords.

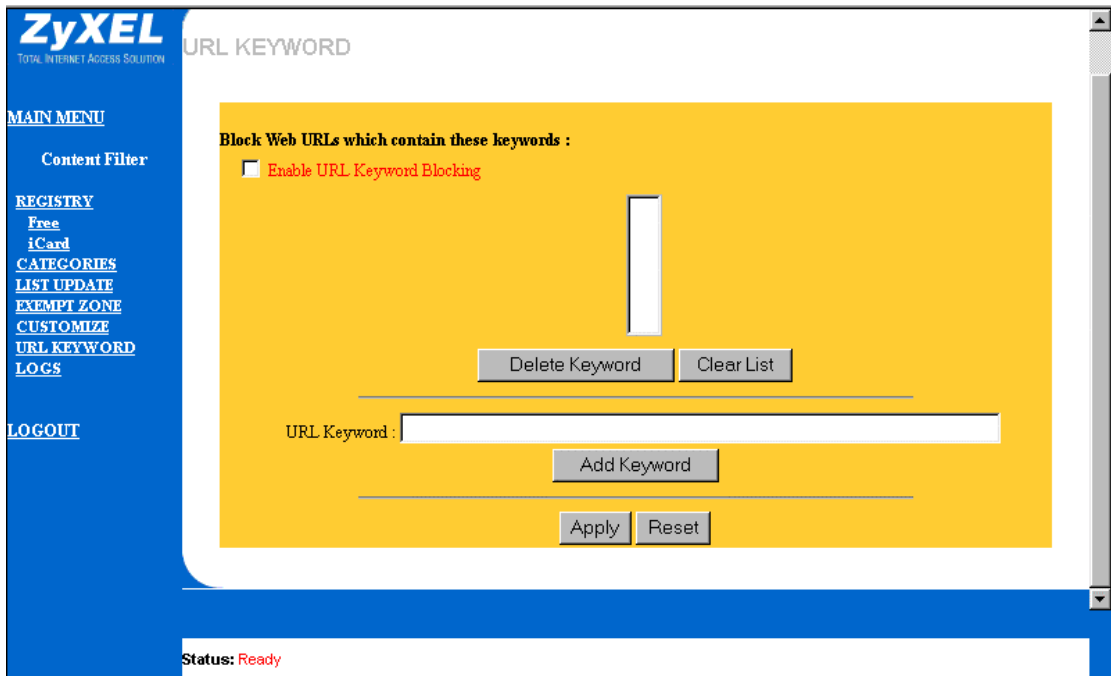


Figure 20-5 Keyword Screen

## 20.6 Log Records

This screen records the results of your content filter policies.

**ZyXEL**  
TOTAL INTERNET ACCESS SOLUTION

HELP ?

LOGS

Content Filter Logs (Page 1/0)

no Content Filter Log existing -----

Previous Page Refresh Clear Next Page

Status: Ready

Figure 20-6 Logs Screen



---

---

# Part V:

---

## Troubleshooting, Appendices, Glossary and Index

---

Chapter 21 provides information about solving common problems, followed by some Appendices, a Glossary of Terms and an Index.



# Chapter 21

## Troubleshooting

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

### 21.1 Problems Starting Up the ZyWALL

**Table 21-1 Troubleshooting the Start-Up of your ZyWALL**

Problem	Corrective Action	
None of the LEDs are on when you turn on the ZyWALL.	Check the connection between the power adapter and the ZyWALL. If the error persists, you may have a hardware problem. In this case, you should contact technical support.	
Cannot access the ZyWALL via the console port.	1. Check to see if the ZyWALL is connected to your computer's serial port.	
	2. Check to see if the communications program is configured correctly. The communications software should be configured as follows:	VT100 terminal emulation
		9600 bps is the default speed on leaving the factory. Try other speeds in case the speed has been changed.
	No parity, 8 data bits, 1 stop bit, data flow set to none.	

## 21.2 Problems with the LAN Interface

**Table 21-2 Troubleshooting the LAN Interface**

Problem	Corrective Action
Can't ping any workstation on the LAN.	Check the 10M/100M LEDs on the front panel. One of these LEDs should be on. If they are both off, check the cables between your ZyWALL and hub or the station.
	Verify that the IP address and the subnet mask are consistent between the ZyWALL and the workstations.

## 21.3 Problems with the WAN interface

**Table 21-3 Troubleshooting the WAN interface**

Problem	Corrective Action
Cannot get WAN IP from the ISP.	The WAN IP is provided when the ISP recognizes the user as an authorized user after verifying the MAC address or Host Name or User ID.  Find out the verification method used by your ISP.
	If the ISP checks the LAN MAC Address, tell the ISP the WAN MAC address of the ZyWALL. The WAN MAC can be obtained from menu 24.1.  In case the ISP does not allow you to use a new MAC, you can clone the MAC from the LAN as the WAN MAC and send it to the ISP using <b>Menu 2 - WAN Setup</b> . We recommend you configure this menu anyway even if your ISP presently does not require MAC address authentication
	If the ISP checks the Host Name, enter host name in the <b>System Name</b> field in <b>Menu 1 - General Setup</b> when you connect the ZyWALL to a cable/xDSL modem.
	If the ISP checks the User ID, make sure that you have entered the correct <b>Service Type</b> , user name (in the <b>My Login</b> field) and password (in the <b>My Password</b> field) in <b>Menu 4 - Internet Access Setup</b> .
Can't connect to a remote node or ISP.	Check menu 24.1 to verify the line status. If it indicates <b>Down</b> , then refer to the section on the line problems.

## 21.4 Problems with Internet Access

**Table 21-4 Troubleshooting Internet Access**

Problem	Corrective Action
Cannot access the Internet.	Connect your Cable/xDSL modem with the ZyWALL using appropriate cable.
	Check with the manufacturer of your Cable/xDSL device about your cable requirement because for some devices may require crossover cable and others a regular patch cable.
	Verify your settings in menu 3.2 and menu 4.

## 21.5 Problems with the Firewall

**Table 21-5 Troubleshooting the Firewall**

Problem	Corrective Action
Cannot configure the firewall.	You can ONLY configure the firewall via ZyWALL Web Configurator or CI command. You will not be able to access the ZyWALL Web Configurator from the WAN if:
	The firewall is activated, as the firewall by default, blocks all WAN to LAN traffic. To access the ZyWALL Web Configurator from the WAN when the firewall is activated, you will need to create a firewall rule (see the <i>Example Firewall Rules</i> chapter) to allow web traffic initiated from the WAN.
	You have applied a filter in menu 3.1 (LAN) or in menu 11.5 (WAN) to block web service.
	You have an SMT console session running.



# 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 the PCs use traditional dial-up networking.

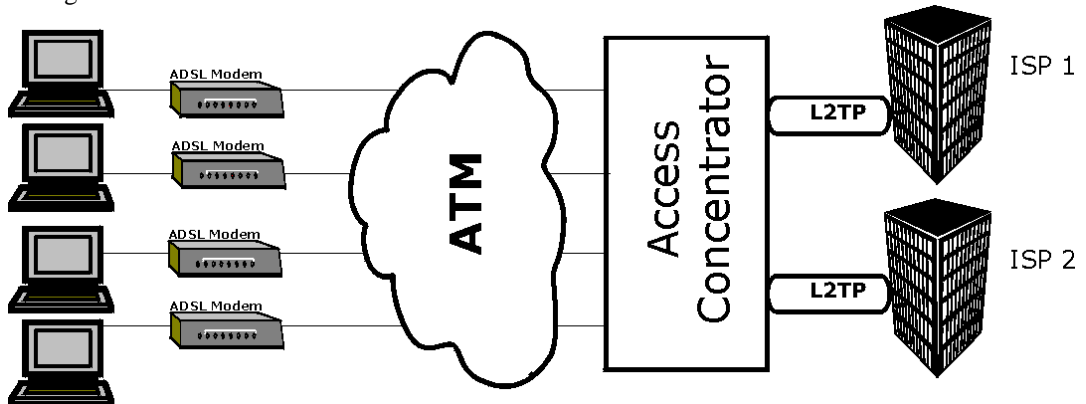


Diagram 1 Single-PC per Modem Hardware Configuration

### 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.

### 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.

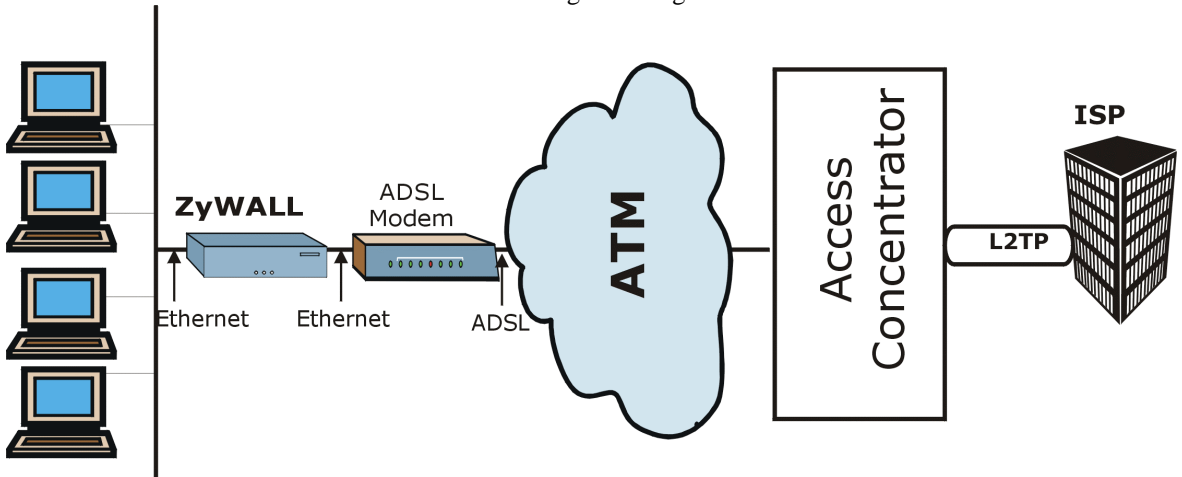


Diagram 2 ZyWALL as a PPPoE Client



# Appendix B

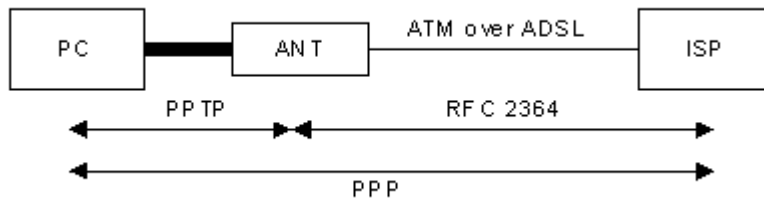
## PPTP

### 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

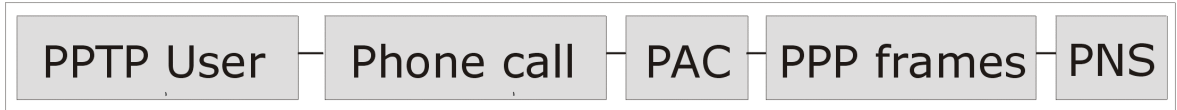
When the ZyWALL is deployed in such a setup, it appears as a PC to the ANT (ADSL Network Termination).

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 (i.e. NT server) behind the NAT. Users need to forward PPTP packets to port 1723 by configuring the server in **Menu 15.2 - Server Set Setup**. 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.

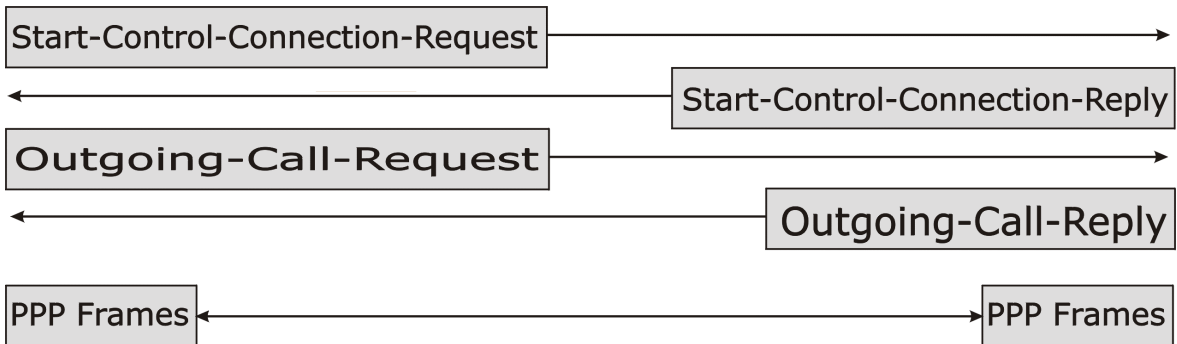
**Control & PPP connections**

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**

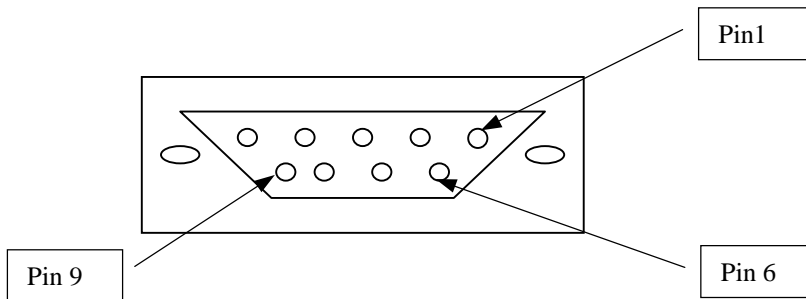
**PPP Data Connection**

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

## Hardware Specifications

Power Specification	I/P AC 120V / 60Hz ; O/P DC 12V 1200 mA
MTBF	100000 hrs
Operation Temperature	0° C ~ 40° C
Ethernet Specification for WAN	10Mbit Half Duplex
Ethernet Specification for LAN	10/100 Mbit Half / Full Auto-negotiation
Console Port RS – 232	Pin 1 = NON ; Pin 2 = DTE-RXD; Pin 3 = DTE-TXD; Pin 4 = DTE-DTR; Pin 5 = GND; Pin 6 = DTE-DSR; Pin 7 = DTE-RTS; Pin 8 = DTE-CTS; PIN 9 = NON. See Figure below



WAN/LAN Cable Pin Layout:			
Straight-Through		Crossover	
(Switch)	(Adapter)	(Switch)	(Switch)
1 IRD +	1 OTD +	1 IRD +	1 IRD +
2 IRD -	2 OTD -	2 IRD -	2 IRD -
3 OTD +	3 IRD +	3 OTD +	3 OTD +
6 OTD -	6 IRD -	6 OTD -	6 OTD -

# Appendix D

## Important Safety Instructions

The following safety instructions apply to the ZyWALL.

1. Be sure to read and follow all warning notices and instructions.
2. The maximum recommended ambient temperature for the ZyWALL is 40° Celsius (104° Fahrenheit). Care must be taken to allow sufficient air circulation or space between units when the ZyWALL is installed inside a closed rack assembly. The operating ambient temperature of the rack environment might be greater than room temperature.
3. Installation in a rack without sufficient airflow can be unsafe.
4. Racks should safely support the combined weight of all equipment.
5. The connections and equipment that supply power to the ZyWALL should be capable of operating safely with the maximum power requirements of the ZyWALL. In case of a power overload, the supply circuits and supply wiring should not become hazardous. The input rating of the ZyWALL is printed on the nameplate.
6. The AC adapter must plug in to the right supply voltage, i.e. 120VAC adapter for North America and 230VAC adapter for Europe. Make sure that the supplied AC voltage is correct and stable. If the input AC voltage is over 10% lower than the standard may cause the ZyWALL to malfunction.
7. Installation in restricted access areas must comply with Articles 110-16, 110-17, and 110-18 of the National Electrical Code, ANSI/NFPA 70.
8. Do not allow anything to rest on the power cord of the AC adapter, and do not locate the product where anyone can walk on the power cord.
9. Do not service the product by yourself. Opening or removing covers can expose you to dangerous high voltage points or other risks. Refer all servicing to qualified service personnel.
10. Generally, when installed after the final configuration, the product must comply with the applicable safety standards and regulatory requirements of the country in which it is installed. If necessary, consult the appropriate regulatory agencies and inspection authorities to ensure compliance.
11. A rare condition can create a voltage potential between the earth grounds of two or more buildings. If products installed in separate building are interconnected, the voltage potential can cause a hazardous condition. Consult a qualified electrical consultant to determine whether or not this phenomenon exists and, if necessary, implement corrective action before interconnecting the products. If the equipment is to be used with telecommunications circuit, take the following precautions:
  - Never install telephone wiring during a lightning storm.
  - Never install telephone jacks in wet location unless the jack is specially designed for wet location.
  - Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
  - Use caution when installing or modifying telephone lines (other than a cordless telephone) during an electrical storm. There is a remote risk of electric shock from lightning.

# Appendix E

## Firewall CLI Commands

The following table describes the syntax used to configure your firewall using Command Line Interface (CLI) commands. Select **Menu 24.8 - Command Interpreter Mode** from the main menu to go into CLI mode. For details on other CLI commands to configure your ZyWALL, please consult the included disk.

Function	CLI Syntax	Description
<b>Firewall Set-Up</b>		
	<code>config edit firewall active &lt;yes   no&gt;</code>	Activates or deactivates the saved firewall settings.
	<code>config retrieve firewall</code>	Retrieves currently saved firewall settings.
	<code>config save firewall</code>	Saves the current firewall settings.
<b>Display</b>		
	<code>config display firewall</code>	Displays the all the firewall settings including e-mail, attack, and sets/rules.
	<code>config display firewall set &lt;set #&gt;</code>	Displays current entries of a set configuration; including timeout values, name, default-permit, and number of rules under it. If you don't put # after set, it will display all the sets/rules information.
	<code>config display firewall set &lt;set #&gt; rule &lt;rule #&gt;</code>	Displays current entries of a rule in a set configuration;
	<code>config display firewall attack</code>	Displays all the settings for attack alert.
	<code>config display firewall e-mail</code>	Displays all the setting for e-mail part.
	<code>config display firewall ?</code>	Displays all the available sub commands.
<b>Edit</b>		
<b>E-mail</b>	<code>config edit firewall e-mail mail- server &lt;ip address of mail server&gt;</code>	Edits the mail server which alerting e-mail messages are sent through.
	<code>config edit firewall e-mail return-addr &lt;e-mail address&gt;</code>	Edits the source address for sending mail usage.

Function	CLI Syntax	Description
	<code>config edit firewall e-mail email-to &lt;e-mail address&gt;</code>	Edits the mail address which you want to send the alert to.
	<code>config edit firewall e-mail policy &lt;full   hourly   daily   weekly&gt;</code>	Edits whether the current firewall traffic log contents are sent through e-mail when the log is full, hourly, daily, or weekly.
	<code>config edit firewall e-mail day &lt;sunday   monday   tuesday   wednesday   thursday   friday   saturday&gt;</code>	Edits the day the current firewall traffic log contents are sent through e-mail; pertains to the weekly policy.
	<code>config edit firewall e-mail hour &lt;0-23&gt;</code>	Edits the hour of the day the current firewall traffic log contents are sent through e-mail; pertains to the hourly, daily & weekly policies.
	<code>config edit firewall e-mail minute &lt;0-59&gt;</code>	Edits the minute of the hour the current firewall traffic log contents are sent through e-mail; pertains to the hourly, daily & weekly policies.
<b>Attack</b>	<code>config edit firewall attack send-alert &lt;yes   no&gt;</code>	Activates or deactivates the firewall DOS attack notification e-mails.
	<code>config edit firewall attack block &lt;yes   no&gt;</code>	Yes: to block the traffics when exceeds the threshold of tcp-max-incomplete . No: to delete the oldest half-open session when exceeds the threshold of tcp-max-incomplete.
	<code>config edit firewall attack block-minute &lt;0-255&gt;</code>	Only valid when sets block to be yes. The unit is minute.
	<code>config edit firewall attack minute-high &lt;0-255&gt;</code>	The threshold to start to delete the old half-opened sessions to minute-low.
	<code>config edit firewall attack minute-low &lt;0-255&gt;</code>	The threshold to stop the deletion of the half-opened sessions.
	<code>config edit firewall attack max-incomplete-high &lt;0-255&gt;</code>	The threshold to start to delete the old half-opened sessions to max-incomplete-low.
	<code>config edit firewall attack max-incomplete-low &lt;0-255&gt;</code>	The threshold to stop the deletion of the half-opened sessions.
	<code>config edit firewall attack tcp-max-incomplete &lt;0-255&gt;</code>	The threshold to start executing the block field.
<b>Sets</b>	<code>config edit firewall set &lt;set #&gt; name &lt;desired name&gt;</code>	Edits the name for a specified set.

Function	CLI Syntax	Description
	<code>Config edit firewall set &lt;set #&gt; default-permit &lt;forward   block&gt;</code>	Edits whether a packet is dropped or allowed through, when it does not meet a rule within the set.
	<code>Config edit firewall set &lt;set #&gt; icmp-timeout &lt;seconds&gt;</code>	Edits the time limit, in seconds, for an idle ICMP session, before it is terminated.
	<code>Config edit firewall set &lt;set #&gt; udp-idle-timeout &lt;seconds&gt;</code>	Edits the time limit, in seconds, for an idle UDP session, before it is terminated.
	<code>Config edit firewall set &lt;set #&gt; connection-timeout &lt;seconds&gt;</code>	Edits the wait time, in seconds, for the SYN traffic in initiating a TCP session, before it is terminated.
	<code>Config edit firewall set &lt;set #&gt; fin-wait-timeout &lt;seconds&gt;</code>	Edits the wait time, in seconds, for the FIN traffic in concluding a TCP session, before it is terminated.
	<code>Config edit firewall set &lt;set #&gt; tcp-idle-timeout &lt;seconds&gt;</code>	Edits the time limit, in seconds, for an idle TCP session, before it is terminated.
	<code>Config edit firewall set &lt;set #&gt; log &lt;yes   no&gt;</code>	Switches on/off the logs for matching default permit.
<b>Rules</b>	<code>Config edit firewall set &lt;set #&gt; rule &lt;rule #&gt; permit &lt;forward   block&gt;</code>	Edits whether a packet is dropped or allowed through, when it meets this rule.
	<code>Config edit firewall set &lt;set #&gt; rule &lt;rule #&gt; active &lt;yes   no&gt;</code>	Edits whether a rule is enabled or not.
	<code>Config edit firewall set &lt;set #&gt; rule &lt;rule #&gt; protocol &lt;integer protocol value &gt;</code>	Edits the protocol specification number made in this rule for ICMP currently.
	<code>Config edit firewall set &lt;set #&gt; rule &lt;rule #&gt; log &lt;none   match   not- match   both&gt;</code>	Edits whether traffic that does match the rule, doesn't match, both or neither is logged.
	<code>Config edit firewall set &lt;set #&gt; rule &lt;rule #&gt; alert &lt;yes   no&gt;</code>	Activates or deactivates the notification function, for when a DOS attack occurs or there is a violation of any alert settings. In case of such instances, the function will send an e-mail to the SMTP destination address and log an alert.
	<code>config edit firewall set &lt;set #&gt; rule &lt;rule #&gt; srcaddr-single &lt;ip address&gt;</code>	Selects and edits a source address of the traffic which comply to this rule.

Function	CLI Syntax	Description
	<pre>config edit firewall set &lt;set #&gt; rule &lt;rule #&gt; srcaddr-subnet &lt;ip address&gt; &lt;subnet mask&gt;</pre>	Selects and edits a source address and subnet mask of traffic which comply to this rule.
	<pre>config edit firewall set &lt;set #&gt; rule &lt;rule #&gt; srcaddr-range &lt;start ip address&gt; &lt;end ip address&gt;</pre>	Selects and edits a source address range of traffic which comply to this rule.
	<pre>config edit firewall set &lt;set #&gt; rule &lt;rule #&gt; destaddr-single &lt;ip address&gt;</pre>	Selects and edits a destination address of the traffic which comply to this rule.
	<pre>config edit firewall set &lt;set #&gt; rule &lt;rule #&gt; destaddr-subnet &lt;ip address&gt; &lt;subnet mask&gt;</pre>	Selects and edits a destination address and subnet mask of traffic which comply to this rule.
	<pre>config edit firewall set &lt;set #&gt; rule &lt;rule #&gt; destaddr-range &lt;start ip address&gt; &lt;end ip address&gt;</pre>	Selects and edits a destination address range of traffic which comply to this rule.
	<pre>config edit firewall set &lt;set #&gt; rule &lt;rule #&gt; TCP destport-single &lt;port #&gt;</pre>	Selects and edits the destination port of the traffic which comply with this rule. For non-consecutive port numbers, the user may repeat this command line to enter in the multiple port numbers.
	<pre>config edit firewall set &lt;set #&gt; rule &lt;rule #&gt; TCP destport-range &lt;start port #&gt; &lt;end port #&gt;</pre>	Selects and edits a destination port range of traffic which comply to this rule.
	<pre>config edit firewall set &lt;set #&gt; rule &lt;rule #&gt; UDP destport-single &lt;port #&gt;</pre>	Selects and edits the destination port of the traffic which comply with this rule. For non-consecutive port numbers, the user may repeat this command line to enter in the multiple port numbers.
	<pre>config edit firewall set &lt;set #&gt; rule &lt;rule #&gt; UDP destport-range &lt;start port #&gt; &lt;end port #&gt;</pre>	Selects and edits a destination port range of traffic which comply to this rule.
	<pre>config edit firewall set&lt;set #&gt; rule &lt;rule #&gt; destport-custom &lt;desired custom port name&gt;</pre>	Types in the desired custom port name.



Function	CLI Syntax	Description
Delete	<code>config delete firewall e-mail</code>	Removes all the settings for e-mail alert.
	<code>config delete firewall attack</code>	Resets all the settings for attack to default setting.
	<code>config delete firewall set &lt;set #&gt;</code>	Removes the specified set from the firewall configuration.
	<code>config delete firewall set &lt;set #&gt; rule &lt;rule #&gt;</code>	Removes the specified rule in a set from the firewall configuration.

# Appendix F

## Power Adapter Specifications

---

---

### AC Power Adapter Specifications

---

---

#### North America

---

---

AC Power Adapter model MW48-1201200

Input power: AC120Volts/60Hz

Output power: DC12Volts/1.2A

Power consumption: 9 W

Plug: North American standards

Safety standards: UL, CUL (UL 1310, CSA C22.2 No.233-M91)

---

AC Power Adapter model AD48-1201200DUY

Input power: AC120Volts/60Hz

Output power: DC12Volts/1.2A

Power consumption: 9 W

Plug: North American standards

Safety standards: UL, CUL (UL1950, CSA C22.2 NO. 234-M90)

---

---

#### European Union

---

---

AC Power Adapter model AD-1201200DV

Input power: AC230Volts/50Hz,

Output power: DC12Volts/1.2A

Power consumption: 9 W

Plug: European Union standards

Safety standards: TUV, CE (EN 60950)

---

AC Power Adapter model JAD-121200E

Input power: AC230Volts/50Hz,

Output power: DC12Volts/1.2A

Power consumption: 9 W

Plug: European Union standards

Safety standards: TUV, CE (EN 60950)

---

---

#### UK

---

---

AC Power Adapter model AD-1201200DK

Input power: AC230Volts/50Hz,

Output power: DC12Volts/1.2A

Power consumption: 9 W

Plug: United Kingdom standards

Safety standards: TUV, CE (EN 60950, BS7002)

---

---

---

---

Japan

---

AC Power Adapter model JOD-48-1124  
Input power: AC100Volts/ 50/60Hz/ 27VA  
Output power: DC12Volts/1.2A  
Power consumption: 9 W  
Plug: Japan standards  
Safety standards: T-Mark

---

---

---

Australia and New Zealand

---

AC Power Adapter model AD-1201200DS  
Input power: AC240Volts/50Hz/0.2A  
Output power: DC12Volts/1.2A  
Power consumption: 9 W  
Plug: Australia and New Zealand standards  
Safety standards: NATA (AS 3260)

---

# Glossary of Terms

10BaseT	The 10-Mbps baseband Ethernet specification that uses two pairs of twisted-pair cabling (Category 3 or 5): one pair for transmitting data and the other for receiving data.
ARP	Address Resolution Protocol is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address that is recognized in the local network.
Authenticity	Proof that the information came from the person or location that reportedly sent it. One example of authenticating software is through digital signatures.
Back Door	A deliberately planned security breach in a program. Back doors allow special access to a computer or program. Sometimes back doors can be exploited and allow a cracker unauthorized access to data.
Backbone	A high-speed line or series of connections that forms a major pathway within a network.
BackOrifice	BackOrifice is a remote administration tool which allows a user to control a computer across a TCP/IP connection using a simple console or GUI application. BackOrifice is a potentially disastrous Trojan horse since it can provide the user unlimited access to a system.
Bandwidth	This is the capacity on a link usually measured in bits-per-second (bps).
Bit	(Binary Digit) -- A single digit number in base-2, in other words, either a 1 or a zero. The smallest unit of computerized data.
Brute Force Hacking	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.
Byte	A set of bits that represent a single character. There are 8 bits in a Byte.
Camping Out	Staying in a "safe" place once a hacker has broken into a system. The term can be used with a physical location, electronic reference, or an entry point for future attacks.
CDR	Call Detail Record. This is a name used by telephone companies for call related information.
CHAP	Challenge Handshake Authentication Protocol is an alternative protocol that avoids sending passwords over the wire by using a challenge/response technique.
Cipher Text	Text that has been scrambled or encrypted so that it cannot be read without deciphering it. See Encryption
Client	A software program that is used to contact and obtain data from a Server software program on another computer. Each Client program is designed to work with one or more specific kinds of Server programs, and each Server requires a specific kind of Client. A Web Browser is a specific kind of Client.

Cookie	A string of characters saved by a web browser on the user's hard disk. Many web pages send cookies to track specific user information. Cookies can be used to retain information as the user browses a web site. For example, cookies are used to 'remember' the items a shopper may have in a shopping cart.
Countermeasures	Techniques, programs, or other tools that can protect your computer against threats.
Cracker	Another term for hackers. Generally, the term cracker refers specifically to a person who maliciously attempts to break encryption, software locks, or network security.
Cracker Tools	Programs used to break into computers. Cracker tools are widely distributed on the Internet. They include password crackers, Trojans, viruses, war-dialers, and worms.
Cracking	The act of breaking into computers or cracking encryption.
Crossover Ethernet cable	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.
Cryptoanalysis	The act of analyzing (or breaking into) secure documents or systems that are protected with encryption.
CSU/DSU	Channel Service Unit/Data Service Unit. CSUs (channel service units) and DSUs (data service units) are actually two separate devices, but they are used in conjunction and often combined into the same box. The devices are part of the hardware you need to connect computer equipment to digital transmission lines. The Channel Service Unit device connects with the digital communication line and provides a termination for the digital signal. The Data Service Unit device, sometimes called a digital service unit, is the hardware component you need to transmit digital data over the hardware channel. The device converts signals from bridges, routers, and multiplexors into the bipolar digital signals used by the digital lines. Multiplexors mix voice signals and data on the same line.
DCE	Data Communications Equipment is typically a modem or other type of communication device. The DCE sits between the DTE (data terminal equipment) and a transmission circuit such as a phone line.
Decryption	The act of restoring an encrypted file to its original state.
Denial of Service	Act of preventing customers, users, clients or other machines from accessing data on a computer. This is usually accomplished by interrupting or overwhelming the computer with bad or excessive information requests.
DHCP	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 addresses are made available to assign to other systems.

Digital Signature	Digital code that authenticates whomever signed the document or software. Software, messages, Email, and other electronic documents can be signed electronically so that they cannot be altered by anyone else. If someone alters a signed document, the signature is no longer valid. Digital signatures are created when someone generates a hash from a message, then encrypts and sends both the hash and the message to the intended recipient. The recipient decrypts the hash and original message, makes a new hash on the message itself, and compares the new hash with the old one. If the hashes are the same, the recipient knows that the message has not been changed. Also see Public-key encryption.
DNS	Domain Name System. A database of domain names and their IP addresses. DNS is the primary naming system for many distributed networks, including the Internet.
Domain Name	The unique name that identifies an Internet site. Domain Names always have 2 or more parts, separated by dots. The part on the left is the most specific, and the part on the right is the most general.
DRAM	Dynamic RAM that stores information in capacitors that must be refreshed periodically.
DSL	Digital Subscriber Line technologies enhances the data capacity of the existing twisted-pair wire that runs between the local telephone company switching offices and most homes and offices. There are actually seven types of DSL service, ranging in speeds from 16 Kbits/sec to 52 Mbits/sec. The services are either symmetrical (traffic flows at the same speed in both directions), or asymmetrical (the downstream capacity is higher than the upstream capacity). DSL connections are point-to-point dedicated circuits, meaning that they are always connected. There is no dial-up. There is also no switching, which means that the line is a direct connection into the carrier's frame relay, ATM (Asynchronous Transfer Mode), or Internet-connect system.
DSLAM	A Digital Subscriber Line Access Multiplexer (DSLAM) is a network device, usually at a telephone company central office, that receives signals from multiple customer Digital Subscriber Line connections and puts the signals on a high-speed backbone line using multiplexing techniques. Depending on the product, DSLAM multiplexers connect DSL lines with some combination of asynchronous transfer mode ATM, frame relay, or IP networks.
DTE	Originally, the DTE (data terminal equipment) meant a dumb terminal or printer, but today it is a computer, or a bridge or router that interconnects local area networks.
EMI	ElectroMagnetic Interference. The interference by electromagnetic signals that can cause reduced data integrity and increased error rates on transmission channels.
Encryption	The act of substituting numbers and characters in a file so that the file is unreadable until it is decrypted. Encryption is usually done using a mathematical formula that determines how the file is decrypted.
Ethernet	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.

Events	These are network activities. Some activities are direct attacks on your system, while others might be depending on the circumstances. Therefore, any activity, regardless of severity is called an event. An event may or may not be a direct attack on your system.
FAQ	(Frequently Asked Questions) -- FAQs are documents that list and answer the most common questions on a particular subject.
FCC	The FCC (Federal Communications Commission) is in charge of allocating the electromagnetic spectrum and thus the bandwidth of various communication systems.
Firewall	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.
Flash memory	The nonvolatile storage that can be electrically erased and reprogrammed so that data can be stored, booted, and rewritten as necessary.
FTP	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.
Gateway	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.
Hacker	Generally, a hacker is anyone who enjoys experimenting with technology including computers and networks. Not all hackers are criminals breaking into systems. Some are legitimate users and hobbyists. Nevertheless, some are dedicated criminals or vandals.
HDLC	HDLC (High-level Data Link Control) is a bit-oriented (the data is monitored bit by bit), link layer protocol for the transmission of data over synchronous networks.
Host	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.
HTTP	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.
IANA	Internet Assigned Number Authority acts as the clearinghouse to assign and coordinate the use of numerous Internet protocol parameters such as Internet addresses, domain names, protocol numbers, and more. The IANA Web site is at <a href="http://www.isi.edu/iana">http://www.isi.edu/iana</a> .
ICMP	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.

Integrity	Proof that the data is the same as originally intended. Unauthorized software or people have not altered the original information.
internet	(Lower case i) Any time you connect 2 or more networks together, you have an internet.
Internet	(Upper case I) The vast collection of inter-connected networks that all use the TCP/IP protocols and that evolved from the ARPANET of the late 60's and early 70's. The Internet now (July 1995) connects roughly 60,000 independent networks into a vast global internet
Internet Worm	See Worm.
Intranet	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.
Intruder	Person or software interested in breaking computer security to access, modify, or damage data. Also see Cracker.
IP	Internet Protocol the IP (currently IP version 4, or IPv4), is the underlying protocol for routing packets on the Internet and other TCP/IP-based networks.
IPCP (PPP)	IP Control Protocol allows changes to IP parameters such as the IP address.
IPX	Internetwork Packet eXchange The native NetWare internetworking protocol is IPX (Internetwork Packet Exchange). Like IP (Internet Protocol), IPX is an internetworking protocol that provides datagram services.
IRC	Internet Relay Chat. IRC was developed in the late 1980s as a way for multiple users on a system to "chat" over the network. Today IRC is a very popular way to "talk" in real time with other people on the Internet. However, IRC is also one avenue hackers use to get information from you about your system and your company. Moreover, IRC sessions are prone to numerous attacks that while not dangerous can cause your system to crash.
ISP	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.
LAN	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.
Linux	A version of the UNIX operating system designed to run on IBM Compatible computers.
Logic Bomb	A virus that only activates itself when certain conditions are met. Logic bombs usually damage files or cause other serious problems when they are activated.
MAC	On a local area network (LAN) or other network, the MAC (Media Access Control) address is your 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.
Name Resolution	The allocation of an IP address to a host name. See DNS
NAT	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.
NDIS	Network Driver Interface Specification is a Windows specification for how communication protocol programs (such as TCP/IP) and network device drivers should communicate with each other.
NetBIOS	Network Basic Input / Output System. NetBIOS is an extension of the DOS BIOS that enables a PC to connect to and communicate with a LAN.
Network	Any time you connect 2 or more computers together so that they can share resources, you have a computer network. Connect 2 or more networks together and you have an internet.
NIC	Network Interface Card. A board that provides network communication capabilities to and from a computer system. Also called an adapter.
Node	Any single computer connected to a network
PAC	The box that calls/answers the phone call and relays the PPP frames to the PNS. A PAC must have IP and dial-up capability.
Packet Filter	A filter that scans packets and decides whether to let them through.
PAP	Password Authentication Protocol PAP is a security protocol that requires users to enter a password before accessing a secure system. The user's name and password are sent over the wire to a server, where they are compared with a database of user account names and passwords. This technique is vulnerable to wiretapping (eavesdropping) because the password can be captured and used by someone to log onto the system.
Password Cracker	A program that uses a dictionary of words, phrases, names, etc. to guess a password.
Password encryption	A system of encrypting electronic files using a single key or password. Anyone who knows the password can decrypt the file.
Password Shadowing	The encrypted password is not visible in the password file but stored in a shadow file that is only readable by root. This prevents brute force attacks on the encrypted field to guess the password. see e.g.: <a href="http://whatis.com/shadowpa.htm">http://whatis.com/shadowpa.htm</a>
Penetration	Gaining access to computers or networks by bypassing security programs and passwords.
Phreaking	Breaking into phone or other communication systems. Phreaking sites on the Internet are popular among crackers and other criminals
Ping Attack	An attack that slows down the network until it is unusable. The attacker sends a "ping" command to the network repeatedly to slow it down. See also Denial of Service.
Pirate	Someone who steals or distributes software without paying the legitimate owner for it.

	<p>This category of computer criminal includes several different types of illegal activities Making copies of software for others to use. Distributing pirated software over the Internet or a Bulletin Board System. Receiving or downloading illegal copies of software in any form.</p>
Pirated Software	<p>Software that has been illegally copied, or that is being used in violation of the software's licensing agreement. Pirated software is often distributed through pirate bulletin boards or on the Internet. In the internet underground it is known as Warez.</p>
Plain Text	<p>The opposite of Cipher Text, Plain Text is readable by anyone.</p>
ZyWALL Web Configurator	<p>This is a web-based ZyWALL router (not all) configurator that includes an Internet Access Wizard, Advanced and Firewall (not all ZyWALL models) configurations.</p>
PNS	<p>PPTP Network Server. A PNS must have IP connectivity.</p>
POP	<p>Post Office Protocol. This is a common protocol used for sending, receiving, and delivering mail messages.</p>
Port (H/W)	<p>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.</p>
Port	<p>An Internet port refers to a number that is part of a URL, appearing after a colon (:) right after the domain name. Every service on an Internet server listens on a particular port number on that server. Most services have standard port numbers, e.g. Web servers normally listen on port 80.</p>
POTS	<p>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.</p>
PPP	<p>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.</p>
PPTP	<p>Point-to-Point Tunneling Protocol.</p>
Promiscuous Packet Capture	<p>Actively capturing packet information from a network. Most computers only collect packets specifically addressed to them. Promiscuous packet capture acquires all network traffic it can regardless of where the packets are addressed.</p>
Protocol	<p>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.</p>

Proxy Server	A server that performs network operations in lieu of other systems on the network. Proxy Servers are most often used as part of a firewall to mask the identity of users inside a corporate network yet still provide access to the Internet. When a user connects to a proxy server, via a web browser or other networked application, he submits commands to the proxy server. The server then submits those same commands to the Internet, yet without revealing any information about the system that originally requested the information. Proxy servers are an ideal way to also have all users on a corporate network channel through one point for all external communications. Proxy servers can be configured to block certain kinds of connections and stop some hacks.
PSTN	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 callee.
Public Key Encryption	System of encrypting electronic files using a key pair. The key pair contains a public key used during encryption, and a corresponding private key used during decryption.
PVC	Permanent Virtual Circuit. A PVC is a logical point-to-point circuit between customer sites. PVCs are low-delay circuits because routing decisions do not need to be made along the way. Permanent means that the circuit is preprogrammed by the carrier as a path through the network. It does not need to be set up or torn down for each session.
Reconnaissance	The finding and observation of potential targets for a cracker to attack.
RFC	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.
RIP	Routing Information Protocol is an interior or intra-domain routing protocol that uses the 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.
Router	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.
SAP	In NetWare, the SAP (Service Advertising Protocol) broadcasts information about available services on the network that other network devices can listen to. A server sends out SAP messages every 60 seconds. A server also sends out SAP messages to inform other devices that it is closing down. Workstations use SAP to find services they need on the network.
SATAN	A UNIX program that gathers information on networks and stores it in databases. It is helpful in finding security flaws such as incorrect settings, software bugs and poor policy decisions. It shows network services that are running, the different types of hardware and software on the network, and other information. It was written to help users find

	security flaws in their network systems.
Server	A computer, or a software package, that provides a specific kind of service to client software running on other computers.
Shoulder Surfing	Looking over someone's shoulder to see the numbers they dial on a phone, or the information they enter into a computer.
SNMP	System 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.
Snooping	Passively watching a network for information that could be used to a hacker's advantage, such as passwords. Usually done while Camping Out.
SOCKS	A protocol that handles TCP traffic through proxy servers.
SPAM	Unwanted e-mail, usually in the form of advertisements.
Spoofing	To forge something, such as an IP address. IP Spoofing is a common way for hackers to hide their location and identity
SSL (Secured Socket Layer)	Technology that allows you to send information that only the server can read. SSL allows servers and browsers to encrypt data as they communicate with each other. This makes it very difficult for third parties to understand the communications.
STP	Twisted-pair cable consists of copper-core wires surrounded by an insulator. Two wires are twisted together to form a pair, and the pair form a balanced circuit. The twisting prevents interference problems. STP (shielded twisted-pair) provides protection against external crosstalk.
Straight through Ethernet cable	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 common cable used.
SUA	Single User Account – The ZyWALL's SUA (Single User Account) feature allows multiple user Internet access for the cost of a single ISP account - see also NAT.
TCP	Transmission Control Protocol handles flow control and packet recovery and IP providing basic addressing and packet-forwarding services.
Telnet	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
Tempest	Illegal interception of data from computers and video signals.
Terminal	A device that allows you to send commands to a computer somewhere else. At a minimum, this usually means a keyboard and a display screen and some simple circuitry.
Terminal Software	Software that pretends to be (emulates) a physical terminal and allows you to type commands to a computer somewhere else.

TFTP	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).
Trojan or Trojan Horse	Like the fabled gift to the residents of Troy, a Trojan Horse is an application designed to look innocuous. Yet, when you run the program it installs a virus or memory resident application that can steal passwords, corrupt data, or provide hackers a back door into your computer. Trojan applications are particularly dangerous since they can often run exactly as expected without showing any visible signs of intrusion.
UDP	UDP is a connectionless transport service that dispenses with the reliability services provided by TCP. UDP gives applications a direct interface with IP and the ability to address a particular application process running on a host via a port number without setting up a connection session.
UNIX	A widely used operating system in large networks.
URL	(Uniform Resource Locator) URL is an object on the Internet or an intranet that resides on a host system. Objects include directories and an assortment of file types, including text files, graphics, video, and audio. A URL is the address of an object that is normally typed in the Address field of a Web browser. The URL is basically a pointer to the location of an object.
VPN	Virtual Private Network. These networks use public connections (such as the Internet) to transfer information. That information is usually encrypted for security purposes.
Vulnerability	Point where a system can be attacked.
WAN	Wide Area Network s 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.
War Dialer	A program that automatically dials phone numbers looking for computers on the other end. They catalog numbers so that hackers can call back and try to break in.
Warez	A term that describes Pirated Software on the Internet. Warez include cracked games or other programs that software pirates distribute on the Internet
Wire Tapping	Connecting to a network and monitoring all traffic. Most wire tapping features can only monitor the traffic on their subnet.
Worm	A program that seeks access into other computers. Once a worm penetrates another computer it continues seeking access to other areas. Worms are often equipped with dictionary-based password crackers and other cracker tools that enable them to penetrate more systems. Worms often steal or vandalize computer data.
WWW	(World Wide Web) -- Frequently used when referring to "The Internet", WWW has two major meanings - First, loosely used: the whole constellation of resources that can be accessed using Gopher, FTP, HTTP, telnet, USENET, WAIS and some other tools. Second, the universe of hypertext servers (HTTP servers).



# Index

## A

Action for Matched Packets .....	16-11
Activate The Firewall .....	19-3
Alert Schedule .....	15-5
Application-level Firewalls .....	13-1
AT command .....	10-1
Attack	
Reasons .....	18-2
Attack Alert .....	15-7, 15-8, 15-9, 15-10
Attack Types .....	14-3
Reason .....	14-5
Authentication .....	4-3, 4-4

## B

BackOrifice .....	N
backup .....	10-2
Big Picture	
Filtering, Firewall and NAT .....	14-5
Blocking Time .....	15-8, 15-11
Boot commands .....	11-8
Broadband Access Security Gateway ...i, xxvii, 1-1	
Brute Force Hacking .....	N
Budget Management .....	11-2, 11-3

## C

Cable Modem .....	2-2, 2-3, 13-2
Call Control .....	11-2
Call History .....	11-3, 11-4
Call-Trigerring Packet .....	9-10
CDR .....	9-7
CHAP .....	4-4
CLI Commands .....	G
Command Interpreter Mode .....	11-1
Configuring A POP Custom Port .....	19-8
Console Port .....	2-2, 9-3, 9-5, E
Content Filtering .....	20-1
Categories .....	20-1
Customizing .....	20-5
Days and Times .....	20-1

Exempting Computers .....	20-4
Filter List .....	20-1
Keywords .....	20-6
Log Records .....	20-7
Restrict Web Features .....	20-1
Update List .....	20-3
Custom Ports	
Creating/Editing .....	17-3
Introduction .....	17-1
Customer Support .....	viii
Customized Services .....	17-2

## D

DDNS	
Configuration .....	2-11
Default Permit Log .....	16-6
Denial of Service .....	13-2, 13-3, 14-1, 15-8
Denial of Services	
Thresholds .....	15-10
DestAdd .....	19-10
Destination Address .....	16-2, 16-11
DHCP (Dynamic Host Configuration Protocol) .....	
.....	1-2, 3-1
DHCP Ethernet Setup .....	3-4
DHCP Negotiation .....	19-12
Diagnostic .....	9-10
DNS .....	3-1
Domain Name .....	3-1, 6-14, 9-3, 9-4, P
DoS	
Basics .....	13-3
Types .....	13-4
DoS (Denial of Service) .....	1-1
Dynamic DNS .....	2-10, 2-11
DYNDNS Wildcard .....	2-10

## E

EG 2 - Internet Rule Summary .....	19-12
EG 2 - Local Network Rule Summary .....	19-10
EG 3 - Rule Summary .....	19-14
E-mail Alerts .....	15-5
E-mail Screen .....	19-4

E-mail tab .....15-4  
 Encapsulation  
     PPP over Ethernet.....A  
 Ethernet Encapsulation3-8, 4-1, 4-5, 4-6, 4-10, 6-12, 6-14  
 Example E-mail Log .....15-6  
 Examples .....19-1

*F*

Factory Default .....2-13  
 Filename Conventions.....10-1  
 Filter ..... 2-14, 4-9, 7-1  
     About..... 7-1  
     Applying..... 7-16  
     Configuring ..... 7-4  
     Example..... 7-13  
     Filter log ..... 9-7  
     Generic Filter Rule ..... 7-11  
     NAT ..... 7-15  
     Structure ..... 7-2  
 Filters  
     Executing a Filter Rule..... 7-2  
     Logic Flow of an IP Filter ..... 7-10  
 Firewall  
     Address Type ..... 16-13  
     Alerts ..... 15-3  
     Connection Direction ..... 16-3  
     Creating/Editing Rules ..... 16-10  
     E-mail..... 15-3  
     Guidelines For Enhancing Security ..... 13-9  
     Logs..... 15-4  
     Policies ..... 16-1  
     Rule Logic..... 16-1  
     Rule Precedence ..... 16-4  
     Services ..... 16-7  
     SMT Log ..... 14-2  
     SMT Menus..... 14-1  
     Types ..... 13-1  
     Vs Filters ..... 14-6  
     Web Configurator..... 15-1  
     When To Use..... 14-7  
 Flow Control .....2-3  
 Front Panel LEDs .....2-1  
 FTP File Transfer .....10-9  
 FTP Server..... 1-3, 6-18

*G*

General Setup .....2-9

*H*

Half-Open Sessions ..... 15-8  
 Hidden Menus .....2-5  
 HTTP..... 6-14, 13-1, 13-3, 13-4, Q, T, W  
 HyperTerminal program ..... 10-3

*I*

IANA .....3-2  
 ICMP echo ..... 13-6, 14-3  
 idle timeout ..... 4-3  
 IGMP (Internet Group Multicast Protocol) ..... 3-3  
 Initial Screen ..... 2-4  
 Installation Requirements ..... 2-3  
 Internet access.....3-1  
 Internet Access Setup..... 3-8, 3-9, 6-5, 21-2  
 Internet Assigned Numbers Authority .... See IANA  
 Internet Control Message Protocol (ICMP)13-6, 14-3  
 IP address.....3-2, 3-6  
 IP Address Assignment.....4-6, 4-8  
 IP Alias Setup ..... 3-7  
 IP Multicast ..... 1-2, 3-3  
     Internet Group Management Protocol (IGMP) .... 1-2  
 IP Network Number.....3-2  
 IP Pool .....3-1, 3-6  
 IP Ports ..... 13-4  
 IP Spoofing ..... 13-4, 13-6, 14-2, V  
 IP Static Route .....5-1, 5-2, 5-3

*K*

Key Fields For Configuring Rules ..... 16-2

*L*

LAN Setup ..... 2-13, 2-14, 3-4, 3-5  
 LAN to WAN Rules ..... 16-3  
 LAND .....13-4, 13-5, 14-2  
 Local Network



Rule Summary .....	16-4
log.....	9-5
Log Facility .....	9-7
Log Screen .....	18-1
Login screen.....	15-1

*M*

MAC Address .....	2-13, 21-2
Mail Server .....	15-5
Main Menu.....	2-6
maximum incomplete high.....	15-10
maximum incomplete low .....	15-10
max-incomplete high .....	15-8
max-incomplete low.....	15-8, 15-11
Metric.....	4-6, 4-8, 5-3
My WAN Address .....	4-8

*N*

nailed-up connection .....	4-3
NAT .....	4-6, 4-8, 7-15
Application.....	6-4
Applying NAT in the SMT Menus .....	6-5
Configuring.....	6-7
Definitions .....	6-1
Examples.....	6-15
How NAT Works.....	6-2
Mapping Types .....	6-3
Multiple Servers.....	6-13
Non NAT Friendly Application Programs .....	6-20
Ordering Rules.....	6-10
What NAT does .....	6-1
NetBIOS commands.....	14-3
Network Address Translation (NAT) .	1-2, 6-1, 12-1

*O*

one minute high.....	15-10
one minute ow .....	15-10
one-minute high.....	15-8
Online Registration.....	vii

*P*

Packet Filtering Firewalls .....	13-1
Packet Information .....	18-2
Packet Triggered.....	9-7
Packing List Card .....	xxviii
PAP .....	4-4
Password .....	2-4, 2-9
Ping.....	9-12
Ping of Death .....	13-4
POP3.....	13-3, 13-4
Port Configuration .....	17-4
Power Adapter .....	2-3
PPP log .....	9-7
PPPoE Encapsulation.....	3-8, 3-11, 4-1, 4-3, 4-4, 4-9, 4-10
PPTP Encapsulation .....	1-2, 3-10, 4-4, 4-7
Private.....	3-2, 3-3, 4-7, 4-9, 5-3, W
Private IP Addresses.....	3-2

*R*

Read Me First.....	xxviii
Rear Panel .....	2-2
Related Documentation.....	xxviii
Relay .....	3-6
Remote Management Setup .....	11-7
remote node .....	4-1
Remote Node	
Remote Node Setup .....	2-7
Remote Node Filter .....	4-9
Required fields .....	2-5
Resetting the ZyWALL .....	2-9
Restore Configuration .....	10-4
return address.....	15-5
RIP .....	3-3, 3-6, 4-7, 4-9
ROM File .....	10-6
Rule Checklist .....	16-1
Rule Summary.....	16-4, 16-6, 19-4, 19-6, 19-8, 19-10, 19-11, 19-14

*S*

Safety Instructions.....	F
saving the state .....	13-6
Security In General .....	13-10

Security Ramifications.....	16-2
Send Alerts When Attacked .....	19-7
Server .....	
3-1, 3-9, 4-2, 6-3, 6-4, 6-7, 6-9, 6-12, 6-13, 6-14, 6-16, 6-17, 11-6, N, U, V	
Service .....	vii, 16-2
Service Type .....	3-9, 4-2, 17-4, 21-2
Services Supported .....	16-8
SMT .....	2-4
SMT Menus at a Glance.....	2-9
SMT Error Messages.....	15-6
Smurf.....	13-6, 14-3
SNMP .....	8-1
About.....	8-1
Configuring .....	8-1
Community .....	8-1
Trap.....	8-2
Trusted Host.....	8-2
SNMP ( Simple Network Management Protocol) ...	
.....	1-2
Source & Destination Addresses.....	16-12
Source Address.....	16-2, 16-11
SrcAdd .....	19-9
Stateful Inspection.....	1-1, 13-1, 13-2, 13-6, 13-7
Process .....	13-7
ZyWALL.....	13-8
Structure of this Manual .....	xxvii
SUA (Single User Account).....	See NAT
Subnet Mask ....	3-2, 3-6, 3-10, 4-6, 4-8, 5-3, 16-13
Support Disk.....	xxviii
SYN Flood.....	13-4, 13-5, 14-4
SYN-ACK .....	13-5, 14-4
Syslog .....	19-12
Syslog IP Address .....	9-7
System Information .....	9-1, 9-3, 9-4
System Maintenance.....	9-1, 9-2, 9-3, 9-4, 9-5, 9-6, 9-7, 9-11, 9-12, 10-2, 10-4, 10-5, 10-6, 10-7, 10-8, 10-10, 11-1, 11-2, 11-3, 11-5
System Name.....	2-11
System Status .....	9-1
System Timeout .....	12-2

*T*

TCP Maximum Incomplete.....	15-8, 15-11
TCP Security .....	13-8

TCP/IP .....	
3-1, 3-4, 3-6, 4-6, 4-9, 7-7, 7-8, 7-9, 7-12, 7-15, 12-1, 13-3, 13-4, N, Q, R, S, V	
TCP/IP filter rule.....	7-7
Teardrop .....	13-4, 14-4
telnet .....	12-1
Telnet Configuration.....	12-1
Telnet Under NAT .....	12-1
TFTP File Transfer.....	10-7
The Big Picture .....	14-5
Three-Way Handshake .....	13-5
Threshold Values .....	15-7
Time and Date Setting .....	1-3, 11-4, 11-5, 11-6
Time Zone.....	11-6
Timeout.....	3-11, 3-12, 4-4, 16-14, 16-15
Trace.....	9-5
Traceroute .....	14-4
Troubleshooting the Firewall .....	21-3
Troubleshooting .....	21-1
Internet Access.....	21-3
LAN Interface .....	21-2
WAN Interface .....	21-2

*U*

UDP/ICMP Security .....	13-9
Unicast.....	3-3
UNIX Syslog.....	9-6, 9-7
Upload Firmware.....	10-5
Upper Layer Protocols .....	13-8, 13-9

*V*

View Firewall Log.....	14-4
VT100 .....	2-3

*W*

WAN DHCP .....	9-11, 9-12
WAN Setup .....	2-12, 2-13, 21-2
WAN to LAN Rules .....	16-3
Web Configurator.....	13-9
Welcome screen .....	15-1
www.zyxel.com .....	vii

**X**

xDSL modem..... 1-3, 1-4, 2-3, 2-4, 4-3, 21-2, 21-3  
XMODEM protocol..... 10-2

**Z**

ZyNOS..... 2-13, 6-4, 6-7, 9-3, 9-4, 10-1, 10-2

ZyNOS FW Version..... 9-3, 9-4, 10-1  
ZyWALL Firewall Application.....13-3  
ZyWALL Web Configurator .....  
.....13-2, 13-8, 13-9, 14-2, 15-1, 15-2, 16-2, 19-2  
ZyXEL Limited Warranty  
    Note ..... vii  
ZyXEL website ..... vii  
ZyXEL's Firewall  
    Introduction .....13-2