

# *ZyWALL 5/35/70 Series*

*Internet Security Appliance*

## ***User's Guide***

Version 4.00  
12/2005

The logo for ZyXEL, featuring the word "ZyXEL" in a bold, blue, sans-serif font. The "Zy" is lowercase and the "XEL" is uppercase. The letters are closely spaced and have a slight shadow effect.

# Copyright

Copyright © 2005 by ZyXEL Communications Corporation.

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

Published by ZyXEL Communications Corporation. All rights reserved.

## **Disclaimer**

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

## **Trademarks**

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

# Federal Communications Commission (FCC) Interference Statement

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

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

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

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

- 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.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

## Certifications

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





# Safety Warnings

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

- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel can service the device. Please contact your vendor for further information.
- Connect the power cord to the right supply voltage (110V AC in North America or 230V AC in Europe).
- Place connecting cables carefully so that no one will step on them or stumble over them. Do NOT allow anything to rest on the power cord and do NOT locate the product where anyone can walk on the power cord.
- If you wall mount your device, make sure that no electrical, gas or water pipes will be damaged.
- Do NOT install nor use your device during a thunderstorm. There may be a remote risk of electric shock from lightning.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Make sure to connect the cables to the correct ports.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Do NOT store things on the device.
- Connect ONLY suitable accessories to the device.

# ZyXEL Limited Warranty

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

## Note

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

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

# Customer Support

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

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

METHOD	SUPPORT E-MAIL	TELEPHONE <sup>A</sup>	WEB SITE	REGULAR MAIL
LOCATION	SALES E-MAIL	FAX	FTP SITE	
CORPORATE HEADQUARTERS (WORLDWIDE)	support@zyxel.com.tw	+886-3-578-3942	www.zyxel.com www.europe.zyxel.com	ZyXEL Communications Corp. 6 Innovation Road II Science Park Hsinchu 300 Taiwan
	sales@zyxel.com.tw	+886-3-578-2439	ftp.zyxel.com ftp.europe.zyxel.com	
CZECH REPUBLIC	info@cz.zyxel.com	+420-241-091-350	www.zyxel.cz	ZyXEL Communications Czech s.r.o. Modranská 621 143 01 Praha 4 - Modrany Ceská Republika
	info@cz.zyxel.com	+420-241-091-359		
DENMARK	support@zyxel.dk	+45-39-55-07-00	www.zyxel.dk	ZyXEL Communications A/S Columbusvej 2860 Soeborg Denmark
	sales@zyxel.dk	+45-39-55-07-07		
FINLAND	support@zyxel.fi	+358-9-4780-8411	www.zyxel.fi	ZyXEL Communications Oy Malminkaari 10 00700 Helsinki Finland
	sales@zyxel.fi	+358-9-4780 8448		
FRANCE	info@zyxel.fr	+33-4-72-52-97-97	www.zyxel.fr	ZyXEL France 1 rue des Vergers Bat. 1 / C 69760 Limonest France
		+33-4-72-52-19-20		
GERMANY	support@zyxel.de	+49-2405-6909-0	www.zyxel.de	ZyXEL Deutschland GmbH. Adenauerstr. 20/A2 D-52146 Wuerselen Germany
	sales@zyxel.de	+49-2405-6909-99		
HUNGARY	support@zyxel.hu	+36-1-3361649	www.zyxel.hu	ZyXEL Hungary 48, Zoldlomb Str. H-1025, Budapest Hungary
	info@zyxel.hu	+36-1-3259100		
KAZAKHSTAN	http://zyxel.kz/support	+7-3272-590-698	www.zyxel.kz	ZyXEL Kazakhstan 43, Dostyk ave., Office 414 Dostyk Business Centre 050010, Almaty Republic of Kazakhstan
	sales@zyxel.kz	+7-3272-590-689		
NORTH AMERICA	support@zyxel.com	1-800-255-4101 +1-714-632-0882	www.us.zyxel.com	ZyXEL Communications Inc. 1130 N. Miller St. Anaheim CA 92806-2001 U.S.A.
	sales@zyxel.com	+1-714-632-0858	ftp.us.zyxel.com	
NORWAY	support@zyxel.no	+47-22-80-61-80	www.zyxel.no	ZyXEL Communications A/S Niils Hansens vei 13 0667 Oslo Norway
	sales@zyxel.no	+47-22-80-61-81		

METHOD	SUPPORT E-MAIL	TELEPHONE <sup>A</sup>	WEB SITE	REGULAR MAIL
	SALES E-MAIL	FAX	FTP SITE	
POLAND	info@pl.zyxel.com	+48-22-5286603	www.pl.zyxel.com	ZyXEL Communications ul.Emilli Plater 53 00-113 Warszawa Poland
		+48-22-5206701		
RUSSIA	http://zyxel.ru/support	+7-095-542-89-29	www.zyxel.ru	ZyXEL Russia Ostrovityanova 37a Str. Moscow, 117279 Russia
	sales@zyxel.ru	+7-095-542-89-25		
SPAIN	support@zyxel.es	+34-902-195-420	www.zyxel.es	ZyXEL Communications Alejandro Villegas 33 1º, 28043 Madrid Spain
	sales@zyxel.es	+34-913-005-345		
SWEDEN	support@zyxel.se	+46-31-744-7700	www.zyxel.se	ZyXEL Communications A/S Sjöporten 4, 41764 Göteborg Sweden
	sales@zyxel.se	+46-31-744-7701		
UKRAINE	support@ua.zyxel.com	+380-44-247-69-78	www.ua.zyxel.com	ZyXEL Ukraine 13, Pimonenko Str. Kiev, 04050 Ukraine
	sales@ua.zyxel.com	+380-44-494-49-32		
UNITED KINGDOM	support@zyxel.co.uk	+44-1344 303044 08707 555779 (UK only)	www.zyxel.co.uk	ZyXEL Communications UK Ltd., 11 The Courtyard, Eastern Road, Bracknell, Berkshire, RG12 2XB, United Kingdom (UK)
	sales@zyxel.co.uk	+44-1344 303034	ftp.zyxel.co.uk	

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



# Table of Contents

<b>Copyright .....</b>	<b>2</b>
<b>Federal Communications Commission (FCC) Interference Statement .....</b>	<b>3</b>
<b>Safety Warnings .....</b>	<b>5</b>
<b>ZyXEL Limited Warranty .....</b>	<b>6</b>
<b>Customer Support.....</b>	<b>7</b>
<b>Table of Contents .....</b>	<b>10</b>
<b>List of Figures .....</b>	<b>32</b>
<b>List of Tables .....</b>	<b>44</b>
<b>Preface .....</b>	<b>52</b>
<b>Chapter 1</b>	
<b>Getting to Know Your ZyWALL .....</b>	<b>54</b>
1.1 ZyWALL Internet Security Appliance Overview .....	54
1.2 ZyWALL Features .....	54
1.2.1 Physical Features .....	55
1.2.2 Non-Physical Features .....	56
1.3 Applications for the ZyWALL .....	62
1.3.1 Secure Broadband Internet Access via Cable or DSL Modem .....	62
1.3.2 VPN Application .....	62
1.3.3 Front Panel LEDs .....	63
<b>Chapter 2</b>	
<b>Introducing the Web Configurator.....</b>	<b>66</b>
2.1 Web Configurator Overview .....	66
2.2 Accessing the ZyWALL Web Configurator .....	66
2.3 Resetting the ZyWALL .....	67
2.3.1 Procedure To Use The Reset Button .....	68
2.3.2 Uploading a Configuration File Via Console Port .....	68
2.4 Navigating the ZyWALL Web Configurator .....	68
2.4.1 Router Mode.....	69
2.4.2 Bridge Mode .....	71
2.4.3 Navigation Panel .....	74
2.4.4 System Statistics.....	79

2.4.5 Show Statistics: Line Chart .....	80
2.4.6 DHCP Table Screen .....	81
2.4.7 VPN Status .....	82
<b>Chapter 3</b>	
<b>Wizard Setup .....</b>	<b>84</b>
3.1 Wizard Setup Overview .....	84
3.2 Internet Access .....	84
3.2.1 ISP Parameters .....	84
3.2.1.1 Ethernet .....	84
3.2.1.2 PPPoE Encapsulation .....	86
3.2.1.3 PPTP Encapsulation .....	87
3.2.2 Internet Access Wizard: Second Screen .....	89
3.2.3 Internet Access Wizard: Registration.....	90
3.3 VPN Wizard Gateway Setting .....	93
3.4 VPN Wizard Network Setting .....	94
3.5 VPN Wizard IKE Tunnel Setting (IKE Phase 1) .....	96
3.6 VPN Wizard IPSec Setting (IKE Phase 2) .....	98
3.7 VPN Wizard Status Summary .....	99
3.8 VPN Wizard Setup Complete .....	102
<b>Chapter 4</b>	
<b>Registration .....</b>	<b>104</b>
4.1 myZyXEL.com overview .....	104
4.1.1 Subscription Services Available on the ZyWALL .....	104
4.2 Registration .....	105
4.3 Service .....	107
<b>Chapter 5</b>	
<b>LAN Screens .....</b>	<b>110</b>
5.1 LAN Overview .....	110
5.2 DHCP Setup .....	110
5.2.1 IP Pool Setup .....	110
5.3 LAN TCP/IP .....	110
5.3.1 Factory LAN Defaults .....	110
5.3.2 IP Address and Subnet Mask .....	111
5.3.3 RIP Setup .....	111
5.3.4 Multicast .....	112
5.4 DNS Servers .....	112
5.5 LAN .....	112
5.6 LAN Static DHCP .....	115
5.7 LAN IP Alias .....	116
5.8 LAN Port Roles .....	118

<b>Chapter 6</b>	
<b>Bridge Screens</b>	<b>122</b>
6.1 Bridge Loop	122
6.2 Spanning Tree Protocol (STP)	122
6.2.1 Rapid STP	123
6.2.2 STP Terminology	123
6.2.3 How STP Works	123
6.2.4 STP Port States	124
6.3 Bridge	124
6.4 Bridge Port Roles	126
<b>Chapter 7</b>	
<b>WAN Screens</b>	<b>130</b>
7.1 WAN Overview	130
7.2 Multiple WAN	130
7.3 Load Balancing Introduction	131
7.4 Load Balancing Algorithms	131
7.4.1 Least Load First	131
7.4.1.1 Example 1	132
7.4.1.2 Example 2	132
7.4.2 Weighted Round Robin	133
7.4.3 Spillover	133
7.5 TCP/IP Priority (Metric)	134
7.6 WAN General	134
7.7 Configuring Load Balancing	137
7.7.1 Least Load First	138
7.7.2 Weighted Round Robin	139
7.7.3 Spillover	139
7.8 WAN Route	140
7.9 WAN IP Address Assignment	142
7.10 DNS Server Address Assignment	142
7.11 WAN MAC Address	143
7.12 WAN	143
7.12.1 WAN Ethernet Encapsulation	143
7.12.2 PPPoE Encapsulation	146
7.12.3 PPTP Encapsulation	150
7.13 Traffic Redirect	153
7.14 Configuring Traffic Redirect	154
7.15 Configuring Dial Backup	155
7.16 Advanced Modem Setup	159
7.16.1 AT Command Strings	159
7.16.2 DTR Signal	159
7.16.3 Response Strings	159



7.17 Configuring Advanced Modem Setup .....	159
<b>Chapter 8</b>	
<b>DMZ Screens .....</b>	<b>162</b>
8.1 DMZ .....	162
8.2 Configuring DMZ .....	162
8.3 DMZ Static DHCP .....	165
8.4 DMZ IP Alias .....	167
8.5 DMZ Public IP Address Example .....	168
8.6 DMZ Private and Public IP Address Example .....	169
8.7 DMZ Port Roles .....	170
<b>Chapter 9</b>	
<b>Wireless LAN .....</b>	<b>174</b>
9.1 Wireless LAN Introduction .....	174
9.1.1 Additional Installation Requirements for Using 802.1x .....	174
9.2 Configuring WLAN .....	174
9.3 WLAN Static DHCP .....	177
9.4 WLAN IP Alias .....	178
9.5 WLAN Port Roles .....	180
9.6 Wireless Security .....	182
9.6.1 Encryption .....	183
9.6.2 Authentication .....	183
9.6.3 Restricted Access .....	184
9.6.4 Hide ZyWALL Identity .....	184
9.7 Security Parameters Summary .....	184
9.8 WEP Encryption .....	184
9.9 802.1x Overview .....	185
9.9.1 Introduction to RADIUS .....	185
9.9.1.1 Types of RADIUS Messages .....	185
9.9.2 EAP Authentication Overview .....	186
9.10 Dynamic WEP Key Exchange .....	186
9.11 Introduction to WPA .....	187
9.11.1 User Authentication .....	187
9.11.2 Encryption .....	187
9.12 WPA-PSK Application Example .....	188
9.13 Introduction to RADIUS .....	189
9.14 WPA with RADIUS Application Example .....	189
9.15 Wireless Client WPA Supplicants .....	190
9.16 Wireless Card .....	190
9.16.1 Static WEP .....	192
9.16.2 WPA-PSK .....	193
9.16.3 WPA .....	195

9.16.4 IEEE 802.1x + Dynamic WEP .....	196
9.16.5 IEEE 802.1x + Static WEP .....	197
9.16.6 IEEE 802.1x + No WEP .....	198
9.16.7 No Access 802.1x + Static WEP .....	199
9.16.8 No Access 802.1x + No WEP .....	200
9.17 MAC Filter .....	200
<b>Chapter 10</b>	
<b>Firewalls.....</b>	<b>202</b>
10.1 Firewall Overview .....	202
10.2 Types of Firewalls .....	202
10.2.1 Packet Filtering Firewalls .....	202
10.2.2 Application-level Firewalls .....	202
10.2.3 Stateful Inspection Firewalls .....	203
10.3 Introduction to ZyXEL's Firewall .....	203
10.4 Denial of Service .....	204
10.4.1 Basics .....	204
10.4.2 Types of DoS Attacks .....	205
10.4.2.1 ICMP Vulnerability .....	207
10.4.2.2 Illegal Commands (NetBIOS and SMTP) .....	207
10.4.2.3 Traceroute .....	208
10.5 Stateful Inspection .....	208
10.5.1 Stateful Inspection Process .....	209
10.5.2 Stateful Inspection and the ZyWALL .....	210
10.5.3 TCP Security .....	210
10.5.4 UDP/ICMP Security .....	211
10.5.5 Upper Layer Protocols .....	211
10.6 Guidelines For Enhancing Security With Your Firewall .....	212
10.7 Packet Filtering Vs Firewall .....	212
10.7.1 Packet Filtering: .....	212
10.7.1.1 When To Use Filtering .....	212
10.7.2 Firewall .....	213
10.7.2.1 When To Use The Firewall .....	213
<b>Chapter 11</b>	
<b>Firewall Screens.....</b>	<b>214</b>
11.1 Access Methods .....	214
11.2 Firewall Policies Overview .....	214
11.3 Rule Logic Overview .....	216
11.3.1 Rule Checklist .....	216
11.3.2 Security Ramifications .....	216
11.3.3 Key Fields For Configuring Rules .....	216
11.3.3.1 Action .....	216

11.3.3.2 Service .....	217
11.3.3.3 Source Address .....	217
11.3.3.4 Destination Address .....	217
11.4 Connection Direction Examples .....	217
11.4.1 LAN To WAN Rules .....	217
11.4.2 WAN To LAN Rules .....	218
11.5 Alerts .....	218
11.6 Firewall Default Rule (Router Mode) .....	219
11.7 Firewall Default Rule (Bridge Mode) .....	220
11.8 Firewall Rule Summary .....	222
11.8.1 Firewall Edit Rule .....	223
11.9 Anti-Probing .....	226
11.10 Firewall Threshold .....	227
11.10.1 Threshold Values .....	227
11.10.2 Half-Open Sessions .....	227
11.10.2.1 TCP Maximum Incomplete and Blocking Time .....	228
11.11 Service .....	230
11.11.1 Firewall Edit Custom Service .....	232
11.11.2 Predefined Services .....	233
11.12 Example Firewall Rule .....	235
<b>Chapter 12</b>	
<b>Intrusion Detection and Prevention (IDP) .....</b>	<b>240</b>
12.1 Introduction to IDP .....	240
12.1.1 Firewalls and Intrusions .....	240
12.1.2 IDS and IDP .....	241
12.1.3 Host IDP .....	241
12.1.4 Network IDP .....	241
12.1.5 Example Intrusions .....	242
12.1.5.1 SQL Slammer Worm .....	242
12.1.5.2 Blaster W32.Worm .....	242
12.1.5.3 Nimda .....	242
12.1.5.4 MyDoom .....	243
12.1.6 ZyWALL IDP .....	243
<b>Chapter 13</b>	
<b>Configuring IDP .....</b>	<b>244</b>
13.1 Overview .....	244
13.1.1 Interfaces .....	244
13.2 General Setup .....	245
13.3 IDP Signatures .....	246
13.3.1 Attack Types .....	246
13.3.2 Intrusion Severity .....	248

13.3.3 Signature Actions .....	248
13.3.4 Configuring IDP Signatures .....	249
13.3.5 Query View .....	251
13.3.5.1 Query Example 1 .....	251
13.3.5.2 Query Example 2 .....	253
13.4 Update .....	254
13.4.1 mySecurity Zone .....	254
13.4.2 Configuring IDP Update .....	255
13.5 Backup and Restore .....	257
<b>Chapter 14</b>	
<b>Anti-Virus .....</b>	<b>258</b>
14.1 Anti-Virus Overview .....	258
14.1.1 Types of Computer Viruses .....	258
14.1.2 Computer Virus Infection and Prevention .....	258
14.1.3 Types of Anti-Virus Scanner .....	259
14.2 Introduction to the ZyWALL Anti-Virus Scanner .....	259
14.2.1 How the ZyWALL Anti-Virus Scanner Works .....	260
14.2.2 Notes About the ZyWALL Anti-Virus .....	260
14.3 General Anti-Virus Setup .....	261
14.4 Signature Update .....	262
14.4.1 mySecurity Zone .....	263
14.4.2 Configuring Anti-virus Update .....	263
<b>Chapter 15</b>	
<b>Anti-Spam .....</b>	<b>266</b>
15.1 Anti-Spam Overview .....	266
15.1.1 Anti-Spam External Database .....	266
15.1.1.1 SpamBulk Engine .....	267
15.1.1.2 SpamRepute Engine .....	267
15.1.1.3 SpamContent Engine .....	267
15.1.1.4 SpamTricks Engine .....	268
15.1.2 Spam Threshold .....	268
15.1.3 Phishing .....	268
15.1.4 Whitelist .....	269
15.1.5 Blacklist .....	269
15.1.6 SMTP and POP3 .....	269
15.1.7 MIME Headers .....	270
15.2 Anti-Spam General Screen .....	270
15.3 Anti-Spam External DB Screen .....	271
15.4 Anti-Spam Lists Screen .....	273
15.5 Anti-Spam Rule Edit Screen .....	275

<b>Chapter 16</b>	
<b>Content Filtering Screens .....</b>	<b>278</b>
16.1 Content Filtering Overview .....	278
16.1.1 Restrict Web Features .....	278
16.1.2 Create a Filter List .....	278
16.1.3 Customize Web Site Access .....	278
16.2 Content Filter General .....	278
16.3 Content Filtering with an External Database .....	280
16.4 Content Filter Categories .....	281
16.5 Content Filter Customization .....	288
16.6 Customizing Keyword Blocking URL Checking .....	290
16.6.1 Domain Name or IP Address URL Checking .....	290
16.6.2 Full Path URL Checking .....	290
16.6.3 File Name URL Checking .....	290
16.7 Content Filtering Cache .....	291
<b>Chapter 17</b>	
<b>Content Filtering Reports .....</b>	<b>294</b>
17.1 Checking Content Filtering Activation .....	294
17.2 Viewing Content Filtering Reports .....	294
17.3 Web Site Submission .....	299
<b>Chapter 18</b>	
<b>Introduction to IPSec .....</b>	<b>302</b>
18.1 VPN Overview .....	302
18.1.1 IPSec .....	302
18.1.2 Security Association .....	302
18.1.3 Other Terminology .....	302
18.1.3.1 Encryption .....	302
18.1.3.2 Data Confidentiality .....	303
18.1.3.3 Data Integrity .....	303
18.1.3.4 Data Origin Authentication .....	303
18.1.4 VPN Applications .....	303
18.1.4.1 Linking Two or More Private Networks Together .....	303
18.1.4.2 Accessing Network Resources When NAT Is Enabled .....	303
18.1.4.3 Unsupported IP Applications .....	303
18.2 IPSec Architecture .....	304
18.2.1 IPSec Algorithms .....	304
18.2.2 Key Management .....	304
18.3 Encapsulation .....	304
18.3.1 Transport Mode .....	305
18.3.2 Tunnel Mode .....	305
18.4 IPSec and NAT .....	305

<b>Chapter 19</b>	
<b>VPN Screens</b>	<b>308</b>
19.1 VPN/IPSec Overview	308
19.2 IPSec Algorithms	308
19.2.1 AH (Authentication Header) Protocol	308
19.2.2 ESP (Encapsulating Security Payload) Protocol	308
19.3 My ZyWALL	309
19.4 Remote Gateway Address	309
19.4.1 Dynamic Remote Gateway Address	310
19.5 Nailed Up	310
19.6 NAT Traversal	310
19.6.1 NAT Traversal Configuration	311
19.7 ID Type and Content	311
19.7.1 ID Type and Content Examples	312
19.8 IKE Phases	313
19.8.1 Negotiation Mode	314
19.8.2 Pre-Shared Key	314
19.8.3 Diffie-Hellman (DH) Key Groups	315
19.8.4 Perfect Forward Secrecy (PFS)	315
19.9 X-Auth (Extended Authentication)	315
19.9.1 Authentication Server	315
19.10 VPN Rules (IKE)	316
19.11 VPN Rules (IKE) Gateway Policy Edit	318
19.12 VPN Rules (IKE): Network Policy Edit	324
19.13 VPN Rules (IKE): Network Policy Move	328
19.14 VPN Rules (Manual)	329
19.15 VPN Rules (Manual): Edit	331
19.15.1 Security Parameter Index (SPI)	331
19.16 VPN SA Monitor	335
19.17 VPN Global Setting	336
19.18 Telecommuter VPN/IPSec Examples	337
19.18.1 Telecommuters Sharing One VPN Rule Example	337
19.18.2 Telecommuters Using Unique VPN Rules Example	338
19.19 VPN and Remote Management	340
<b>Chapter 20</b>	
<b>Certificates</b>	<b>342</b>
20.1 Certificates Overview	342
20.1.1 Advantages of Certificates	343
20.2 Self-signed Certificates	343
20.3 Configuration Summary	343
20.4 My Certificates	344
20.5 My Certificate Import	346

20.5.1 Certificate File Formats .....	346
20.6 My Certificate Create .....	347
20.7 My Certificate Details .....	350
20.8 Trusted CAs .....	353
20.9 Trusted CA Import .....	355
20.10 Trusted CA Details .....	356
20.11 Trusted Remote Hosts .....	359
20.12 Verifying a Trusted Remote Host's Certificate .....	361
20.12.1 Trusted Remote Host Certificate Fingerprints .....	361
20.13 Trusted Remote Hosts Import .....	362
20.14 Trusted Remote Host Certificate Details .....	363
20.15 Directory Servers .....	366
20.16 Directory Server Add or Edit .....	367

## **Chapter 21**

### **Authentication Server ..... 370**

21.1 Authentication Server Overview .....	370
21.1.1 Local User Database .....	370
21.1.2 RADIUS .....	370
21.2 Local User Database .....	370
21.3 RADIUS .....	372

## **Chapter 22**

### **Network Address Translation (NAT) ..... 374**

22.1 NAT Overview .....	374
22.1.1 NAT Definitions .....	374
22.1.2 What NAT Does .....	375
22.1.3 How NAT Works .....	375
22.1.4 NAT Application .....	376
22.1.5 Port Restricted Cone NAT .....	377
22.1.6 NAT Mapping Types .....	377
22.2 Using NAT .....	378
22.2.1 SUA (Single User Account) Versus NAT .....	378
22.3 NAT Overview .....	379
22.4 NAT Address Mapping .....	380
22.4.1 NAT Address Mapping Edit .....	382
22.5 Port Forwarding .....	383
22.5.1 Default Server IP Address .....	384
22.5.2 Port Forwarding: Services and Port Numbers .....	384
22.5.3 Configuring Servers Behind Port Forwarding (Example) .....	384
22.5.4 NAT and Multiple WAN .....	385
22.5.5 Port Translation .....	385
22.6 Port Forwarding .....	386

22.7 Port Triggering .....	388
<b>Chapter 23</b>	
<b>Static Route .....</b>	<b>392</b>
23.1 IP Static Route .....	392
23.2 IP Static Route .....	392
23.2.1 IP Static Route Edit .....	394
<b>Chapter 24</b>	
<b>Policy Route .....</b>	<b>396</b>
24.1 Policy Route .....	396
24.2 Benefits .....	396
24.3 Routing Policy .....	396
24.4 IP Routing Policy Setup .....	397
24.5 Policy Route Edit .....	398
<b>Chapter 25</b>	
<b>Bandwidth Management .....</b>	<b>402</b>
25.1 Bandwidth Management Overview .....	402
25.2 Bandwidth Classes and Filters .....	402
25.3 Proportional Bandwidth Allocation .....	403
25.4 Application-based Bandwidth Management .....	403
25.5 Subnet-based Bandwidth Management .....	403
25.6 Application and Subnet-based Bandwidth Management .....	404
25.7 Scheduler .....	404
25.7.1 Priority-based Scheduler .....	404
25.7.2 Fairness-based Scheduler .....	404
25.7.3 Maximize Bandwidth Usage .....	404
25.7.4 Reserving Bandwidth for Non-Bandwidth Class Traffic .....	405
25.7.5 Maximize Bandwidth Usage Example .....	405
25.7.5.1 Priority-based Allotment of Unused and Unbudgeted Bandwidth	406
25.7.5.2 Fairness-based Allotment of Unused and Unbudgeted Bandwidth	406
25.8 Bandwidth Borrowing .....	407
25.8.1 Bandwidth Borrowing Example .....	407
25.9 Maximize Bandwidth Usage With Bandwidth Borrowing .....	408
25.10 Configuring Summary .....	408
25.11 Configuring Class Setup .....	410
25.11.1 Bandwidth Manager Class Configuration .....	411
25.11.2 Bandwidth Management Statistics .....	414
25.12 Configuring Monitor .....	415



<b>Chapter 26</b>	
<b>DNS</b> .....	<b>418</b>
26.1 DNS Overview .....	418
26.2 DNS Server Address Assignment .....	418
26.3 DNS Servers .....	418
26.4 Address Record .....	419
26.4.1 DNS Wildcard .....	419
26.5 Name Server Record .....	419
26.5.1 Private DNS Server .....	419
26.6 System Screen .....	420
26.6.1 Adding an Address Record .....	422
26.6.2 Inserting a Name Server record .....	423
26.7 DNS Cache .....	424
26.8 Configure DNS Cache .....	425
26.9 Configuring DNS DHCP .....	426
26.10 Dynamic DNS .....	428
26.10.1 DYNDNS Wildcard .....	428
26.10.2 High Availability .....	428
26.11 Configuring Dynamic DNS .....	428
<b>Chapter 27</b>	
<b>Remote Management</b> .....	<b>432</b>
27.1 Remote Management Overview .....	432
27.1.1 Remote Management Limitations .....	432
27.1.2 System Timeout .....	433
27.2 Introduction to HTTPS .....	433
27.3 WWW .....	434
27.4 HTTPS Example .....	436
27.4.1 Internet Explorer Warning Messages .....	436
27.4.2 Netscape Navigator Warning Messages .....	437
27.4.3 Avoiding the Browser Warning Messages .....	438
27.4.4 Login Screen .....	438
27.5 SSH .....	441
27.6 How SSH works .....	441
27.7 SSH Implementation on the ZyWALL .....	442
27.7.1 Requirements for Using SSH .....	443
27.8 Configuring SSH .....	443
27.9 Secure Telnet Using SSH Examples .....	444
27.9.1 Example 1: Microsoft Windows .....	444
27.9.2 Example 2: Linux .....	444
27.10 Secure FTP Using SSH Example .....	445
27.11 Telnet .....	446
27.12 Configuring TELNET .....	446

27.13 FTP .....	447
27.14 SNMP .....	448
27.14.1 Supported MIBs .....	450
27.14.2 SNMP Traps .....	450
27.14.3 REMOTE MANAGEMENT: SNMP .....	450
27.15 DNS .....	452
27.16 Introducing Vantage CNM .....	452
27.17 Configuring CNM .....	453

## Chapter 28

### UPnP..... 456

28.1 Universal Plug and Play Overview .....	456
28.1.1 How Do I Know If I'm Using UPnP? .....	456
28.1.2 NAT Traversal .....	456
28.1.3 Cautions with UPnP .....	456
28.1.4 UPnP and ZyXEL .....	457
28.2 Configuring UPnP .....	457
28.3 Displaying UPnP Port Mapping .....	458
28.4 Installing UPnP in Windows Example .....	459
28.4.1 Installing UPnP in Windows Me .....	460
28.4.2 Installing UPnP in Windows XP .....	461
28.5 Using UPnP in Windows XP Example .....	461
28.5.1 Auto-discover Your UPnP-enabled Network Device .....	462
28.5.2 Web Configurator Easy Access .....	463

## Chapter 29

### ALG Screen..... 466

29.1 ALG Introduction .....	466
29.1.1 ALG and NAT .....	466
29.1.2 ALG and the Firewall .....	466
29.1.3 ALG and Multiple WAN .....	466
29.2 FTP .....	467
29.3 H.323 .....	467
29.4 RTP .....	467
29.4.1 H.323 ALG Details .....	467
29.5 SIP .....	469
29.5.1 STUN .....	469
29.5.2 SIP ALG Details .....	469
29.5.3 SIP Signaling Session Timeout .....	470
29.5.4 SIP Audio Session Timeout .....	470
29.6 ALG Screen .....	470

<b>Chapter 30</b>	
<b>Logs Screens</b>	<b>472</b>
30.1 Configuring View Log	472
30.2 Log Description Example	473
30.2.1 Certificate Not Trusted Log Note	474
30.3 Configuring Log Settings	475
30.4 Configuring Reports	478
30.4.1 Viewing Web Site Hits	480
30.4.2 Viewing Protocol/Port	480
30.4.3 Viewing Host IP Address	482
30.4.4 Reports Specifications	483
<b>Chapter 31</b>	
<b>Maintenance</b>	<b>484</b>
31.1 Maintenance Overview	484
31.2 General Setup	484
31.2.1 General Setup and System Name	484
31.2.2 General Setup	484
31.3 Configuring Password	485
31.4 Time and Date	486
31.5 Pre-defined NTP Time Servers List	489
31.5.1 Resetting the Time	489
31.5.2 Time Server Synchronization	489
31.6 Introduction To Transparent Bridging	491
31.7 Transparent Firewalls	491
31.8 Configuring Device Mode (Router)	492
31.9 Configuring Device Mode (Bridge)	493
31.10 F/W Upload Screen	494
31.11 Backup and Restore	496
31.11.1 Backup Configuration	497
31.11.2 Restore Configuration	497
31.11.3 Back to Factory Defaults	499
31.12 Restart Screen	499
<b>Chapter 32</b>	
<b>Introducing the SMT</b>	<b>500</b>
32.1 Introduction to the SMT	500
32.2 Accessing the SMT via the Console Port	500
32.2.1 Initial Screen	500
32.2.2 Entering the Password	501
32.3 Navigating the SMT Interface	501
32.3.1 Main Menu	502
32.3.2 SMT Menus Overview	504

32.4 Changing the System Password .....	506
32.5 Resetting the ZyWALL .....	507
<b>Chapter 33</b>	
<b>SMT Menu 1 - General Setup.....</b>	<b>508</b>
33.1 Introduction to General Setup .....	508
33.2 Configuring General Setup .....	508
33.2.1 Configuring Dynamic DNS .....	510
33.2.1.1 Editing DDNS Host .....	510
<b>Chapter 34</b>	
<b>WAN and Dial Backup Setup.....</b>	<b>514</b>
34.1 Introduction to WAN and Dial Backup Setup .....	514
34.2 WAN Setup .....	514
34.3 Dial Backup .....	515
34.4 Configuring Dial Backup in Menu 2 .....	515
34.5 Advanced WAN Setup .....	516
34.6 Remote Node Profile (Backup ISP) .....	518
34.7 Editing PPP Options .....	520
34.8 Editing TCP/IP Options .....	521
34.9 Editing Login Script .....	523
34.10 Remote Node Filter .....	525
<b>Chapter 35</b>	
<b>LAN Setup.....</b>	<b>526</b>
35.1 Introduction to LAN Setup .....	526
35.2 Accessing the LAN Menus .....	526
35.3 LAN Port Filter Setup .....	526
35.4 TCP/IP and DHCP Ethernet Setup Menu .....	527
35.4.1 IP Alias Setup .....	530
<b>Chapter 36</b>	
<b>Internet Access .....</b>	<b>532</b>
36.1 Introduction to Internet Access Setup .....	532
36.2 Ethernet Encapsulation .....	532
36.3 Configuring the PPTP Client .....	534
36.4 Configuring the PPPoE Client .....	534
36.5 Basic Setup Complete .....	535
<b>Chapter 37</b>	
<b>DMZ Setup .....</b>	<b>536</b>
37.1 Configuring DMZ Setup .....	536
37.2 DMZ Port Filter Setup .....	536

37.3 TCP/IP Setup .....	536
37.3.1 IP Address .....	537
37.3.2 IP Alias Setup .....	538
<b>Chapter 38</b>	
<b>Route Setup .....</b>	<b>540</b>
38.1 Configuring Route Setup .....	540
38.2 Route Assessment .....	540
38.3 Traffic Redirect .....	541
38.4 Route Failover .....	542
<b>Chapter 39</b>	
<b>Wireless Setup .....</b>	<b>544</b>
39.1 Wireless LAN Setup .....	544
39.1.1 MAC Address Filter Setup .....	546
39.2 TCP/IP Setup .....	547
39.2.1 IP Address .....	547
39.2.2 IP Alias Setup .....	548
<b>Chapter 40</b>	
<b>Remote Node Setup .....</b>	<b>550</b>
40.1 Introduction to Remote Node Setup .....	550
40.2 Remote Node Setup .....	550
40.3 Remote Node Profile Setup .....	551
40.3.1 Ethernet Encapsulation .....	551
40.3.2 PPPoE Encapsulation .....	553
40.3.2.1 Outgoing Authentication Protocol .....	553
40.3.2.2 Nailed-Up Connection .....	553
40.3.2.3 Metric .....	554
40.3.3 PPTP Encapsulation .....	554
40.4 Edit IP .....	555
40.5 Remote Node Filter .....	557
40.6 Traffic Redirect .....	558
<b>Chapter 41</b>	
<b>IP Static Route Setup .....</b>	<b>560</b>
41.1 IP Static Route Setup .....	560
<b>Chapter 42</b>	
<b>Network Address Translation (NAT) .....</b>	<b>562</b>
42.1 Using NAT .....	562
42.1.1 SUA (Single User Account) Versus NAT .....	562
42.1.2 Applying NAT .....	562

42.2 NAT Setup .....	564
42.2.1 Address Mapping Sets .....	565
42.2.1.1 SUA Address Mapping Set .....	565
42.2.1.2 User-Defined Address Mapping Sets .....	566
42.2.1.3 Ordering Your Rules .....	567
42.3 Configuring a Server behind NAT .....	569
42.4 General NAT Examples .....	572
42.4.1 Internet Access Only .....	572
42.4.2 Example 2: Internet Access with an Default Server .....	574
42.4.3 Example 3: Multiple Public IP Addresses With Inside Servers .....	574
42.4.4 Example 4: NAT Unfriendly Application Programs .....	578
42.5 Trigger Port Forwarding .....	579
42.5.1 Two Points To Remember About Trigger Ports .....	579
<b>Chapter 43</b>	
<b>Introducing the ZyWALL Firewall .....</b>	<b>582</b>
43.1 Using ZyWALL SMT Menus .....	582
43.1.1 Activating the Firewall .....	582
<b>Chapter 44</b>	
<b>Filter Configuration .....</b>	<b>584</b>
44.1 Introduction to Filters .....	584
44.1.1 The Filter Structure of the ZyWALL .....	585
44.2 Configuring a Filter Set .....	587
44.2.1 Configuring a Filter Rule .....	588
44.2.2 Configuring a TCP/IP Filter Rule .....	589
44.2.3 Configuring a Generic Filter Rule .....	591
44.3 Example Filter .....	593
44.4 Filter Types and NAT .....	595
44.5 Firewall Versus Filters .....	595
44.6 Applying a Filter .....	596
44.6.1 Applying LAN Filters .....	596
44.6.2 Applying DMZ Filters .....	596
44.6.3 Applying Remote Node Filters .....	597
<b>Chapter 45</b>	
<b>SNMP Configuration .....</b>	<b>598</b>
45.1 SNMP Configuration .....	598
45.2 SNMP Traps .....	599
<b>Chapter 46</b>	
<b>System Information &amp; Diagnosis .....</b>	<b>600</b>
46.1 Introduction to System Status .....	600

46.2 System Status .....	600
46.3 System Information and Console Port Speed .....	602
46.3.1 System Information .....	602
46.3.2 Console Port Speed .....	603
46.4 Log and Trace .....	604
46.4.1 Viewing Error Log .....	604
46.4.2 Syslog Logging .....	605
46.4.3 Call-Triggering Packet .....	608
46.5 Diagnostic .....	608
46.5.1 WAN DHCP .....	609

## **Chapter 47**

### **Firmware and Configuration File Maintenance ..... 612**

47.1 Introduction .....	612
47.2 Filename Conventions .....	612
47.3 Backup Configuration .....	613
47.3.1 Backup Configuration .....	613
47.3.2 Using the FTP Command from the Command Line .....	614
47.3.3 Example of FTP Commands from the Command Line .....	615
47.3.4 GUI-based FTP Clients .....	615
47.3.5 File Maintenance Over WAN .....	615
47.3.6 Backup Configuration Using TFTP .....	616
47.3.7 TFTP Command Example .....	616
47.3.8 GUI-based TFTP Clients .....	617
47.3.9 Backup Via Console Port .....	617
47.4 Restore Configuration .....	618
47.4.1 Restore Using FTP .....	618
47.4.2 Restore Using FTP Session Example .....	620
47.4.3 Restore Via Console Port .....	620
47.5 Uploading Firmware and Configuration Files .....	621
47.5.1 Firmware File Upload .....	621
47.5.2 Configuration File Upload .....	622
47.5.3 FTP File Upload Command from the DOS Prompt Example .....	623
47.5.4 FTP Session Example of Firmware File Upload .....	623
47.5.5 TFTP File Upload .....	623
47.5.6 TFTP Upload Command Example .....	624
47.5.7 Uploading Via Console Port .....	624
47.5.8 Uploading Firmware File Via Console Port .....	624
47.5.9 Example Xmodem Firmware Upload Using HyperTerminal .....	625
47.5.10 Uploading Configuration File Via Console Port .....	625
47.5.11 Example Xmodem Configuration Upload Using HyperTerminal .....	626

<b>Chapter 48</b>	
<b>System Maintenance Menus 8 to 10</b> .....	<b>628</b>
48.1 Command Interpreter Mode .....	628
48.1.1 Command Syntax .....	628
48.1.2 Command Usage .....	629
48.2 Call Control Support .....	630
48.2.1 Budget Management .....	630
48.2.2 Call History .....	631
48.3 Time and Date Setting .....	632
<b>Chapter 49</b>	
<b>Remote Management</b> .....	<b>636</b>
49.1 Remote Management .....	636
49.1.1 Remote Management Limitations .....	638
<b>Chapter 50</b>	
<b>IP Policy Routing</b> .....	<b>640</b>
50.1 IP Routing Policy Summary .....	640
50.2 IP Routing Policy Setup .....	641
50.2.1 Applying Policy to Packets .....	643
50.3 IP Policy Routing Example .....	644
<b>Chapter 51</b>	
<b>Call Scheduling</b> .....	<b>648</b>
51.1 Introduction to Call Scheduling .....	648
<b>Chapter 52</b>	
<b>Troubleshooting</b> .....	<b>652</b>
52.1 Problems Starting Up the ZyWALL .....	652
52.2 Problems with the LAN Interface .....	652
52.3 Problems with the DMZ Interface .....	653
52.4 Problems with the WAN Interface .....	653
52.5 Problems Accessing the ZyWALL .....	654
52.5.1 Pop-up Windows, JavaScripts and Java Permissions .....	654
52.5.1.1 Internet Explorer Pop-up Blockers .....	655
52.5.1.2 JavaScripts .....	658
52.5.1.3 Java Permissions .....	660
52.6 Packet Flow .....	662
<b>Appendix A</b>	
<b>Product Specifications</b> .....	<b>664</b>
<b>Appendix B</b>	



<b>Hardware Installation .....</b>	<b>672</b>
<b>Appendix C</b>	
<b>Removing and Installing a Fuse .....</b>	<b>676</b>
<b>Appendix D</b>	
<b>Setting up Your Computer's IP Address.....</b>	<b>678</b>
<b>Appendix E</b>	
<b>IP Subnetting .....</b>	<b>694</b>
<b>Appendix F</b>	
<b>PPPoE .....</b>	<b>702</b>
<b>Appendix G</b>	
<b>PPTP.....</b>	<b>704</b>
<b>Appendix H</b>	
<b>Wireless LANs .....</b>	<b>708</b>
<b>Appendix I</b>	
<b>Triangle Route.....</b>	<b>722</b>
<b>Appendix J</b>	
<b>Windows 98 SE/Me Requirements for Anti-Virus Message Display.....</b>	<b>726</b>
<b>Appendix K</b>	
<b>VPN Setup.....</b>	<b>730</b>
<b>Appendix L</b>	
<b>Importing Certificates .....</b>	<b>742</b>
<b>Appendix M</b>	
<b>Command Interpreter.....</b>	<b>754</b>
<b>Appendix N</b>	
<b>Firewall Commands .....</b>	<b>756</b>
<b>Appendix O</b>	
<b>NetBIOS Filter Commands .....</b>	<b>762</b>
<b>Appendix P</b>	
<b>Certificates Commands .....</b>	<b>766</b>
<b>Appendix Q</b>	
<b>Brute-Force Password Guessing Protection.....</b>	<b>770</b>
<b>Appendix R</b>	
<b>Boot Commands .....</b>	<b>772</b>

**Appendix S**  
**Log Descriptions** ..... **774**  
**Index** ..... **798**



# List of Figures

Figure 1 Secure Internet Access via Cable, DSL or Wireless Modem .....	62
Figure 2 VPN Application .....	63
Figure 3 ZyWALL 70 Front Panel .....	63
Figure 4 ZyWALL 35 Front Panel .....	63
Figure 5 ZyWALL 5 Front Panel .....	63
Figure 6 Change Password Screen .....	67
Figure 7 Replace Certificate Screen .....	67
Figure 8 Example Xmodem Upload .....	68
Figure 9 Web Configurator HOME Screen in Router Mode .....	69
Figure 10 Web Configurator HOME Screen in Bridge Mode .....	72
Figure 11 Home : Show Statistics .....	79
Figure 12 Home : Show Statistics: Line Chart .....	80
Figure 13 Home : DHCP Table .....	81
Figure 14 Home : VPN Status .....	83
Figure 15 ISP Parameters : Ethernet Encapsulation .....	85
Figure 16 ISP Parameters : PPPoE Encapsulation .....	86
Figure 17 ISP Parameters: PPTP Encapsulation .....	88
Figure 18 Internet Access Wizard: Second Screen .....	89
Figure 19 Internet Access Setup Complete .....	90
Figure 20 Internet Access Wizard: Registration .....	90
Figure 21 Internet Access Wizard: Registration in Progress .....	91
Figure 22 Internet Access Wizard: Status .....	92
Figure 23 Internet Access Wizard: Registration Failed .....	92
Figure 24 Internet Access Wizard: Registered Device .....	92
Figure 25 Internet Access Wizard: Activated Services .....	93
Figure 26 VPN Wizard: Gateway Setting .....	93
Figure 27 VPN Wizard: Network Setting .....	95
Figure 28 VPN Wizard: IKE Tunnel Setting .....	96
Figure 29 VPN Wizard: IPSec Setting .....	98
Figure 30 VPN Wizard: VPN Status .....	100
Figure 31 VPN Wizard Setup Complete .....	102
Figure 32 Registration .....	105
Figure 33 Registration: Registered Device .....	107
Figure 34 Registration: Service .....	107
Figure 35 LAN .....	113
Figure 36 LAN Static DHCP .....	115
Figure 37 Physical Network & Partitioned Logical Networks .....	116
Figure 38 LAN IP Alias .....	117

Figure 39 WLAN Port Role Example .....	118
Figure 40 LAN Port Roles .....	119
Figure 41 Port Roles Change Complete .....	120
Figure 42 Bridge Loop: Bridge Connected to Wired LAN .....	122
Figure 43 Bridge .....	125
Figure 44 WLAN Port Role Example .....	127
Figure 45 Bridge Port Roles .....	127
Figure 46 Port Roles Change Complete .....	128
Figure 47 Least Load First Example .....	132
Figure 48 Weighted Round Robin Algorithm Example .....	133
Figure 49 Spillover Algorithm Example .....	134
Figure 50 WAN General .....	135
Figure 51 Load Balancing: Least Load First .....	138
Figure 52 Load Balancing: Weighted Round Robin .....	139
Figure 53 Load Balancing: Spillover .....	140
Figure 54 WAN Route .....	141
Figure 55 WAN: Ethernet Encapsulation .....	144
Figure 56 WAN: PPPoE Encapsulation .....	147
Figure 57 WAN: PPTP Encapsulation .....	150
Figure 58 Traffic Redirect WAN Setup .....	153
Figure 59 Traffic Redirect LAN Setup .....	154
Figure 60 Traffic Redirect .....	154
Figure 61 Dial Backup .....	156
Figure 62 Advanced Setup .....	160
Figure 63 DMZ .....	163
Figure 64 DMZ Static DHCP .....	166
Figure 65 DMZ: IP Alias .....	167
Figure 66 DMZ Public Address Example .....	169
Figure 67 DMZ Private and Public Address Example .....	170
Figure 68 WLAN Port Role Example .....	171
Figure 69 DMZ: Port Roles .....	172
Figure 70 WLAN .....	175
Figure 71 WLAN Static DHCP .....	178
Figure 72 WLAN IP Alias .....	179
Figure 73 WLAN Port Role Example .....	180
Figure 74 WLAN Port Roles .....	181
Figure 75 WLAN Port Roles Change Complete .....	182
Figure 76 ZyWALL Wireless Security Levels .....	183
Figure 77 EAP Authentication .....	186
Figure 78 WPA-PSK Authentication .....	189
Figure 79 WPA with RADIUS Application Example .....	190
Figure 80 Wireless Card: No Security .....	191
Figure 81 Wireless Card: Static WEP .....	193

Figure 82 Wireless Card: WPA-PSK .....	194
Figure 83 Wireless Card: WPA .....	195
Figure 84 Wireless Card: 802.1x + Dynamic WEP .....	196
Figure 85 Wireless Card: 802.1x + Static WEP .....	197
Figure 86 Wireless Card: 802.1x + No WEP .....	198
Figure 87 Wireless Card: No Access 802.1x + Static WEP .....	199
Figure 88 Wireless Card: MAC Address Filter .....	201
Figure 89 ZyWALL Firewall Application .....	204
Figure 90 Three-Way Handshake .....	205
Figure 91 SYN Flood .....	206
Figure 92 Smurf Attack .....	207
Figure 93 Stateful Inspection .....	209
Figure 94 LAN to WAN Traffic .....	218
Figure 95 WAN to LAN Traffic .....	218
Figure 96 Default Rule (Router Mode) .....	219
Figure 97 Default Rule (Bridge Mode) .....	221
Figure 98 Rule Summary .....	222
Figure 99 Firewall Edit Rule .....	224
Figure 100 Anti-Probing .....	226
Figure 101 Firewall Threshold .....	229
Figure 102 Firewall Service .....	231
Figure 103 Firewall Edit Custom Service .....	232
Figure 104 Service .....	236
Figure 105 Edit Custom Service Example .....	236
Figure 106 Rule Summary .....	237
Figure 107 Rule Edit Example .....	237
Figure 108 My Service Rule Configuration .....	238
Figure 109 My Service Example Rule Summary .....	239
Figure 110 Network Intrusions .....	240
Figure 111 Applying IDP to Interfaces .....	245
Figure 112 IDP: General .....	246
Figure 113 Attack Types .....	247
Figure 114 Signature Actions .....	249
Figure 115 IDP: Signatures .....	250
Figure 116 Signature Query by Partial Name .....	252
Figure 117 Signature Query by Complete ID .....	253
Figure 118 Signature Query by Attribute. ....	254
Figure 119 Signatures Update .....	255
Figure 120 IDP: Backup & Restore .....	257
Figure 121 ZyWALL Anti-virus Example .....	260
Figure 122 Anti-Virus: General .....	261
Figure 123 Anti-Virus: Update .....	264
Figure 124 Anti-spam External Database Example .....	268

Figure 125 Anti-Spam: General .....	270
Figure 126 Anti-Spam: External DB .....	272
Figure 127 Anti-Spam: Lists .....	274
Figure 128 Anti-Spam Rule Edit .....	275
Figure 129 Content Filter : General .....	279
Figure 130 Content Filtering Lookup Procedure .....	281
Figure 131 Content Filter : Categories .....	282
Figure 132 Content Filter: Customization .....	288
Figure 133 Content Filter: Cache .....	291
Figure 134 myZyXEL.com: Login .....	295
Figure 135 myZyXEL.com: Welcome .....	295
Figure 136 myZyXEL.com: Service Management .....	296
Figure 137 Blue Coat: Login .....	296
Figure 138 Content Filtering Reports Main Screen .....	297
Figure 139 Blue Coat: Report Home .....	297
Figure 140 Global Report Screen Example .....	298
Figure 141 Requested URLs Example .....	299
Figure 142 Web Page Review Process Screen .....	300
Figure 143 Encryption and Decryption .....	303
Figure 144 IPSec Architecture .....	304
Figure 145 Transport and Tunnel Mode IPSec Encapsulation .....	305
Figure 146 NAT Router Between IPSec Routers .....	311
Figure 147 Two Phases to Set Up the IPSec SA .....	313
Figure 148 VPN Rules (IKE) .....	316
Figure 149 Gateway and Network Policies .....	317
Figure 150 IPSec Fields Summary .....	317
Figure 151 VPN Rules (IKE): Gateway Policy: Edit .....	319
Figure 152 VPN Rules (IKE): Network Policy Edit .....	325
Figure 153 VPN Rules (IKE): Network Policy Move .....	329
Figure 154 VPN Rules (Manual) .....	330
Figure 155 VPN Rules (Manual): Edit .....	332
Figure 156 VPN: SA Monitor .....	335
Figure 157 VPN: Global Setting .....	336
Figure 158 Telecommuters Sharing One VPN Rule Example .....	338
Figure 159 Telecommuters Using Unique VPN Rules Example .....	339
Figure 160 Certificate Configuration Overview .....	343
Figure 161 My Certificates .....	344
Figure 162 My Certificate Import .....	347
Figure 163 My Certificate Create .....	348
Figure 164 My Certificate Details .....	351
Figure 165 Trusted CAs .....	354
Figure 166 Trusted CA Import .....	355
Figure 167 Trusted CA Details .....	357

Figure 168 Trusted Remote Hosts .....	360
Figure 169 Remote Host Certificates .....	361
Figure 170 Certificate Details .....	362
Figure 171 Trusted Remote Host Import .....	363
Figure 172 Trusted Remote Host Details .....	364
Figure 173 Directory Servers .....	366
Figure 174 Directory Server Add .....	367
Figure 175 Local User Database .....	371
Figure 176 RADIUS .....	372
Figure 177 How NAT Works .....	376
Figure 178 NAT Application With IP Alias .....	376
Figure 179 Port Restricted Cone NAT Example .....	377
Figure 180 NAT Overview .....	379
Figure 181 NAT Address Mapping .....	381
Figure 182 NAT Address Mapping Edit .....	382
Figure 183 Multiple Servers Behind NAT Example .....	385
Figure 184 Port Translation Example .....	386
Figure 185 Port Forwarding .....	387
Figure 186 Trigger Port Forwarding Process: Example .....	388
Figure 187 Port Triggering .....	389
Figure 188 Example of Static Routing Topology .....	392
Figure 189 IP Static Route .....	393
Figure 190 IP Static Route Edit .....	394
Figure 191 Policy Route Summary .....	397
Figure 192 Edit IP Policy Route .....	399
Figure 193 Subnet-based Bandwidth Management Example .....	403
Figure 194 Bandwidth Management: Summary .....	409
Figure 195 Bandwidth Management: Class Setup .....	410
Figure 196 Bandwidth Management: Edit Class .....	412
Figure 197 Bandwidth Management: Statistics .....	415
Figure 198 Bandwidth Management: Monitor .....	416
Figure 199 Private DNS Server Example .....	420
Figure 200 System DNS .....	421
Figure 201 System DNS: Add Address Record .....	422
Figure 202 System DNS: Insert Name Server Record .....	423
Figure 203 DNS Cache .....	425
Figure 204 DNS DHCP .....	427
Figure 205 DDNS .....	429
Figure 206 HTTPS Implementation .....	434
Figure 207 WWW .....	435
Figure 208 Security Alert Dialog Box (Internet Explorer) .....	436
Figure 209 Security Certificate 1 (Netscape) .....	437
Figure 210 Security Certificate 2 (Netscape) .....	437



Figure 211 Login Screen (Internet Explorer) .....	439
Figure 212 Login Screen (Netscape) .....	439
Figure 213 Replace Certificate .....	440
Figure 214 Device-specific Certificate .....	440
Figure 215 Common ZyWALL Certificate .....	441
Figure 216 SSH Communication Example .....	441
Figure 217 How SSH Works .....	442
Figure 218 SSH .....	443
Figure 219 SSH Example 1: Store Host Key .....	444
Figure 220 SSH Example 2: Test .....	445
Figure 221 SSH Example 2: Log in .....	445
Figure 222 Secure FTP: Firmware Upload Example .....	446
Figure 223 Telnet Configuration on a TCP/IP Network .....	446
Figure 224 Telnet .....	447
Figure 225 FTP .....	448
Figure 226 SNMP Management Model .....	449
Figure 227 SNMP .....	451
Figure 228 DNS .....	452
Figure 229 CNM .....	453
Figure 230 UPnP .....	457
Figure 231 UPnP Ports .....	458
Figure 232 H.323 ALG Example .....	468
Figure 233 H.323 with Multiple WAN IP Addresses .....	468
Figure 234 H.323 Calls from the WAN with Multiple Outgoing Calls .....	469
Figure 235 SIP ALG Example .....	470
Figure 236 ALG .....	471
Figure 237 View Log .....	472
Figure 238 myZyXEL.com: Download Center .....	474
Figure 239 myZyXEL.com: Certificate Download .....	475
Figure 240 Log Settings .....	476
Figure 241 Reports .....	479
Figure 242 Web Site Hits Report Example .....	480
Figure 243 Protocol/Port Report Example .....	481
Figure 244 Host IP Address Report Example .....	482
Figure 245 General Setup .....	485
Figure 246 Password Setup .....	486
Figure 247 Time and Date .....	487
Figure 248 Synchronization in Process .....	490
Figure 249 Synchronization is Successful .....	490
Figure 250 Synchronization Fail .....	490
Figure 251 Device Mode (Router Mode) .....	492
Figure 252 Device Mode (Bridge Mode) .....	493
Figure 253 Firmware Upload .....	495

Figure 254 Firmware Upload In Process .....	495
Figure 255 Network Temporarily Disconnected .....	496
Figure 256 Firmware Upload Error .....	496
Figure 257 Backup and Restore .....	497
Figure 258 Configuration Upload Successful .....	498
Figure 259 Network Temporarily Disconnected .....	498
Figure 260 Configuration Upload Error .....	498
Figure 261 Reset Warning Message .....	499
Figure 262 Restart Screen .....	499
Figure 263 Initial Screen .....	501
Figure 264 Password Screen .....	501
Figure 265 Main Menu (Router Mode) .....	503
Figure 266 Main Menu (Bridge Mode) .....	503
Figure 267 Menu 23: System Password .....	507
Figure 268 Menu 1: General Setup (Router Mode) .....	508
Figure 269 Menu 1: General Setup (Bridge Mode) .....	509
Figure 270 Menu 1.1: Configure Dynamic DNS .....	510
Figure 271 Menu 1.1.1: DDNS Host Summary .....	511
Figure 272 Menu 1.1.1: DDNS Edit Host .....	512
Figure 273 MAC Address Cloning in WAN Setup .....	514
Figure 274 Menu 2: Dial Backup Setup .....	516
Figure 275 Menu 2.1: Advanced WAN Setup .....	517
Figure 276 Menu 11.3: Remote Node Profile (Backup ISP) .....	519
Figure 277 Menu 11.3.1: Remote Node PPP Options .....	521
Figure 278 Menu 11.3.2: Remote Node Network Layer Options .....	522
Figure 279 Menu 11.3.3: Remote Node Script .....	524
Figure 280 Menu 11.3.4: Remote Node Filter .....	525
Figure 281 Menu 3: LAN Setup .....	526
Figure 282 Menu 3.1: LAN Port Filter Setup .....	527
Figure 283 Menu 3: TCP/IP and DHCP Setup .....	527
Figure 284 Menu 3.2: TCP/IP and DHCP Ethernet Setup .....	528
Figure 285 Menu 3.2.1: IP Alias Setup .....	530
Figure 286 Menu 4: Internet Access Setup (Ethernet) .....	532
Figure 287 Internet Access Setup (PPTP) .....	534
Figure 288 Internet Access Setup (PPPoE) .....	535
Figure 289 Menu 5: DMZ Setup .....	536
Figure 290 Menu 5.1: DMZ Port Filter Setup .....	536
Figure 291 Menu 5: DMZ Setup .....	537
Figure 292 Menu 5.2: TCP/IP and DHCP Ethernet Setup .....	537
Figure 293 Menu 5.2.1: IP Alias Setup .....	538
Figure 294 Menu 6: Route Setup .....	540
Figure 295 Menu 6.1: Route Assessment .....	540
Figure 296 Menu 6.2: Traffic Redirect .....	541

Figure 297 Menu 6.3: Route Failover .....	542
Figure 298 Menu 7.1: Wireless Setup .....	544
Figure 299 Menu 7.1.1: WLAN MAC Address Filter .....	546
Figure 300 Menu 7: WLAN Setup .....	547
Figure 301 Menu 7.2: TCP/IP and DHCP Ethernet Setup .....	548
Figure 302 Menu 7.2.1: IP Alias Setup .....	549
Figure 303 Menu 11: Remote Node Setup .....	551
Figure 304 Menu 11.1: Remote Node Profile for Ethernet Encapsulation .....	551
Figure 305 Menu 11.1: Remote Node Profile for PPPoE Encapsulation .....	553
Figure 306 Menu 11.1: Remote Node Profile for PPTP Encapsulation .....	555
Figure 307 Menu 11.1.2: Remote Node Network Layer Options for Ethernet Encapsulation 556	
Figure 308 Menu 11.1.4: Remote Node Filter (Ethernet Encapsulation) .....	558
Figure 309 Menu 11.1.4: Remote Node Filter (PPPoE or PPTP Encapsulation) .....	558
Figure 310 Menu 11.1.5: Traffic Redirect Setup .....	559
Figure 311 Menu 12: IP Static Route Setup .....	560
Figure 312 Menu 12. 1: Edit IP Static Route .....	561
Figure 313 Menu 4: Applying NAT for Internet Access .....	563
Figure 314 Menu 11.1.2: Applying NAT to the Remote Node .....	563
Figure 315 Menu 15: NAT Setup .....	564
Figure 316 Menu 15.1: Address Mapping Sets .....	565
Figure 317 Menu 15.1.255: SUA Address Mapping Rules .....	565
Figure 318 Menu 15.1.1: First Set .....	567
Figure 319 Menu 15.1.1.1: Editing/Configuring an Individual Rule in a Set .....	568
Figure 320 Menu 15.2: NAT Server Sets .....	569
Figure 321 Menu 15.2.1: NAT Server Sets .....	570
Figure 322 15.2.1.2: NAT Server Configuration .....	571
Figure 323 Menu 15.2.1: NAT Server Setup .....	572
Figure 324 Server Behind NAT Example .....	572
Figure 325 NAT Example 1 .....	573
Figure 326 Menu 4: Internet Access & NAT Example .....	573
Figure 327 NAT Example 2 .....	574
Figure 328 Menu 15.2.1: Specifying an Inside Server .....	574
Figure 329 NAT Example 3 .....	575
Figure 330 Example 3: Menu 11.1.2 .....	576
Figure 331 Example 3: Menu 15.1.1.1 .....	576
Figure 332 Example 3: Final Menu 15.1.1 .....	577
Figure 333 Example 3: Menu 15.2.1 .....	577
Figure 334 NAT Example 4 .....	578
Figure 335 Example 4: Menu 15.1.1.1: Address Mapping Rule .....	578
Figure 336 Example 4: Menu 15.1.1: Address Mapping Rules .....	579
Figure 337 Menu 15.3.1: Trigger Port Setup .....	580
Figure 338 Menu 21: Filter and Firewall Setup .....	582

Figure 339 Menu 21.2: Firewall Setup .....	583
Figure 340 Outgoing Packet Filtering Process .....	584
Figure 341 Filter Rule Process .....	586
Figure 342 Menu 21: Filter and Firewall Setup .....	587
Figure 343 Menu 21.1: Filter Set Configuration .....	587
Figure 344 Menu 21.1.1.1: TCP/IP Filter Rule .....	589
Figure 345 Executing an IP Filter .....	591
Figure 346 Menu 21.1.1.1: Generic Filter Rule .....	592
Figure 347 Telnet Filter Example .....	593
Figure 348 Example Filter: Menu 21.1.3.1 .....	594
Figure 349 Example Filter Rules Summary: Menu 21.1.3 .....	594
Figure 350 Protocol and Device Filter Sets .....	595
Figure 351 Filtering LAN Traffic .....	596
Figure 352 Filtering DMZ Traffic .....	597
Figure 353 Filtering Remote Node Traffic .....	597
Figure 354 Menu 22: SNMP Configuration .....	598
Figure 355 Menu 24: System Maintenance .....	600
Figure 356 Menu 24.1: System Maintenance: Status .....	601
Figure 357 Menu 24.2: System Information and Console Port Speed .....	602
Figure 358 Menu 24.2.1: System Maintenance: Information .....	603
Figure 359 Menu 24.2.2: System Maintenance: Change Console Port Speed .....	604
Figure 360 Menu 24.3: System Maintenance: Log and Trace .....	604
Figure 361 Examples of Error and Information Messages .....	605
Figure 362 Menu 24.3.2: System Maintenance: Syslog Logging .....	605
Figure 363 Call-Triggering Packet Example .....	608
Figure 364 Menu 24.4: System Maintenance: Diagnostic .....	609
Figure 365 WAN & LAN DHCP .....	609
Figure 366 Telnet into Menu 24.5 .....	614
Figure 367 FTP Session Example .....	615
Figure 368 System Maintenance: Backup Configuration .....	617
Figure 369 System Maintenance: Starting Xmodem Download Screen .....	617
Figure 370 Backup Configuration Example .....	618
Figure 371 Successful Backup Confirmation Screen .....	618
Figure 372 Telnet into Menu 24.6 .....	619
Figure 373 Restore Using FTP Session Example .....	620
Figure 374 System Maintenance: Restore Configuration .....	620
Figure 375 System Maintenance: Starting Xmodem Download Screen .....	620
Figure 376 Restore Configuration Example .....	620
Figure 377 Successful Restoration Confirmation Screen .....	621
Figure 378 Telnet Into Menu 24.7.1: Upload System Firmware .....	622
Figure 379 Telnet Into Menu 24.7.2: System Maintenance .....	622
Figure 380 FTP Session Example of Firmware File Upload .....	623
Figure 381 Menu 24.7.1 As Seen Using the Console Port .....	625

Figure 382 Example Xmodem Upload .....	625
Figure 383 Menu 24.7.2 As Seen Using the Console Port .....	626
Figure 384 Example Xmodem Upload .....	626
Figure 385 Command Mode in Menu 24 .....	628
Figure 386 Valid Commands .....	629
Figure 387 Call Control .....	630
Figure 388 Budget Management .....	631
Figure 389 Call History .....	632
Figure 390 Menu 24: System Maintenance .....	633
Figure 391 Menu 24.10 System Maintenance: Time and Date Setting .....	633
Figure 392 Menu 24.11 – Remote Management Control .....	637
Figure 393 Menu 25: Sample IP Routing Policy Summary .....	640
Figure 394 Menu 25.1: IP Routing Policy Setup .....	642
Figure 395 Menu 25.1.1: IP Routing Policy Setup .....	644
Figure 396 Example of IP Policy Routing .....	645
Figure 397 IP Routing Policy Example 1 .....	645
Figure 398 IP Routing Policy Example 2 .....	646
Figure 399 Schedule Setup .....	648
Figure 400 Schedule Set Setup .....	649
Figure 401 Applying Schedule Set(s) to a Remote Node (PPPoE) .....	650
Figure 402 Applying Schedule Set(s) to a Remote Node (PPTP) .....	651
Figure 403 Pop-up Blocker .....	655
Figure 404 Internet Options: Privacy .....	656
Figure 405 Internet Options: Privacy .....	657
Figure 406 Pop-up Blocker Settings .....	658
Figure 407 Internet Options: Security .....	659
Figure 408 Security Settings - Java Scripting .....	660
Figure 409 Security Settings - Java .....	661
Figure 410 Java (Sun) .....	662
Figure 411 WLAN Card Installation .....	669
Figure 412 Console/Dial Backup Port Pin Layout .....	669
Figure 413 Ethernet Cable Pin Assignments .....	670
Figure 414 Attaching Rubber Feet .....	673
Figure 415 Attaching Mounting Brackets and Screws .....	674
Figure 416 Rack Mounting .....	674
Figure 417 Windows 95/98/Me: Network: Configuration .....	679
Figure 418 Windows 95/98/Me: TCP/IP Properties: IP Address .....	680
Figure 419 Windows 95/98/Me: TCP/IP Properties: DNS Configuration .....	681
Figure 420 Windows XP: Start Menu .....	682
Figure 421 Windows XP: Control Panel .....	682
Figure 422 Windows XP: Control Panel: Network Connections: Properties .....	683
Figure 423 Windows XP: Local Area Connection Properties .....	683
Figure 424 Windows XP: Internet Protocol (TCP/IP) Properties .....	684

Figure 425 Windows XP: Advanced TCP/IP Properties .....	685
Figure 426 Windows XP: Internet Protocol (TCP/IP) Properties .....	686
Figure 427 Macintosh OS 8/9: Apple Menu .....	687
Figure 428 Macintosh OS 8/9: TCP/IP .....	687
Figure 429 Macintosh OS X: Apple Menu .....	688
Figure 430 Macintosh OS X: Network .....	689
Figure 431 Red Hat 9.0: KDE: Network Configuration: Devices .....	690
Figure 432 Red Hat 9.0: KDE: Ethernet Device: General .....	690
Figure 433 Red Hat 9.0: KDE: Network Configuration: DNS .....	691
Figure 434 Red Hat 9.0: KDE: Network Configuration: Activate .....	691
Figure 435 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0 .....	692
Figure 436 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0 .....	692
Figure 437 Red Hat 9.0: DNS Settings in resolv.conf .....	692
Figure 438 Red Hat 9.0: Restart Ethernet Card .....	693
Figure 439 Red Hat 9.0: Checking TCP/IP Properties .....	693
Figure 440 Single-Computer per Router Hardware Configuration .....	703
Figure 441 ZyWALL as a PPPoE Client .....	703
Figure 442 Transport PPP frames over Ethernet .....	704
Figure 443 PPTP Protocol Overview .....	705
Figure 444 Example Message Exchange between Computer and an ANT .....	706
Figure 445 Peer-to-Peer Communication in an Ad-hoc Network .....	708
Figure 446 Basic Service Set .....	709
Figure 447 Infrastructure WLAN .....	710
Figure 448 RTS/CTS .....	711
Figure 449 EAP Authentication .....	714
Figure 450 WEP Authentication Steps .....	717
Figure 451 Roaming Example .....	720
Figure 452 Ideal Setup .....	722
Figure 453 "Triangle Route" Problem .....	723
Figure 454 IP Alias .....	724
Figure 455 Gateways on the WAN Side .....	724
Figure 456 Windows 98 SE: WinPopup .....	726
Figure 457 Windows 98 SE: Program Task Bar .....	727
Figure 458 Windows 98 SE: Task Bar Properties .....	727
Figure 459 Windows 98 SE: StartUp .....	728
Figure 460 Windows 98 SE: Startup: Create Shortcut .....	728
Figure 461 Windows 98 SE: Startup: Select a Title for the Program .....	729
Figure 462 Windows 98 SE: Startup: Shortcut .....	729
Figure 463 VPN Rules .....	731
Figure 464 Headquarters Gateway Policy Edit .....	732
Figure 465 Branch Office Gateway Policy Edit .....	733
Figure 466 Headquarters VPN Rule .....	734
Figure 467 Branch Office VPN Rule .....	734

Figure 468 Headquarters Network Policy Edit .....	735
Figure 469 Branch Office Network Policy Edit .....	736
Figure 470 VPN Rule Configured .....	737
Figure 471 VPN Dial .....	737
Figure 472 VPN Tunnel Established .....	737
Figure 473 VPN Log Example .....	739
Figure 474 IKE/IPSec Debug Example .....	740
Figure 475 Security Certificate .....	742
Figure 476 Login Screen .....	743
Figure 477 Certificate General Information before Import .....	743
Figure 478 Certificate Import Wizard 1 .....	744
Figure 479 Certificate Import Wizard 2 .....	744
Figure 480 Certificate Import Wizard 3 .....	745
Figure 481 Root Certificate Store .....	745
Figure 482 Certificate General Information after Import .....	746
Figure 483 ZyWALL Trusted CA Screen .....	747
Figure 484 CA Certificate Example .....	748
Figure 485 Personal Certificate Import Wizard 1 .....	749
Figure 486 Personal Certificate Import Wizard 2 .....	749
Figure 487 Personal Certificate Import Wizard 3 .....	750
Figure 488 Personal Certificate Import Wizard 4 .....	750
Figure 489 Personal Certificate Import Wizard 5 .....	751
Figure 490 Personal Certificate Import Wizard 6 .....	751
Figure 491 Access the ZyWALL Via HTTPS .....	751
Figure 492 SSL Client Authentication .....	752
Figure 493 ZyWALL Secure Login Screen .....	752
Figure 494 Option to Enter Debug Mode .....	772
Figure 495 Boot Module Commands .....	773
Figure 496 Displaying Log Categories Example .....	796
Figure 497 Displaying Log Parameters Example .....	796

# List of Tables

Table 1 Model Specific Features .....	54
Table 2 Front Panel LEDs .....	64
Table 3 Web Configurator HOME Screen in Router Mode .....	70
Table 4 Web Configurator HOME Screen in Bridge Mode .....	72
Table 5 Bridge and Router Mode Features Comparison .....	74
Table 6 Screens Summary .....	75
Table 7 Home: Show Statistics .....	79
Table 8 Home: Show Statistics: Line Chart .....	81
Table 9 Home: DHCP Table .....	82
Table 10 Home : VPN Status .....	83
Table 11 ISP Parameters : Ethernet Encapsulation .....	85
Table 12 ISP Parameters: PPPoE Encapsulation .....	86
Table 13 ISP Parameters : PPTP Encapsulation .....	88
Table 14 Internet Access Wizard: Registration .....	91
Table 15 VPN Wizard: Gateway Setting .....	94
Table 16 VPN Wizard : Network Setting .....	95
Table 17 VPN Wizard: IKE Tunnel Setting .....	97
Table 18 VPN Wizard: IPSec Setting .....	98
Table 19 VPN Wizard: VPN Status .....	100
Table 20 Registration .....	106
Table 21 Service .....	108
Table 22 LAN .....	113
Table 23 LAN Static DHCP .....	115
Table 24 LAN IP Alias .....	117
Table 25 LAN Port Roles .....	119
Table 26 STP Path Costs .....	123
Table 27 STP Port States .....	124
Table 28 Bridge .....	125
Table 29 Bridge Port Roles .....	127
Table 30 Least Load First: Example 1 .....	132
Table 31 Least Load First: Example 2 .....	132
Table 32 WAN General .....	136
Table 33 Load Balancing: Least Load First .....	138
Table 34 Load Balancing: Weighted Round Robin .....	139
Table 35 Load Balancing: Spillover .....	140
Table 36 WAN Route .....	141
Table 37 Private IP Address Ranges .....	142
Table 38 Example of Network Properties for LAN Servers with Fixed IP Addresses .....	143



Table 39 WAN: Ethernet Encapsulation .....	144
Table 40 WAN: PPPoE Encapsulation .....	148
Table 41 WAN: PPTP Encapsulation .....	151
Table 42 Traffic Redirect .....	154
Table 43 Dial Backup .....	157
Table 44 Advanced Setup .....	160
Table 45 DMZ .....	163
Table 46 DMZ Static DHCP .....	166
Table 47 DMZ: IP Alias .....	167
Table 48 DMZ: Port Roles .....	172
Table 49 WLAN .....	175
Table 50 WLAN Static DHCP .....	178
Table 51 WLAN IP Alias .....	179
Table 52 WLAN Port Roles .....	181
Table 53 Wireless Security Relational Matrix .....	184
Table 54 Wireless Card: No Security .....	191
Table 55 Wireless Card: Static WEP .....	193
Table 56 Wireless Card: WPA-PSK .....	194
Table 57 Wireless Card: WPA .....	195
Table 58 Wireless Card: 802.1x + Dynamic WEP .....	196
Table 59 Wireless Card: 802.1x + Static WEP .....	197
Table 60 Wireless Card: 802.1x + No WEP .....	199
Table 61 Wireless Card: No Access 802.1x + Static WEP .....	200
Table 62 Wireless Card: MAC Address Filter .....	201
Table 63 Common IP Ports .....	204
Table 64 ICMP Commands That Trigger Alerts .....	207
Table 65 Legal NetBIOS Commands .....	207
Table 66 Legal SMTP Commands .....	208
Table 67 Default Rule (Router Mode) .....	219
Table 68 Default Rule (Bridge Mode) .....	221
Table 69 Rule Summary .....	222
Table 70 Firewall Edit Rule .....	225
Table 71 Anti-Probing .....	226
Table 72 Firewall Threshold .....	229
Table 73 Firewall Service .....	231
Table 74 Firewall Edit Custom Service .....	232
Table 75 Predefined Services .....	233
Table 76 IDP: General Setup .....	246
Table 77 Attack Types .....	247
Table 78 Intrusion Severity .....	248
Table 79 Signature Actions .....	249
Table 80 IDP Signatures: Group View .....	250
Table 81 Signatures Update .....	256

Table 82 Common Computer Virus Types .....	258
Table 83 Anti-Virus: General .....	262
Table 84 Anti-Virus: Update .....	264
Table 85 Anti-Spam: General .....	271
Table 86 Anti-Spam: External DB .....	272
Table 87 Anti-Spam: Lists .....	274
Table 88 Anti-Spam Rule Edit .....	276
Table 89 Content Filter : General .....	279
Table 90 Content Filter: Categories .....	282
Table 91 Content Filter: Customization .....	289
Table 92 Content Filter: Cache .....	292
Table 93 VPN and NAT .....	306
Table 94 ESP and AH .....	309
Table 95 Local ID Type and Content Fields .....	312
Table 96 Peer ID Type and Content Fields .....	312
Table 97 Matching ID Type and Content Configuration Example .....	312
Table 98 Mismatching ID Type and Content Configuration Example .....	313
Table 99 IPSec Fields Summary .....	316
Table 100 VPN screen Icons Key .....	317
Table 101 VPN Rules (IKE): Gateway Policy: Edit .....	320
Table 102 VPN Rules (IKE): Network Policy Edit .....	326
Table 103 VPN Rules (IKE): Network Policy Move .....	329
Table 104 VPN Rules (Manual) .....	330
Table 105 VPN Rules (Manual) Edit .....	332
Table 106 VPN: SA Monitor .....	335
Table 107 VPN: Global Setting .....	336
Table 108 Telecommuters Sharing One VPN Rule Example .....	338
Table 109 Telecommuters Using Unique VPN Rules Example .....	339
Table 110 My Certificates .....	344
Table 111 My Certificate Import .....	347
Table 112 My Certificate Create .....	348
Table 113 My Certificate Details .....	352
Table 114 Trusted CAs .....	354
Table 115 Trusted CA Import .....	356
Table 116 Trusted CA Details .....	357
Table 117 Trusted Remote Hosts .....	360
Table 118 Trusted Remote Host Import .....	363
Table 119 Trusted Remote Host Details .....	364
Table 120 Directory Servers .....	367
Table 121 Directory Server Add .....	368
Table 122 Local User Database .....	372
Table 123 RADIUS .....	373
Table 124 NAT Definitions .....	374

Table 125 NAT Mapping Types .....	378
Table 126 NAT Overview .....	379
Table 127 NAT Address Mapping .....	381
Table 128 NAT Address Mapping Edit .....	383
Table 129 Services and Port Numbers .....	384
Table 130 Port Forwarding .....	387
Table 131 Port Triggering .....	389
Table 132 IP Static Route .....	393
Table 133 IP Static Route Edit .....	394
Table 134 Policy Route Summary .....	398
Table 135 Edit IP Policy Route .....	399
Table 136 Application and Subnet-based Bandwidth Management Example .....	404
Table 137 Maximize Bandwidth Usage Example .....	405
Table 138 Priority-based Allotment of Unused and Unbudgeted Bandwidth Example .....	406
Table 139 Fairness-based Allotment of Unused and Unbudgeted Bandwidth Example .....	406
Table 140 Bandwidth Borrowing Example .....	407
Table 141 Bandwidth Management: Summary .....	409
Table 142 Bandwidth Management: Class Setup .....	410
Table 143 Bandwidth Management: Edit Class .....	412
Table 144 Services and Port Numbers .....	414
Table 145 Bandwidth Management: Statistics .....	415
Table 146 Bandwidth Management: Monitor .....	416
Table 147 System DNS .....	421
Table 148 System DNS: Add Address Record .....	423
Table 149 System DNS: Insert Name Server Record .....	424
Table 150 DNS Cache .....	425
Table 151 DNS DHCP .....	427
Table 152 DDNS .....	429
Table 153 WWW .....	435
Table 154 SSH .....	443
Table 155 Telnet .....	447
Table 156 FTP .....	448
Table 157 SNMP Traps .....	450
Table 158 SNMP .....	451
Table 159 DNS .....	452
Table 160 CNM .....	453
Table 161 UPnP .....	457
Table 162 UPnP Ports .....	459
Table 163 ALG .....	471
Table 164 View Log .....	473
Table 165 Example Log Description .....	473
Table 166 Log Settings .....	477
Table 167 Reports .....	479

Table 168 Web Site Hits Report .....	480
Table 169 Protocol/ Port Report .....	481
Table 170 Host IP Address Report .....	482
Table 171 Report Specifications .....	483
Table 172 General Setup .....	485
Table 173 Password Setup .....	486
Table 174 Time and Date .....	487
Table 175 Default Time Servers .....	489
Table 176 MAC-address-to-port Mapping Table .....	491
Table 177 Device Mode (Router Mode) .....	492
Table 178 Device Mode (Bridge Mode) .....	493
Table 179 Firmware Upload .....	495
Table 180 Restore Configuration .....	497
Table 181 Main Menu Commands .....	501
Table 182 Main Menu Summary .....	503
Table 183 SMT Menus Overview .....	504
Table 184 Menu 1: General Setup (Router Mode) .....	508
Table 185 Menu 1: General Setup (Bridge Mode) .....	509
Table 186 Menu 1.1: Configure Dynamic DNS .....	510
Table 187 Menu 1.1.1: DDNS Host Summary .....	511
Table 188 Menu 1.1.1: DDNS Edit Host .....	512
Table 189 MAC Address Cloning in WAN Setup .....	515
Table 190 Menu 2: Dial Backup Setup .....	516
Table 191 Advanced WAN Port Setup: AT Commands Fields .....	517
Table 192 Advanced WAN Port Setup: Call Control Parameters .....	518
Table 193 Menu 11.3: Remote Node Profile (Backup ISP) .....	519
Table 194 Menu 11.3.1: Remote Node PPP Options .....	521
Table 195 Menu 11.3.2: Remote Node Network Layer Options .....	522
Table 196 Menu 11.3.3: Remote Node Script .....	525
Table 197 Menu 3.2: DHCP Ethernet Setup Fields .....	528
Table 198 Menu 3.2: LAN TCP/IP Setup Fields .....	529
Table 199 Menu 3.2.1: IP Alias Setup .....	530
Table 200 Menu 4: Internet Access Setup (Ethernet) .....	533
Table 201 New Fields in Menu 4 (PPTP) Screen .....	534
Table 202 New Fields in Menu 4 (PPPoE) screen .....	535
Table 203 Menu 6.1: Route Assessment .....	541
Table 204 Menu 6.2: Traffic Redirect .....	541
Table 205 Menu 6.3: Route Failover .....	542
Table 206 Menu 7.1: Wireless Setup .....	545
Table 207 Menu 7.1.1: WLAN MAC Address Filter .....	546
Table 208 Menu 11.1: Remote Node Profile for Ethernet Encapsulation .....	552
Table 209 Fields in Menu 11.1 (PPPoE Encapsulation Specific) .....	554
Table 210 Menu 11.1: Remote Node Profile for PPTP Encapsulation .....	555

Table 211 Remote Node Network Layer Options Menu Fields .....	556
Table 212 Menu 11.1.5: Traffic Redirect Setup .....	559
Table 213 Menu 12. 1: Edit IP Static Route .....	561
Table 214 Applying NAT in Menus 4 & 11.1.2 .....	564
Table 215 SUA Address Mapping Rules .....	566
Table 216 Fields in Menu 15.1.1 .....	567
Table 217 Menu 15.1.1.1: Editing/Configuring an Individual Rule in a Set .....	568
Table 218 15.2.1.2: NAT Server Configuration .....	571
Table 219 Menu 15.3.1: Trigger Port Setup .....	580
Table 220 Abbreviations Used in the Filter Rules Summary Menu .....	588
Table 221 Rule Abbreviations Used .....	588
Table 222 Menu 21.1.1.1: TCP/IP Filter Rule .....	589
Table 223 Generic Filter Rule Menu Fields .....	592
Table 224 SNMP Configuration Menu Fields .....	598
Table 225 SNMP Traps .....	599
Table 226 System Maintenance: Status Menu Fields .....	601
Table 227 Fields in System Maintenance: Information .....	603
Table 228 System Maintenance Menu Syslog Parameters .....	605
Table 229 System Maintenance Menu Diagnostic .....	610
Table 230 Filename Conventions .....	613
Table 231 General Commands for GUI-based FTP Clients .....	615
Table 232 General Commands for GUI-based TFTP Clients .....	617
Table 233 Valid Commands .....	629
Table 234 Budget Management .....	631
Table 235 Call History .....	632
Table 236 Menu 24.10 System Maintenance: Time and Date Setting .....	634
Table 237 Menu 24.11 – Remote Management Control .....	637
Table 238 Menu 25: Sample IP Routing Policy Summary .....	640
Table 239 IP Routing Policy Setup .....	641
Table 240 Menu 25.1: IP Routing Policy Setup .....	642
Table 241 Menu 25.1.1: IP Routing Policy Setup .....	644
Table 242 Schedule Set Setup .....	649
Table 243 Troubleshooting the Start-Up of Your ZyWALL .....	652
Table 244 Troubleshooting the LAN Interface .....	652
Table 245 Troubleshooting the DMZ Interface .....	653
Table 246 Troubleshooting the WAN Interface .....	653
Table 247 Troubleshooting Accessing the ZyWALL .....	654
Table 248 Device Specifications .....	664
Table 249 Performance .....	665
Table 250 Firmware Features .....	665
Table 251 Feature Specifications .....	667
Table 252 Compatible ZyXEL WLAN Cards and Security Features .....	668
Table 253 Console/Dial Backup Port Pin Assignments .....	670

Table 254 Classes of IP Addresses .....	694
Table 255 Allowed IP Address Range By Class .....	695
Table 256 "Natural" Masks .....	695
Table 257 Alternative Subnet Mask Notation .....	696
Table 258 Two Subnets Example .....	696
Table 259 Subnet 1 .....	697
Table 260 Subnet 2 .....	697
Table 261 Subnet 1 .....	698
Table 262 Subnet 2 .....	698
Table 263 Subnet 3 .....	698
Table 264 Subnet 4 .....	699
Table 265 Eight Subnets .....	699
Table 266 Class C Subnet Planning .....	699
Table 267 Class B Subnet Planning .....	700
Table 268 IEEE802.11g .....	712
Table 269 Comparison of EAP Authentication Types .....	718
Table 270 Wireless Security Relational Matrix .....	719
Table 271 Firewall Commands .....	756
Table 272 NetBIOS Filter Default Settings .....	763
Table 273 Certificates Commands .....	766
Table 274 Brute-Force Password Guessing Protection Commands .....	770
Table 275 System Maintenance Logs .....	774
Table 276 System Error Logs .....	775
Table 277 Access Control Logs .....	776
Table 278 TCP Reset Logs .....	777
Table 279 Packet Filter Logs .....	777
Table 280 ICMP Logs .....	778
Table 281 CDR Logs .....	778
Table 282 PPP Logs .....	778
Table 283 UPnP Logs .....	779
Table 284 Content Filtering Logs .....	779
Table 285 Attack Logs .....	780
Table 286 Remote Management Logs .....	781
Table 287 Wireless Logs .....	782
Table 288 IPSec Logs .....	782
Table 289 IKE Logs .....	783
Table 290 PKI Logs .....	786
Table 291 Certificate Path Verification Failure Reason Codes .....	787
Table 292 802.1X Logs .....	787
Table 293 ACL Setting Notes .....	788
Table 294 ICMP Notes .....	789
Table 295 IDP Logs .....	790
Table 296 AV Logs .....	791

Table 297 AS Logs .....	792
Table 298 Syslog Logs .....	794
Table 299 RFC-2408 ISAKMP Payload Types .....	795

# Preface

Congratulations on your purchase of the ZyWALL.

**Note:** Register your product online to receive e-mail notices of firmware upgrades and information at [www.zyxel.com](http://www.zyxel.com) for global products, or at [www.us.zyxel.com](http://www.us.zyxel.com) for North American products.

Your ZyWALL is easy to install and configure.

## About This User's Guide

This manual is designed to guide you through the configuration of your ZyWALL for its various applications. The web configurator parts of this guide contain background information on features configurable by web configurator. The SMT parts of this guide contain background information solely on features not configurable by web configurator.

**Note:** Use the web configurator, System Management Terminal (SMT) or command interpreter interface to configure your ZyWALL. Not all features can be configured through all interfaces.

## Related Documentation

- Supporting Disk

Refer to the included CD for support documents.

- Quick Start Guide

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

- Web Configurator Online Help

Embedded web help for descriptions of individual screens and supplementary information.

- ZyXEL Glossary and Web Site

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

## User Guide Feedback











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



## Syntax Conventions

- “Enter” means for you to type one or more characters. “Select” or “Choose” means for you to use one predefined choices.
- The SMT menu titles and labels are in **Bold Times New Roman** font. Predefined field choices are in **Bold Arial** font. Command and arrow keys are enclosed in square brackets. [ENTER] means the Enter, or carriage return key; [ESC] means the Escape key and [SPACE BAR] means the Space Bar.
- Mouse action sequences are denoted using a comma. For example, “In Windows, click **Start**, **Settings** and then **Control Panel**” means first click the **Start** button, then point your mouse pointer to **Settings** and then click **Control Panel**.
- “e.g.,” is a shorthand for “for instance”, and “i.e.,” means “that is” or “in other words”.

## Graphics Icons Key

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

# CHAPTER 1

## Getting to Know Your ZyWALL

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

### 1.1 ZyWALL Internet Security Appliance Overview

The ZyWALL is loaded with security features including VPN, firewall, content filtering, anti-spam, IDP (Intrusion Detection and Prevention), anti-virus and certificates. The ZyWALL's De-Militarized Zone (DMZ) increases LAN security by providing separate ports for connecting publicly accessible servers. The ZyWALL 70 and ZyWALL 35 are designed for medium sized business that need the increased throughput and reliability of dual WAN ports and load balancing. The ZyWALL 35 and ZyWALL 5 provide the option to change port roles from LAN to DMZ.

You can also deploy the ZyWALL as a transparent firewall in an existing network with minimal configuration.

The ZyWALL provides bandwidth management, NAT, port forwarding, policy routing (not available for the ZyWALL 5), DHCP server and many other powerful features.

The PCMCIA/CardBus slot allows you to add a 802.11b/g-compliant wireless LAN. You can use the wireless card as part of the LAN, DMZ or WLAN. The ZyWALL offers highly secured wireless connectivity to your wired network with IEEE 802.1x, WEP data encryption, WPA (Wi-Fi Protected Access) and MAC address filtering.

### 1.2 ZyWALL Features

The following table lists model specific features.

**Note:** See the product specifications in the appendix for detailed features and standards support.

**Table 1** Model Specific Features

FEATURE	MODEL	ZyWALL 5	ZyWALL 35	ZyWALL 70
Multiple WAN			○	○
Load Balancing			○	○
Changing Port Roles between the LAN and DMZ		○	○	
Policy Route			○	○

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

## 1.2.1 Physical Features

### LAN Port

The 10/100 Mbps auto-negotiating Ethernet LAN port allows the ZyWALL to detect the speed of incoming transmissions and adjust appropriately without manual intervention. It allows data transfer of either 10 Mbps or 100 Mbps in either half-duplex or full-duplex mode depending on your Ethernet network. The port is also auto-crossover (MDI/MDI-X) meaning it automatically adjusts to either a crossover or straight-through Ethernet cable.

### DMZ Ports

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

The 10/100 Mbps auto-negotiating Ethernet ports allow the ZyWALL to detect the speed of incoming transmissions and adjust appropriately without manual intervention. It allows data transfer of either 10 Mbps or 100 Mbps in either half-duplex or full-duplex mode depending on your Ethernet network. The ports are also auto-crossover (MDI/MDI-X) meaning they automatically adjust to either a crossover or straight-through Ethernet cable.

### WLAN Ports

You can set some of the Ethernet ports to a WLAN port role. This allows you to connect wireless LAN Access Points (APs) to extend the ZyWALL's wireless LAN coverage area.

### Dual Auto-negotiating 10/100 Mbps Ethernet WAN (single on the ZyWALL 5)

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

The 10/100 Mbps auto-negotiating Ethernet ports allow the ZyWALL to detect the speed of incoming transmissions and adjust appropriately without manual intervention. They allow data transfers of either 10 Mbps or 100 Mbps in either half-duplex or full-duplex mode depending on your Ethernet network. The ports are also auto-crossover (MDI/MDI-X) meaning they automatically adjust to either a crossover or straight-through Ethernet cable.

### Dial Backup WAN

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

## Time and Date

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

## Reset Button

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

## Dual PCMCIA and CardBus Slot

The dual PCMCIA and CardBus slot provides the option of a wireless LAN. You can alternatively insert a ZyWALL Turbo Card to use the anti-virus and IDP features.

## IEEE 802.11 b/g Wireless LAN

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

## 1.2.2 Non-Physical Features

### Load Balancing

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

### Transparent Firewall

Transparent firewall is also known as a bridge firewall. The ZyWALL can act as a bridge and still have the capability of filtering and inspecting the packets between a router and the LAN, or two routers. You do not need to do any other changes to your existing network.

### SIP Passthrough

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

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

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

## **Bandwidth Management**

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

## **IPSec VPN Capability**

Establish a Virtual Private Network (VPN) to connect with business partners and branch offices using data encryption and the Internet to provide secure communications without the expense of leased site-to-site lines. The ZyWALL VPN is based on the IPSec standard and is fully interoperable with other IPSec-based VPN products.

## **X-Auth (Extended Authentication)**

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

## **Certificates**

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

## **SSH**

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

## **HTTPS**

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

## **Firewall**

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

## **Content Filtering**

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

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

## **Anti-Spam**

The ZyWALL's anti-spam feature helps detect and mark or discard junk e-mail (spam). The ZyWALL has a whitelist for identifying legitimate e-mail and a blacklist for identifying spam email. You can also subscribe to an anti-spam external database service that checks e-mail against more than a million known spam patterns.

## **Anti-Virus Scanner**

With the anti-virus packet scanner, your ZyWALL scans files transmitting through the enabled interfaces into the network. The ZyWALL helps stop threats at the network edge before they reach the local host computers.

## **Intrusion Detection and Prevention (IDP)**

IDP can detect and take actions on malicious or suspicious packets and traffic flows.

## **ZyWALL Turbo Card**

ZyWALL Turbo Card is a co-processor accelerator that is used in conjunction with your ZyWALL for fast, efficient IDP (Intrusion Detection and Prevention) and AV (Anti Virus) traffic inspection.

## **Universal Plug and Play (UPnP)**

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

## **RADIUS (RFC2138, 2139)**

RADIUS (Remote Authentication Dial In User Service) server enables user authentication, authorization and accounting.

## **IEEE 802.1x for Network Security**

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

## **Wi-Fi Protected Access**

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

## **Wireless LAN MAC Address Filtering**

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

## **WEP Encryption**

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

## **Packet Filtering**

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

## **Call Scheduling**

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

## **PPPoE**

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

## **PPTP Encapsulation**

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

PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet. The ZyWALL supports one PPTP server connection at any given time.

## Dynamic DNS Support

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

## IP Multicast

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

## 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, WLAN and/or DMZ interfaces via its single physical Ethernet LAN, WLAN and/or DMZ interface with the ZyWALL itself as the gateway for each network.

## IP Policy Routing

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

## Central Network Management

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

## SNMP

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

## Network Address Translation (NAT)

Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet).



## Traffic Redirect

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

## Port Forwarding

Use this feature to forward incoming service requests to a server on your local network. You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server.

## DHCP (Dynamic Host Configuration Protocol)

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

## Full Network Management

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

## RoadRunner Support

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

## Logging and Tracing

Built-in message logging and packet tracing.

Syslog facility support.

## Upgrade ZyWALL Firmware via LAN

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

## Embedded FTP and TFTP Servers

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

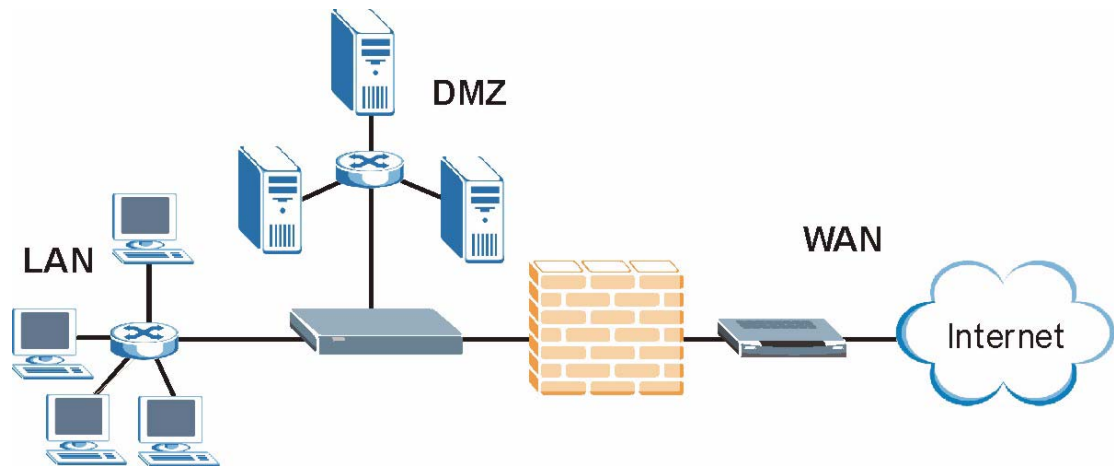
## 1.3 Applications for the ZyWALL

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

### 1.3.1 Secure Broadband Internet Access via Cable or DSL Modem

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

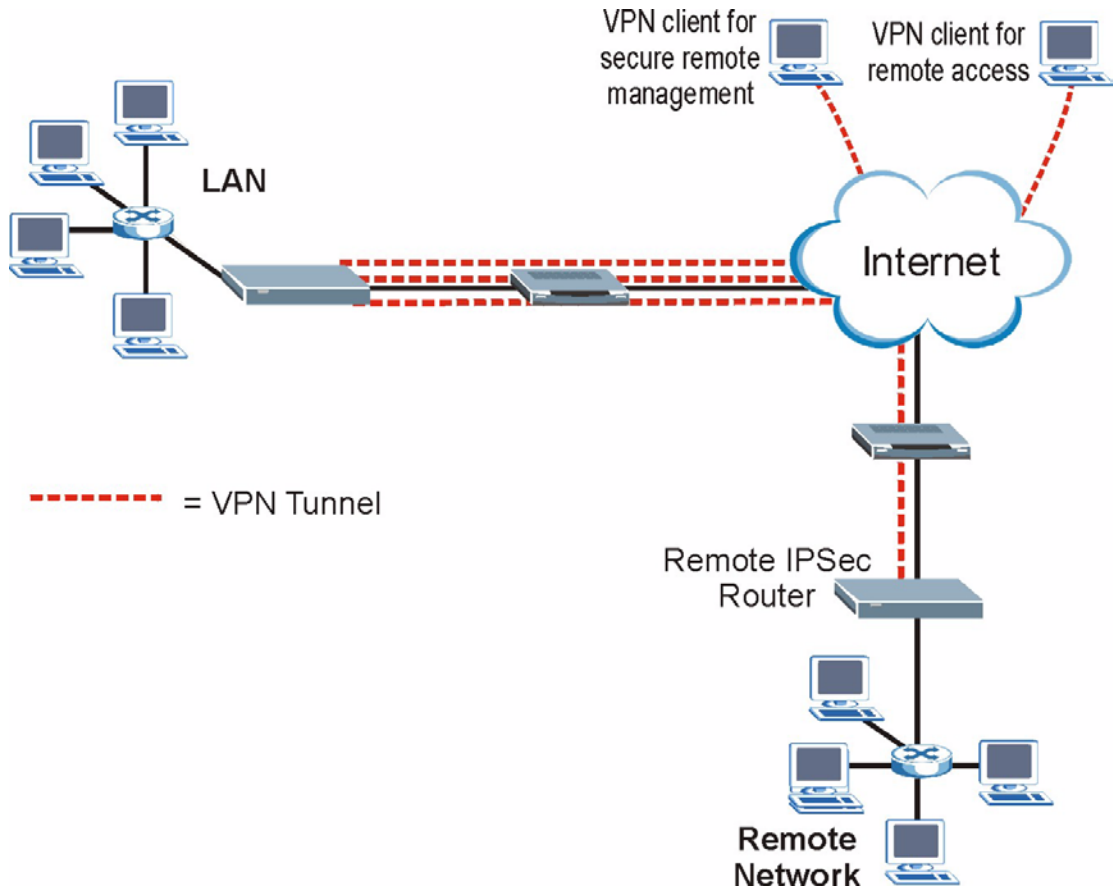
**Figure 1** Secure Internet Access via Cable, DSL or Wireless Modem



### 1.3.2 VPN Application

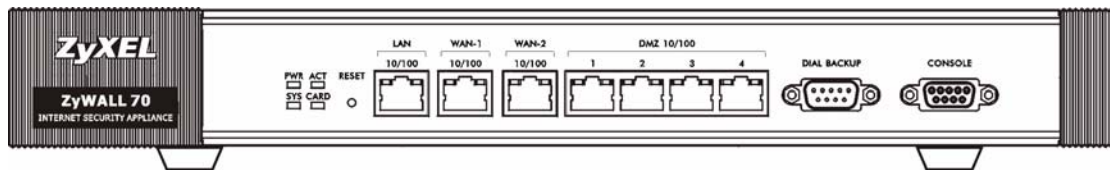
ZyWALL VPN is an ideal cost-effective way to connect branch offices and business partners over the Internet without the need (and expense) for leased lines between sites.

**Figure 2** VPN Application

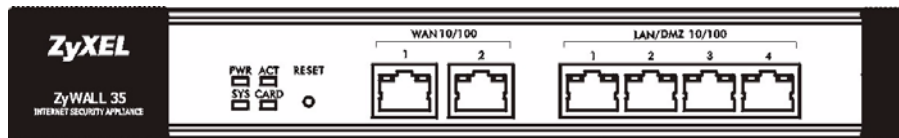


### 1.3.3 Front Panel LEDs

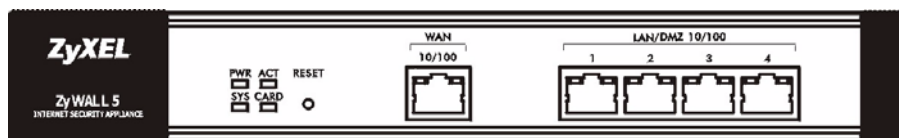
**Figure 3** ZyWALL 70 Front Panel



**Figure 4** ZyWALL 35 Front Panel



**Figure 5** ZyWALL 5 Front Panel



The following table describes the LEDs.

**Table 2** Front Panel LEDs

LED	COLOR	STATUS	DESCRIPTION	
<b>PWR</b>		Off	The ZyWALL is turned off.	
	Green	On	The ZyWALL is turned on.	
	Red	On	The power to the ZyWALL is too low.	
<b>SYS</b>	Green	Off	The ZyWALL is not ready or has failed.	
		On	The ZyWALL is ready and running.	
		Flashing	The ZyWALL is restarting.	
<b>ACT</b>	Green	Off	The backup port is not connected.	
		Flashing	The backup port is sending or receiving packets.	
<b>CARD</b>	Green	Off	The wireless LAN is not ready, or has failed.	
		On	The wireless LAN is ready.	
		Flashing	The wireless LAN is sending or receiving packets.	
<b>LAN 10/100</b> (ZyWALL 70 only)		Off	The LAN/DMZ is not connected.	
		Green	On	The ZyWALL has a successful 10Mbps Ethernet connection.
			Flashing	The 10M LAN is sending or receiving packets.
		Orange	On	The ZyWALL has a successful 100Mbps Ethernet connection.
Flashing	The 100M LAN is sending or receiving packets.			
<b>WAN1/2 10/100</b> or <b>WAN 10/100</b>		Off	The WAN connection is not ready, or has failed.	
		Green	On	The ZyWALL has a successful 10Mbps WAN connection.
			Flashing	The 10M WAN is sending or receiving packets.
		Orange	On	The ZyWALL has a successful 100Mbps WAN connection.
Flashing	The 100M WAN is sending or receiving packets.			
<b>DMZ 10/100</b> (ZyWALL 70 only)		Off	The LAN/DMZ is not connected.	
		Green	On	The ZyWALL has a successful 10Mbps Ethernet connection.
			Flashing	The 10M LAN is sending or receiving packets.
		Orange	On	The ZyWALL has a successful 100Mbps Ethernet connection.
Flashing	The 100M LAN is sending or receiving packets.			
<b>LAN/DMZ 10/100</b> (ZyWALL 35 and ZyWALL 5)		Off	The LAN/DMZ is not connected.	
		Green	On	The ZyWALL has a successful 10Mbps Ethernet connection.
			Flashing	The 10M LAN is sending or receiving packets.
		Orange	On	The ZyWALL has a successful 100Mbps Ethernet connection.
Flashing	The 100M LAN is sending or receiving packets.			



# CHAPTER 2

## Introducing the Web Configurator

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

### 2.1 Web Configurator Overview

The web configurator is an HTML-based management interface that allows easy ZyWALL setup and management via Internet browser. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

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

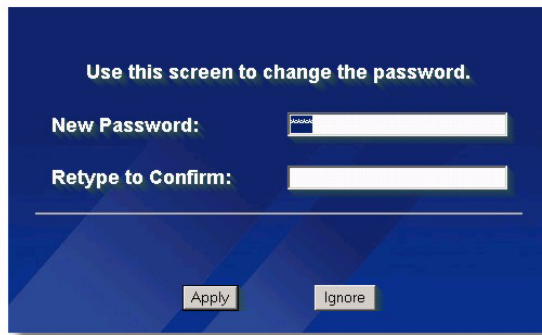
- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

See the **Troubleshooting** chapter if you want to make sure these functions are allowed in Internet Explorer or Netscape Navigator.

### 2.2 Accessing the ZyWALL Web Configurator

**Note:** By default, the packets from WLAN to WLAN/ZyWALL are dropped and users cannot configure the ZyWALL wirelessly.

- 1** Make sure your ZyWALL hardware is properly connected and prepare your computer/ computer network to connect to the ZyWALL (refer to the Quick Start Guide).
- 2** Launch your web browser.
- 3** Type "192.168.1.1" as the URL.
- 4** Type "1234" (default) as the password and click **Login**. In some versions, the default password appears automatically - if this is the case, click **Login**.
- 5** You should see a screen asking you to change your password (highly recommended) as shown next. Type a new password (and retype it to confirm) and click **Apply** or click **Ignore**.

**Figure 6** Change Password Screen

Use this screen to change the password.

New Password:

Retype to Confirm:

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

**Note:** If you do not replace the default certificate here or in the **CERTIFICATES** screen, this screen displays every time you access the web configurator.

**Figure 7** Replace Certificate Screen

Replace Factory Default Certificate

The factory default certificate is common to all ZyWALL models. Click Apply to create a certificate using your ZyWALL's MAC address that will be specific to this device.

**7** You should now see the **HOME** screen (see [Figure 9 on page 69](#)).

**Note:** The management session automatically times out when the time period set in the **Administrator Inactivity Timer** field expires (default five minutes). Simply log back into the ZyWALL if this happens to you.

## 2.3 Resetting the ZyWALL

If you forget your password or cannot access the web configurator, you will need to reload the factory-default configuration file or use the **RESET** button on the back of the ZyWALL. Uploading this configuration file replaces the current configuration file with the factory-default configuration file. This means that you will lose all configurations that you had previously and the speed of the console port will be reset to the default of 9600bps with 8 data bit, no parity, one stop bit and flow control set to none. The password will be reset to 1234, also.

### 2.3.1 Procedure To Use The Reset Button

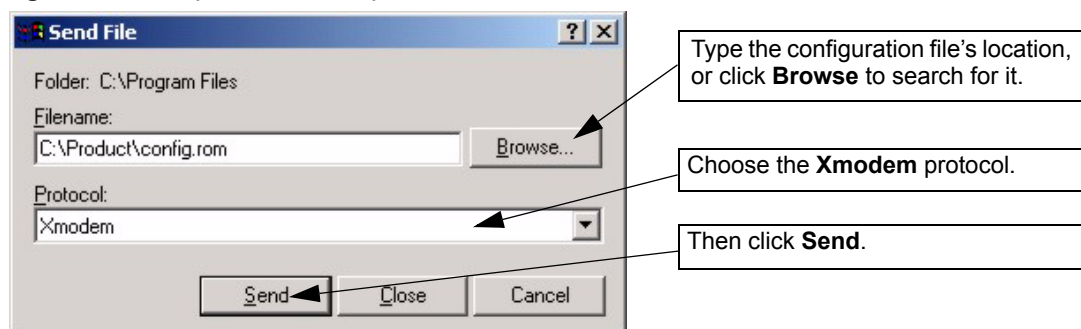
Make sure the **SYS LED** is on (not blinking) before you begin this procedure.

- 1 Press the **RESET** button for ten seconds, and then release it. If the **SYS LED** begins to blink, the defaults have been restored and the ZyWALL restarts. Otherwise, go to step 2.
- 2 Turn the ZyWALL off.
- 3 While pressing the **RESET** button, turn the ZyWALL on.
- 4 Continue to hold the **RESET** button. The **SYS LED** will begin to blink and flicker very quickly after about 20 seconds. This indicates that the defaults have been restored and the ZyWALL is now restarting.
- 5 Release the **RESET** button and wait for the ZyWALL to finish restarting.

### 2.3.2 Uploading a Configuration File Via Console Port

- 1 Download the default configuration file from the ZyXEL FTP site, unzip it and save it in a folder.
- 2 Turn off the ZyWALL, begin a terminal emulation software session and turn on the ZyWALL again. When you see the message "Press Any key to enter Debug Mode within 3 seconds", press any key to enter debug mode.
- 3 Enter "y" at the prompt below to go into debug mode.
- 4 Enter "atlc" after "Enter Debug Mode" message.
- 5 Wait for "Starting XMODEM upload" message before activating Xmodem upload on your terminal. This is an example Xmodem configuration upload using HyperTerminal.

**Figure 8** Example Xmodem Upload




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

## 2.4 Navigating the ZyWALL Web Configurator

The following summarizes how to navigate the web configurator from the **HOME** screen. This guide uses the ZyWALL 70 screenshots as an example. The screens may vary slightly for different ZyWALL models.



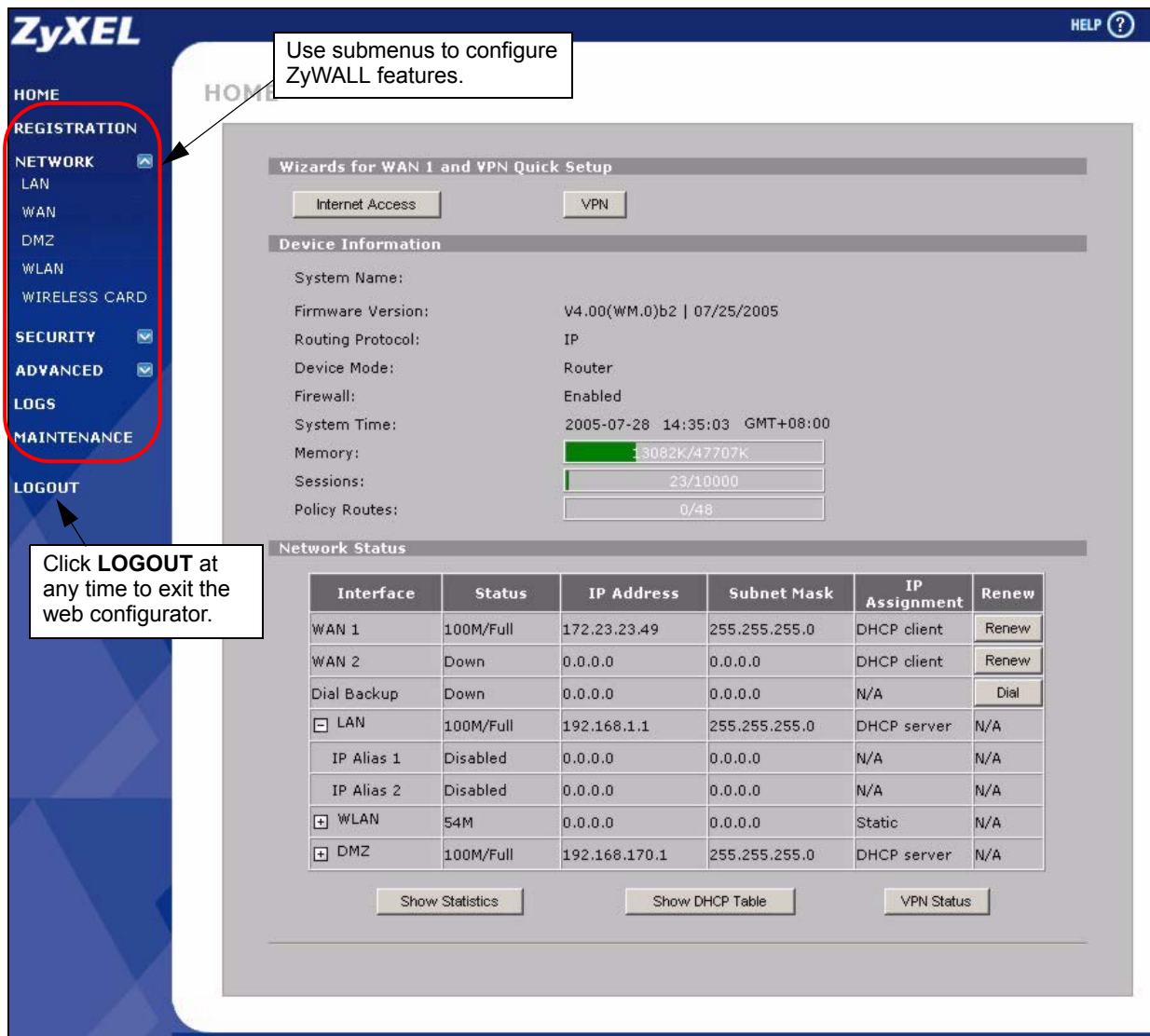
**Note:** Follow the instructions you see in the **HOME** screen or click the  icon.

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

## 2.4.1 Router Mode

The following screen displays when the ZyWALL is set to router mode. The ZyWALL is set to router mode by default. Not all fields are available on all models.

**Figure 9** Web Configurator HOME Screen in Router Mode



Use submenus to configure ZyWALL features.

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

Interface	Status	IP Address	Subnet Mask	IP Assignment	Renew
WAN 1	100M/Full	172.23.23.49	255.255.255.0	DHCP client	Renew
WAN 2	Down	0.0.0.0	0.0.0.0	DHCP client	Renew
Dial Backup	Down	0.0.0.0	0.0.0.0	N/A	Dial
<input type="checkbox"/> LAN	100M/Full	192.168.1.1	255.255.255.0	DHCP server	N/A
IP Alias 1	Disabled	0.0.0.0	0.0.0.0	N/A	N/A
IP Alias 2	Disabled	0.0.0.0	0.0.0.0	N/A	N/A
<input type="checkbox"/> WLAN	54M	0.0.0.0	0.0.0.0	Static	N/A
<input type="checkbox"/> DMZ	100M/Full	192.168.170.1	255.255.255.0	DHCP server	N/A

The following table describes the labels in this screen.

**Table 3** Web Configurator HOME Screen in Router Mode

LABEL	DESCRIPTION
Wizards for WAN 1 (WAN) and VPN Quick Setup	
Internet Access	Click <b>Internet Access</b> to use the initial configuration wizard. This configures WAN1 on a ZyWALL with multiple WAN ports or the WAN port on a ZyWALL with a single WAN port.
VPN	Click <b>VPN</b> to create VPN policies.
Device Information	
System Name	This is the <b>System Name</b> you enter in the <b>MAINTENANCE General</b> screen. It is for identification purposes.
Firmware Version	This is the ZyNOS Firmware version and the date created. ZyNOS is ZyXEL's proprietary Network Operating System design.
Routing Protocol	This shows the routing protocol - <b>IP</b> for which the ZyWALL is configured. This field is not configurable.
Device Mode	This displays whether the ZyWALL is functioning as a router or a bridge.
Firewall	This displays whether or not the ZyWALL's firewall is activated.
System Time	This field displays your ZyWALL's present date and time along with the difference from the Greenwich Mean Time (GMT) zone. The difference from GMT is based on the time zone. It is also adjusted for Daylight Saving Time if you set the ZyWALL to use it.
Memory	<p>The first number shows how many kilobytes of the heap memory the ZyWALL is using. Heap memory refers to the memory that is not used by ZyNOS (ZyXEL Network Operating System) and is thus available for running processes like NAT, VPN and the firewall.</p> <p>The second number shows the ZyWALL's total heap memory (in kilobytes).</p> <p>The bar displays what percent of the ZyWALL's heap memory is in use. The bar turns from green to red when the maximum is being approached.</p>
Sessions	<p>The first number shows how many sessions are currently open on the ZyWALL. This includes all sessions that are currently:</p> <ul style="list-style-type: none"> <li>• Traversing the ZyWALL</li> <li>• Terminating at the ZyWALL</li> <li>• Initiated from the ZyWALL</li> </ul> <p>The second number is the maximum number of sessions that can be open at one time.</p> <p>The bar displays what percent of the maximum number of sessions is in use. The bar turns from green to red when the maximum is being approached.</p>
Policy Routes	<p>The first number shows how many policy routes you have configured.</p> <p>The second number shows the maximum number of policy routes that you can configure on the ZyWALL.</p> <p>The bar displays what percent of the ZyWALL's possible policy routes are configured. The bar turns from green to red when the maximum is being approached.</p>
Network Status	

**Table 3** Web Configurator HOME Screen in Router Mode (continued)

LABEL	DESCRIPTION
Interface	<p>This is the port type.</p> <p>Port types for a ZyWALL with multiple WAN ports are: <b>WAN1, WAN2, Dial Backup, LAN, WLAN</b> and <b>DMZ</b>.</p> <p>Port types for a ZyWALL with a single WAN port are: <b>WAN, Dial Backup, LAN, WLAN</b> and <b>DMZ</b>.</p> <p>Click "+" to expand or "-" to collapse the LAN, WLAN (when the wireless card is part of the WLAN in the <b>Port Roles</b> screen), and DMZ IP alias drop-down lists.</p>
Status	<p>For the LAN and DMZ ports, this displays the port speed and duplex setting.</p> <p>For the WAN and Dial Backup ports, it displays the port speed and duplex setting if you're using Ethernet encapsulation and <b>Down</b> (line is down or not connected), <b>Idle</b> (line (ppp) idle), <b>Dial</b> (starting to trigger a call) or <b>Drop</b> (dropping a call) if you're using PPPoE encapsulation.</p> <p>For the WLAN port, it displays the transmission rate when a wireless LAN card is inserted and WLAN is enabled or <b>Down</b> when a wireless LAN card is not inserted or WLAN is disabled.</p>
IP Address	This shows the port's IP address.
Subnet Mask	This shows the port's subnet mask.
IP Assignment	<p>This shows the WAN port's DHCP role - <b>DHCP Client</b> or <b>Static</b>.</p> <p>This shows the LAN, WLAN or DMZ port's DHCP role - <b>DHCP Server, DHCP Relay</b> or <b>Static</b>.</p> <p>This shows <b>N/A</b> for the Dial Backup port and the WLAN port when you set the wireless card to be part of the DMZ or LAN in the <b>Port Roles</b> screen.</p>
Renew	If you are using Ethernet encapsulation and the WAN port is configured to get the IP address automatically from the ISP, click <b>Renew</b> to release the WAN port's dynamically assigned IP address and get the IP address afresh. Click <b>Dial</b> to dial up the PPTP, PPPoE or dial backup connection.
Show Statistics	Click <b>Show Statistics</b> to see router performance statistics such as the number of packets sent and number of packets received for each port, including WAN (or WAN1, WAN2), Dial Backup, LAN, WLAN and DMZ.
Show DHCP Table	Click <b>Show DHCP Table</b> to show current DHCP client information.
VPN Status	Click <b>VPN Status</b> to display the active VPN connections.

## 2.4.2 Bridge Mode

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

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

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

**Figure 10** Web Configurator HOME Screen in Bridge Mode

The screenshot shows the 'HOME' page of the ZyWALL Web Configurator in Bridge Mode. It features several sections:

- Wizards for VPN Quick Setup:** A button labeled 'VPN'.
- Device Information:**
  - System Name:
  - Firmware Version: V4.00(WM.0)b2 | 07/25/2005
  - Device Mode: Bridge
  - Firewall: Enabled
  - System Time: 2005-07-29 10:02:33 GMT+08:00
  - Memory: 12694K/47707K (with a green progress bar)
  - Sessions: 6/10000 (with a green progress bar)
- Network Status:**
  - IP Address: 192.168.1.1
  - Subnet Mask: 255.255.255.0
  - Gateway IP Address: 0.0.0.0
  - Rapid Spanning Tree Protocol: Disabled
  - Bridge Priority: 250
  - Bridge Hello Time: 2 second(s)
  - Bridge Max Age: 20 second(s)
  - Forward Delay: 15 second(s)
- Bridge Port Table:**

Bridge Port	Port Status	RSTP Status	RSTP Active	RSTP Priority	RSTP Path Cost
WAN1	Down	N/A	No	128	250
WAN2	Down	N/A	No	128	250
LAN	100M/Full	N/A	No	128	250
Wireless Card	Down	N/A	No	128	250
DMZ	100M/Full	N/A	No	128	250
WLAN Interface	100M/Full	N/A	No	128	250
- Buttons:** 'Show Statistics' and 'VPN Status'.

The following table describes the labels in this screen.

**Table 4** Web Configurator HOME Screen in Bridge Mode

LABEL	DESCRIPTION
Wizards for VPN Quick Setup	
VPN	Click <b>VPN</b> to create VPN policies.
Device Information	
System Name	This is the <b>System Name</b> you enter in the <b>MAINTENANCE General</b> screen. It is for identification purposes.

**Table 4** Web Configurator HOME Screen in Bridge Mode (continued)

LABEL	DESCRIPTION
Firmware Version	This is the ZyNOS Firmware version and the date created. ZyNOS is ZyXEL's proprietary Network Operating System design.
Device Mode	This displays whether the ZyWALL is functioning as a router or a bridge.
Firewall	This displays whether or not the ZyWALL's firewall is activated.
System Time	This field displays your ZyWALL's present date and time along with the difference from the Greenwich Mean Time (GMT) zone. The difference from GMT is based on the time zone. It is also adjusted for Daylight Saving Time if you set the ZyWALL to use it.
Memory	<p>The first number shows how many kilobytes of the heap memory the ZyWALL is using. Heap memory refers to the memory that is not used by ZyNOS (ZyXEL Network Operating System) and is thus available for running processes like NAT, VPN and the firewall.</p> <p>The second number shows the ZyWALL's total heap memory (in kilobytes).</p> <p>The bar displays what percent of the ZyWALL's heap memory is in use. The bar turns from green to red when the maximum is being approached.</p>
Sessions	<p>The first number shows how many sessions are currently open on the ZyWALL. This includes all sessions that are currently:</p> <ul style="list-style-type: none"> <li>• Traversing the ZyWALL</li> <li>• Terminating at the ZyWALL</li> <li>• Initiated from the ZyWALL</li> </ul> <p>The second number is the maximum number of sessions that can be open at one time.</p> <p>The bar displays what percent of the maximum number of sessions is in use. The bar turns from green to red when the maximum is being approached.</p>
Network Status	
IP Address	This is the IP address of your ZyWALL in dotted decimal notation.
Subnet Mask	This is the IP subnet mask of the ZyWALL.
Gateway IP Address	This is the gateway IP address.
Rapid Spanning Tree Protocol	This shows whether RSTP (Rapid Spanning Tree Protocol) is active or not. The following labels or values relative to RSTP do not apply when RSTP is disabled.
Bridge Priority	This is the bridge priority of the ZyWALL.
Bridge Hello Time	This is the interval of BPDUs (Bridge Protocol Data Units) from the root bridge.
Bridge Max Age	This is the predefined interval that a bridge waits to get a Hello message (BPDU) from the root bridge.
Forward Delay	This is the forward delay interval.
Bridge Port	This is the port type. Port types are: <b>WAN</b> (or <b>WAN1</b> , <b>WAN2</b> ), <b>LAN</b> , <b>Wireless Card</b> , <b>DMZ</b> and <b>WLAN Interface</b> .
Port Status	For the WAN, LAN, DMZ, and WLAN Interfaces, this displays the port speed and duplex setting. For the WAN port, it displays <b>Down</b> when the link is not ready or has failed. For the wireless card, it displays the transmission rate when a wireless LAN card is inserted and WLAN is enabled or <b>Down</b> when a wireless LAN is not inserted or WLAN is disabled.
RSTP Status	This is the RSTP status of the corresponding port.
RSTP Active	This shows whether or not RSTP is active on the corresponding port.
RSTP Priority	This is the RSTP priority of the corresponding port.

**Table 4** Web Configurator HOME Screen in Bridge Mode (continued)

LABEL	DESCRIPTION
RSTP Path Cost	This is the cost of transmitting a frame from the root bridge to the corresponding port.
Show Statistics	Click <b>Show Statistics</b> to see bridge performance statistics such as the number of packets sent and number of packets received for each port, including WAN (or WAN1, WAN2), Dial Backup, LAN, WLAN and DMZ.
VPN Status	Click <b>VPN Status</b> to display the active VPN connections.

### 2.4.3 Navigation Panel

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

The following table lists the features available for each device mode. Not all ZyWALLs have all features listed in this table.

**Table 5** Bridge and Router Mode Features Comparison

FEATURE	BRIDGE MODE	ROUTER MODE
Internet Access Wizard		O
VPN Wizard	O	O
DHCP Table		O
System Statistics	O	O
Registration	O	O
LAN		O
WAN		O
DMZ		O
Bridge	O	
WLAN		O
Wireless Card	O	O
Firewall	O	O
IDP	O	O
Anti-Virus	O	O
Anti-Spam	O	O
Content Filter	O	O
VPN	O	O
Certificates	O	O
Authentication Server	O	O
NAT		O
Static Route		O
Policy Route		O
Bandwidth Management	O	O

**Table 5** Bridge and Router Mode Features Comparison

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

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

The following table describes the sub-menus.

**Table 6** Screens Summary

LINK	TAB	FUNCTION
HOME		This screen shows the ZyWALL's general device and network status information. Use this screen to access the wizards, statistics and DHCP table.
REGISTRATION	Registration	Use this screen to register your ZyWALL and activate the trial service subscriptions.
	Service	Use this to manage and update the service status and license information.
NETWORK		
LAN	LAN	Use this screen to configure LAN DHCP and TCP/IP settings.
	Static DHCP	Use this screen to assign fixed IP addresses on the LAN.
	IP Alias	Use this screen to partition your LAN interface into subnets.
	Port Roles (ZyWALL 5 and ZyWALL 35)	Use this screen to change the LAN/DMZ/WLAN port roles.
BRIDGE	Bridge	Use this screen to change the bridge settings on the ZyWALL.
	Port Roles	Use this screen to change the DMZ/WLAN port roles on the ZyWALL 70 or the LAN/DMZ/WLAN port roles on the ZyWALL 5 or ZyWALL 35.

**Table 6** Screens Summary (continued)

LINK	TAB	FUNCTION
WAN	General	This screen allows you to configure load balancing, route priority and traffic redirect properties.
	Route (ZyWALL 5 only)	This screen allows you to configure route priority.
	WAN (ZyWALL 5 only)	Use this screen to configure the WAN port for internet access.
	WAN1 (ZyWALL 35 and ZyWALL 70)	Use this screen to configure the WAN1 port for Internet access.
	WAN2 (ZyWALL 35 and ZyWALL 70)	Use this screen to configure the WAN2 port for Internet access.
	Traffic Redirect	Use this screen to configure your traffic redirect properties and parameters.
	Dial Backup	Use this screen to configure the backup WAN dial-up connection.
DMZ	DMZ	Use this screen to configure your DMZ connection.
	Static DHCP	Use this screen to assign fixed IP addresses on the DMZ.
	IP Alias	Use this screen to partition your DMZ interface into subnets.
	Port Roles	Use this screen to change the DMZ/WLAN port roles on the ZyWALL 70 or the LAN/DMZ/WLAN port roles on the ZyWALL 5 or ZyWALL 35.
WLAN	WLAN	Use this screen to configure your WLAN connection.
	Static DHCP	Use this screen to assign fixed IP addresses on the WLAN.
	IP Alias	Use this screen to partition your WLAN interface into subnets.
	Port Roles	Use this screen to change the DMZ/WLAN port roles on the ZyWALL 70 or the LAN/DMZ/WLAN port roles on the ZyWALL 5 or ZyWALL 35.
WIRELESS CARD	Wireless Card	Use this screen to configure the wireless LAN settings and WLAN authentication/security settings.
	MAC Filter	Use this screen to change MAC filter settings on the ZyWALL
SECURITY		
FIREWALL	Default Rule	Use this screen to activate/deactivate the firewall and the direction of network traffic to which to apply the rule
	Rule Summary	This screen shows a summary of the firewall rules, and allows you to edit/add a firewall rule.
	Anti-Probing	Use this screen to change your anti-probing settings.
	Threshold	Use this screen to configure the threshold for DoS attacks.



**Table 6** Screens Summary (continued)

LINK	TAB	FUNCTION
IDP	General	Use this screen to enable IDP on the ZyWALL and choose what interface(s) you want to protect from intrusions.
	Signature	Use these screens to view signatures by attack type or search for signatures by signature name, ID, severity, target operating system, action etc. You can also configure signature actions here.
	Update	Use this screen to download new signature downloads. It is important to do this as new intrusions evolve.
	Backup & Restore	Use this screen to back up, restore or revert to the default signatures' actions.
ANTI-VIRUS	General	Use this screen to activate AV scanning on the interface(s) and specify actions when a virus is detected.
	Update	Use this screen to view the version number of the current signatures and configure the signature update schedule.
ANTI-SPAM	General	Use this screen to turn the anti-spam feature on or off and set how the ZyWALL treats spam.
	External DB	Use this screen to enable or disable the use of the anti-spam external database.
	Customization	Use this screen to configure the whitelist to identify legitimate e-mail and configure the blacklist to identify spam e-mail.
CONTENT FILTER	General	This screen allows you to enable content filtering and block certain web features.
	Categories	Use this screen to select which categories of web pages to filter out, as well as to register for external database content filtering and view reports.
	Customization	Use this screen to customize the content filter list.
	Cache	Use this screen to view and configure the ZyWALL's URL caching.
VPN	VPN Rules (IKE)	Use this screen to configure VPN connections using IKE key management and view the rule summary.
	VPN Rules (Manual)	Use this screen to configure VPN connections using manual key management and view the rule summary.
	SA Monitor	Use this screen to display and manage active VPN connections.
	Global Setting	Use this screen to configure the IPSec timer settings.
CERTIFICATES	My Certificates	Use this screen to view a summary list of certificates and manage certificates and certification requests.
	Trusted CAs	Use this screen to view and manage the list of the trusted CAs.
	Trusted Remote Hosts	Use this screen to view and manage the certificates belonging to the trusted remote hosts.
	Directory Servers	Use this screen to view and manage the list of the directory servers.
AUTH SERVER	Local User Database	Use this screen to configure the local user account(s) on the ZyWALL.
	RADIUS	Configure this screen to use an external server to authenticate wireless and/or VPN users.
ADVANCED		

**Table 6** Screens Summary (continued)

LINK	TAB	FUNCTION
NAT	NAT Overview	Use this screen to enable NAT.
	Address Mapping	Use this screen to configure network address translation mapping rules.
	Port Forwarding	Use this screen to configure servers behind the ZyWALL.
	Port Triggering	Use this screen to change your ZyWALL's port triggering settings.
STATIC ROUTE	IP Static Route	Use this screen to configure IP static routes.
POLICY ROUTE	Policy Rout Summary	Use this screen to view a summary list of all the policies and configure policies for use in IP policy routing.
BW MGMT	Summary	Use this screen to enable bandwidth management on an interface.
	Class Setup	Use this screen to set up the bandwidth classes.
	Monitor	Use this screen to view the ZyWALL's bandwidth usage and allotments.
DNS	System	Use this screen to configure the address and name server records.
	Cache	Use this screen to configure the DNS resolution cache.
	DHCP	Use this screen to configure LAN/DMZ/WLAN DNS information.
	DDNS	Use this screen to set up dynamic DNS.
REMOTE MGMT	WWW	Use this screen to configure through which interface(s) and from which IP address(es) users can use HTTPS or HTTP to manage the ZyWALL.
	SSH	Use this screen to configure through which interface(s) and from which IP address(es) users can use Secure Shell to manage the ZyWALL.
	TELNET	Use this screen to configure through which interface(s) and from which IP address(es) users can use Telnet to manage the ZyWALL.
	FTP	Use this screen to configure through which interface(s) and from which IP address(es) users can use FTP to access the ZyWALL.
	SNMP	Use this screen to configure your ZyWALL's settings for Simple Network Management Protocol management.
	DNS	Use this screen to configure through which interface(s) and from which IP address(es) users can send DNS queries to the ZyWALL.
	CNM	Use this screen to configure and allow your ZyWALL to be managed by the Vantage CNM server.
UPnP	UPnP	Use this screen to enable UPnP on the ZyWALL.
	Ports	Use this screen to view the NAT port mapping rules that UPnP creates on the ZyWALL.
ALG	ALG	Use this screen to allow certain applications to pass through the ZyWALL.
LOGS	View Log	Use this screen to view the logs for the categories that you selected.
	Log Settings	Use this screen to change your ZyWALL's log settings.
	Reports	Use this screen to have the ZyWALL record and display the network usage reports.

**Table 6** Screens Summary (continued)

LINK	TAB	FUNCTION
MAINTENANCE	General	This screen contains administrative.
	Password	Use this screen to change your password.
	Time and Date	Use this screen to change your ZyWALL's time and date.
	Device Mode	Use this screen to configure and have your ZyWALL work as a router or a bridge.
	F/W Upload	Use this screen to upload firmware to your ZyWALL
	Backup & Restore	Use this screen to backup and restore the configuration or reset the factory defaults to your ZyWALL.
	Restart	This screen allows you to reboot the ZyWALL without turning the power off.
LOGOUT		Click this label to exit the web configurator.

## 2.4.4 System Statistics

Click **Show Statistics** in the **HOME** screen. Read-only information here includes port status and packet specific statistics. Also provided is "Up Time" and "poll interval(s)". The **Poll Interval(s)** field is configurable. Not all fields are available on all models.

**Figure 11** Home : Show Statistics

The following table describes the labels in this screen.

**Table 7** Home: Show Statistics

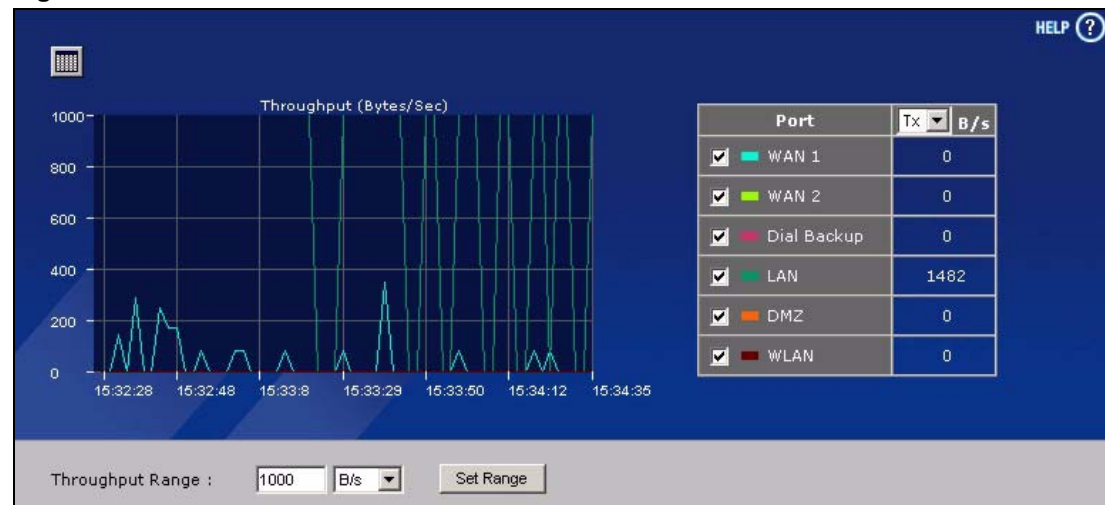
LABEL	DESCRIPTION
	Click the icon to display the chart of throughput statistics.
Port	These are the ZyWALL's interfaces.

**Table 7** Home: Show Statistics (continued)

LABEL	DESCRIPTION
Status	For the LAN and DMZ ports, this displays the port speed and duplex setting. For the WAN and Dial Backup ports, this displays the port speed and duplex setting if you're using Ethernet encapsulation and <b>Down</b> (line is down), <b>Idle</b> (line (ppp) idle), <b>Dial</b> (starting to trigger a call) or <b>Drop</b> (dropping a call) if you're using PPPoE encapsulation. For the WLAN port, it displays the transmission rate when a wireless LAN card is inserted and WLAN is enabled or <b>Down</b> when a wireless LAN is not inserted or WLAN is disabled.
TxPkts	This is the number of transmitted packets on this port.
RxPkts	This is the number of received packets on this port.
Tx B/s	This displays the transmission speed in bytes per second on this port.
Rx B/s	This displays the reception speed in bytes per second on this port.
Up Time	This is the total amount of time the line has been up.
System Up Time	This is the total time the ZyWALL has been on.
Poll Interval(s)	Enter the time interval for refreshing statistics in this field.
Set Interval	Click this button to apply the new poll interval you entered in the <b>Poll Interval(s)</b> field.
Stop	Click <b>Stop</b> to stop refreshing statistics.


## 2.4.5 Show Statistics: Line Chart

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

**Figure 12** Home : Show Statistics: Line Chart

The following table describes the labels in this screen.

**Table 8** Home: Show Statistics: Line Chart

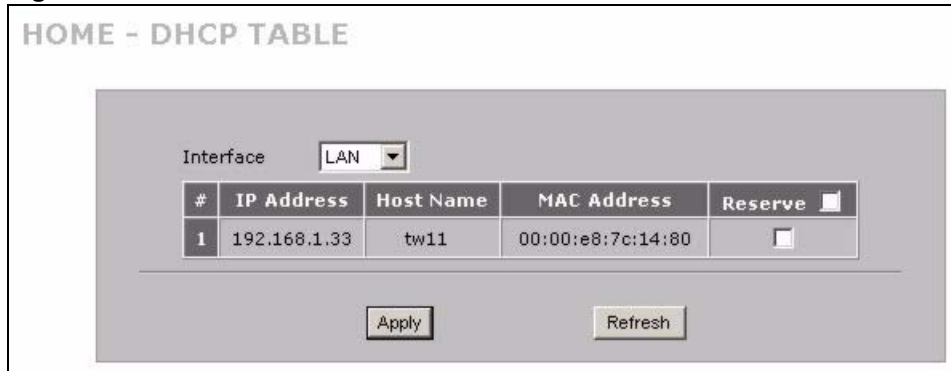
LABEL	DESCRIPTION
	Click the icon to go back to the <b>Show Statistics</b> screen.
Port	Select the check box(es) to display the throughput statistics of the corresponding port(s).
B/s	Specify the direction of the traffic for which you want to show throughput statistics in this table. Select <b>Tx</b>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

### 2.4.6 DHCP Table Screen

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the ZyWALL as a DHCP server or disable it. When configured as a server, the ZyWALL provides the TCP/IP configuration for the clients. If DHCP service is disabled, you must have another DHCP server on your LAN, or else the computer must be manually configured.

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

**Figure 13** Home : DHCP Table



The following table describes the labels in this screen.

**Table 9** Home: DHCP Table

LABEL	DESCRIPTION
Interface	Select <b>LAN</b> , <b>DMZ</b> or <b>WLAN</b> to show the current DHCP client information for the specified interface.
#	This is the index number of the host computer.
IP Address	This field displays the IP address relative to the # field listed above.
Host Name	This field displays the computer host name.
MAC Address	The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal notation). A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address.
Reserve	Select the check box in the heading row to automatically select all check boxes or select the check box(es) in each entry to have the ZyWALL always assign the selected entry(ies)'s IP address(es) to the corresponding MAC address(es) (and host name(s)). You can select up to 128 entries in this table. After you click <b>Apply</b> , the MAC address and IP address also display in the <b>LAN Static DHCP</b> screen (where you can edit them).
Refresh	Click <b>Refresh</b> to reload the DHCP table.

## 2.4.7 VPN Status

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

**Figure 14** Home : VPN Status

The following table describes the labels in this screen.

**Table 10** Home : VPN Status

LABEL	DESCRIPTION
#	This is the security association index number.
Name	This field displays the identification name for this VPN policy.
Local Network	This field displays the IP address of the computer using the VPN IPSec feature of your ZyWALL.
Remote Network	This field displays IP address (in a range) of computers on the remote network behind the remote IPSec router.
Encapsulation	This field displays <b>Tunnel</b> or <b>Transport</b> mode.
IPSec Algorithm	This field displays the security protocols used for an SA. Both AH and ESP increase ZyWALL processing requirements and communications latency (delay).
Poll Interval(s)	Enter the time interval for refreshing statistics in this field.
Set Interval	Click this button to apply the new poll interval you entered in the <b>Poll Interval(s)</b> field.
Stop	Click <b>Stop</b> to stop refreshing statistics.

# CHAPTER 3

## Wizard Setup

This chapter provides information on the **Wizard Setup** screens in the web configurator. The Internet access wizard is only applicable when the ZyWALL is in router mode.

### 3.1 Wizard Setup Overview

The web configurator's setup wizards help you configure **WAN1** on a ZyWALL with multiple WAN ports or the WAN port on a ZyWALL with a single WAN port to access the Internet and edit VPN policies and configure IKE settings to establish a VPN tunnel.

### 3.2 Internet Access

The Internet access wizard screen has three variations depending on what encapsulation type you use. Refer to information provided by your ISP to know what to enter in each field. Leave a field blank if you don't have that information.

#### 3.2.1 ISP Parameters

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

The wizard screen varies according to the type of encapsulation that you select in the **Encapsulation** field.

##### 3.2.1.1 Ethernet

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

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



**Figure 15** ISP Parameters : Ethernet Encapsulation

The following table describes the labels in this screen.

**Table 11** ISP Parameters : Ethernet Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	You must choose the <b>Ethernet</b> option when the WAN port is used as a regular Ethernet. Otherwise, choose <b>PPPoE</b> or <b>PPTP</b> for a dial-up connection.
WAN IP Address Assignment	
IP Address Assignment	Select <b>Dynamic</b> if your ISP did not assign you a fixed IP address. This is the default selection. Select <b>Static</b> if the ISP assigned a fixed IP address. The fields below are available only when you select <b>Static</b> .
My WAN IP Address	Enter your WAN IP address in this field.
My WAN IP Subnet Mask	Enter the IP subnet mask in this field.
Gateway IP Address	Enter the gateway IP address in this field.
First DNS Server Second DNS Server	Enter the DNS server's IP address(es) in the field(s) to the right. Leave the field as <b>0.0.0.0</b> if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it.
Apply	Click <b>Apply</b> to save your changes and go to the next screen.

### 3.2.1.2 PPPoE Encapsulation

Point-to-Point Protocol over Ethernet (PPPoE) functions as a dial-up connection. PPPoE is an IETF (Internet Engineering Task Force) standard specifying how a host personal computer interacts with a broadband modem (for example xDSL, cable, wireless, etc.) to achieve access to high-speed data networks.

**Figure 16** ISP Parameters : PPPoE Encapsulation

The following table describes the labels in this screen.

**Table 12** ISP Parameters: PPPoE Encapsulation

LABEL	DESCRIPTION
ISP Parameter for Internet Access	
Encapsulation	Choose an encapsulation method from the pull-down list box. <b>PPP over Ethernet</b> forms a dial-up connection.
Service Name	Type the name of your service provider.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Retype to Confirm	Type your password again for confirmation.
Nailed-Up	Select <b>Nailed-Up</b> if you do not want the connection to time out.
Idle Timeout	Type the time in seconds that elapses before the router automatically disconnects from the PPPoE server. The default time is <b>100</b> seconds.
WAN IP Address Assignment	

**Table 12** ISP Parameters: PPPoE Encapsulation (continued)

LABEL	DESCRIPTION
IP Address Assignment	Select <b>Dynamic</b> If your ISP did not assign you a fixed IP address. This is the default selection. Select <b>Static</b> If the ISP assigned a fixed IP address. The fields below are available only when you select <b>Static</b> .
My WAN IP Address	Enter your WAN IP address in this field.
First DNS Server Second DNS Server	Enter the DNS server's IP address(es) in the field(s) to the right. Leave the field as <b>0.0.0.0</b> if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it.
Apply	Click <b>Apply</b> to save your changes and go to the next screen.

### 3.2.1.3 PPTP Encapsulation

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

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

Refer to [Appendix G on page 704](#) for more information on PPTP.

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

**Figure 17** ISP Parameters: PPTP Encapsulation

**WIZARD - Internet Access**

**ISP Parameters for Internet Access**

You can select ethernet, PPPoE or PPTP according to in which the network you are. If you don't know, please ask your network administrator. The most popular type of network is ethernet.

Encapsulation:

User Name:

Password:

Retype to Confirm:

Nailed-Up

Idle Timeout:  (Seconds)

**PPTP Configuration**

My IP Address:

My IP Subnet Mask:

Server IP Address:

Connection ID/Name:

**WAN IP Address Assignment**

IP Address Assignment:

The following table describes the labels in this screen.

**Table 13** ISP Parameters : PPTP Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	Select <b>PPTP</b> from the drop-down list box. To configure a PPTP client, you must configure the <b>User Name</b> and <b>Password</b> fields for a PPP connection and the PPTP parameters for a PPTP connection.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the User Name above.
Retype to Confirm	Type your password again for confirmation.
Nailed-Up	Select <b>Nailed-Up</b> if you do not want the connection to time out.
Idle Timeout	Type the time in seconds that elapses before the router automatically disconnects from the PPTP server.
PPTP Configuration	
My IP Address	Type the (static) IP address assigned to you by your ISP.
My IP Subnet Mask	Type the subnet mask assigned to you by your ISP (if given).
Server IP Address	Type the IP address of the PPTP server.

**Table 13** ISP Parameters : PPTP Encapsulation

LABEL	DESCRIPTION
Connection ID/ Name	Enter the connection ID or connection name in this field. It must follow the "c:id" and "n:name" format. For example, C:12 or N:My ISP. This field is optional and depends on the requirements of your xDSL modem.
WAN IP Address Assignment	
IP Address Assignment	Select <b>Dynamic</b> if your ISP did not assign you a fixed IP address. This is the default selection. Select <b>Static</b> if the ISP assigned a fixed IP address. The fields below are available only when you select <b>Static</b> .
My WAN IP Address	Enter your WAN IP address in this field.
First DNS Server Second DNS Server	Enter the DNS server's IP address(es) in the field(s) to the right. Leave the field as <b>0.0.0.0</b> if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it.
Apply	Click <b>Apply</b> to save your changes and go to the next screen.

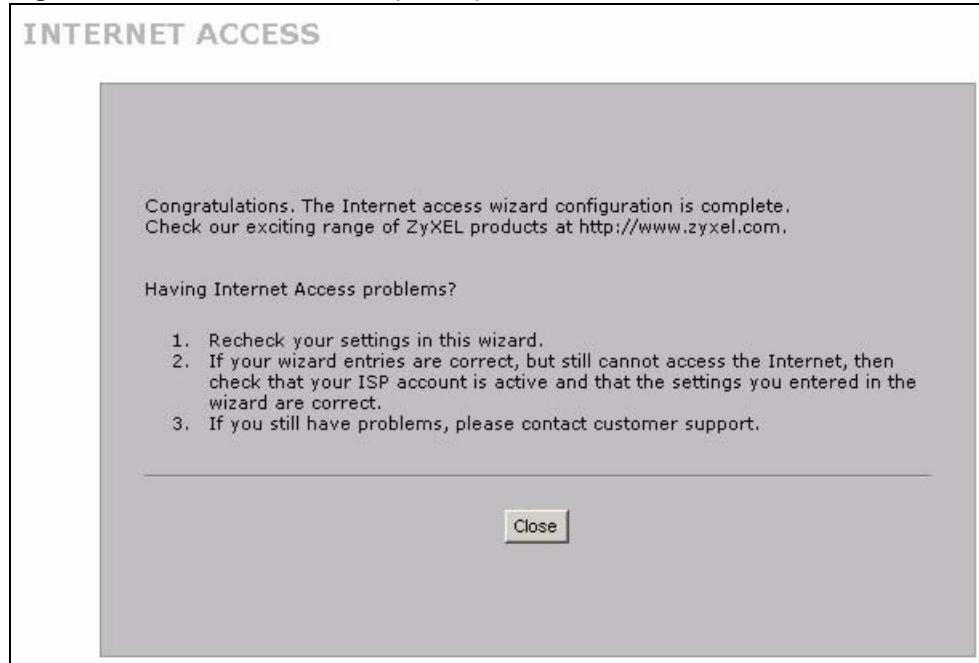
### 3.2.2 Internet Access Wizard: Second Screen

Click **Next** to go to the screen where you can register your ZyWALL and activate the free content filtering, anti-spam, anti-virus and IDP trial applications. Otherwise, click **Skip** to display the congratulations screen and click **Close** to complete the Internet access setup.

**Note:** Make sure you have installed the ZyWALL Turbo Card before you activate the IDP and anti-virus subscription services.

Turn the ZyWALL off before you install or remove the ZyWALL Turbo Card.

**Figure 18** Internet Access Wizard: Second Screen

**Figure 19** Internet Access Setup Complete

### 3.2.3 Internet Access Wizard: Registration

If you clicked **Next** in the previous screen (see [Figure 18 on page 89](#)), the following screen displays.

**Note:** If you want to activate a standard service with your iCard's PIN number (license key), use the **REGISTRATION Service** screen.

**Figure 20** Internet Access Wizard: Registration

**INTERNET ACCESS**

**Device Registration**

New myZyXEL.com account   
  Existing myZyXEL.com account

User Name:    

Password:    
 (Type username and password from 6 to 20 characters.)

Confirm Password:

E-Mail Address:

Country:

Back    Next

The following table describes the labels in this screen.

**Table 14** Internet Access Wizard: Registration

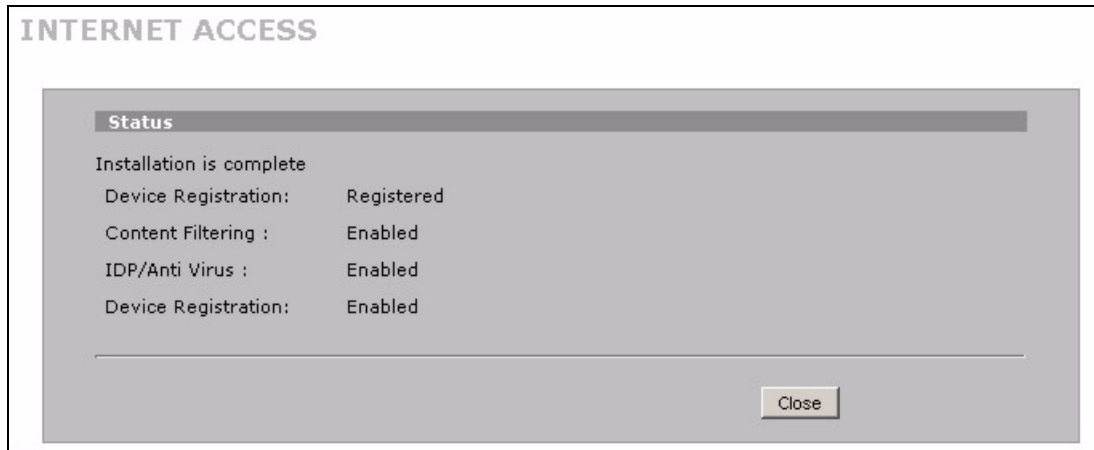
LABEL	DESCRIPTION
Device Registration	If you select <b>Existing myZyXEL.com account</b> , only the <b>User Name</b> and <b>Password</b> fields are available.
New myZyXEL.com account	If you haven't created an account at myZyXEL.com, select this option and configure the following fields to create an account and register your ZyWALL.
Existing myZyXEL.com account	If you already have an account at myZyXEL.com, select this option and enter your user name and password in the fields below to register your ZyWALL.
User Name	Enter a user name for your myZyXEL.com account. The name should be from six to 20 alphanumeric characters (and the underscore). Spaces are not allowed.
Check	Click this button to check with the myZyXEL.com database to verify the user name you entered has not been used.
Password	Enter a password of between six and 20 alphanumeric characters (and the underscore). Spaces are not allowed.
Confirm Password	Enter the password again for confirmation.
E-Mail Address	Enter your e-mail address. You can use up to 80 alphanumeric characters (periods and the underscore are also allowed) without spaces.
Country	Select your country from the drop-down box list.
Back	Click <b>Back</b> to return to the previous screen.
Next	Click <b>Next</b> to continue.

After you fill in the fields and click **Next**, the following screen shows indicating the registration is in progress. Wait for the registration progress to finish.

**Figure 21** Internet Access Wizard: Registration in Progress



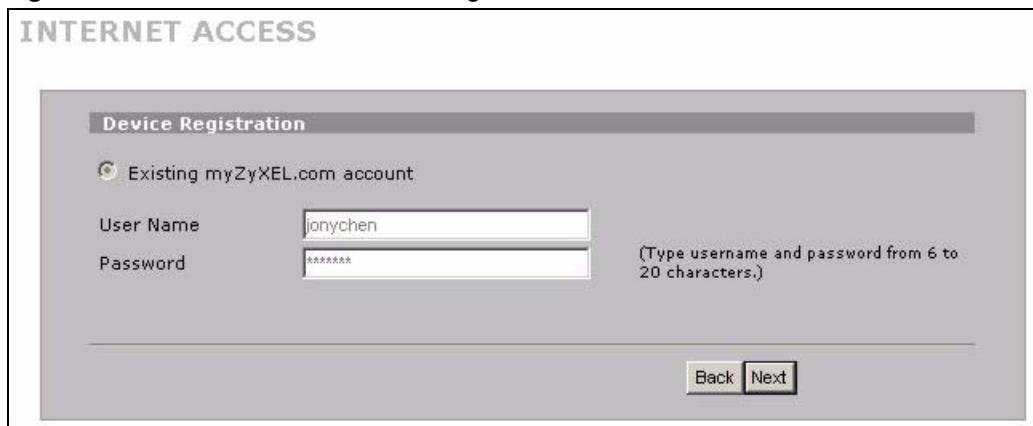
Click **Close** to leave the wizard screen when the registration and activation are done.

**Figure 22** Internet Access Wizard: Status

The following screen appears if the registration was not successful. Click **Return** to go back to the **Device Registration** screen and check your settings.

**Figure 23** Internet Access Wizard: Registration Failed

If the ZyWALL has been registered, the **Device Registration** screen is read-only and the **Service Activation** screen appears indicating what trial applications are activated after you click **Next**.

**Figure 24** Internet Access Wizard: Registered Device



**Figure 25** Internet Access Wizard: Activated Services

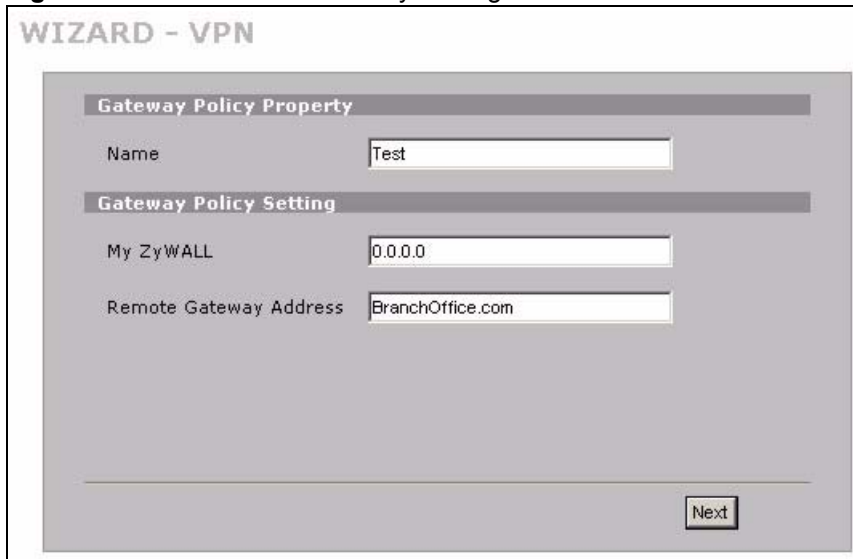


### 3.3 VPN Wizard Gateway Setting

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

Click **VPN Wizard** in the **HOME** screen to open the VPN configuration wizard. The first screen displays as shown next.

**Figure 26** VPN Wizard: Gateway Setting



The following table describes the labels in this screen.

**Table 15** VPN Wizard: Gateway Setting

LABEL	DESCRIPTION
Gateway Policy Property	
Name	Type up to 32 characters to identify this VPN gateway policy. You may use any character, including spaces, but the ZyWALL drops trailing spaces.
My ZyWALL	<p>When the ZyWALL is in router mode, enter the WAN IP address or the domain name of your ZyWALL or leave the field set to <b>0.0.0.0</b>.</p> <p>For a ZyWALL with multiple WAN ports, the following applies if the <b>My ZyWALL</b> field is configured as <b>0.0.0.0</b>:</p> <ul style="list-style-type: none"> <li>• When the WAN port operation mode is set to <b>Active/Passive</b>, the ZyWALL uses the IP address (static or dynamic) of the WAN port that is in use.</li> <li>• When the WAN port operation mode is set to <b>Active/Active</b>, the ZyWALL uses the IP address (static or dynamic) of the primary (highest priority) WAN port to set up the VPN tunnel as long as the corresponding WAN1 or WAN2 connection is up. If the corresponding WAN1 or WAN2 connection goes down, the ZyWALL uses the IP address of the other WAN port.</li> <li>• If both WAN connections go down, the ZyWALL uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect. See the chapter on WAN for details on dial backup and traffic redirect.</li> </ul> <p>A ZyWALL with a single WAN port uses its current WAN IP address (static or dynamic) in setting up the VPN tunnel if you leave this field as <b>0.0.0.0</b>. If the WAN connection goes down, the ZyWALL uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect.</p> <p>The VPN tunnel has to be rebuilt if this IP address changes.</p> <p>When the ZyWALL is in bridge mode, this field is read-only and displays the ZyWALL's IP address.</p>
Remote Gateway Address	Enter the WAN IP address or domain name of the remote IPsec router (secure gateway) in the field below to identify the remote IPsec router by its IP address or a domain name. Set this field to <b>0.0.0.0</b> if the remote IPsec router has a dynamic WAN IP address.
Next	Click <b>Next</b> to continue.

### 3.4 VPN Wizard Network Setting

Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.

**Figure 27** VPN Wizard: Network Setting

The following table describes the labels in this screen.

**Table 16** VPN Wizard : Network Setting

LABEL	DESCRIPTION
Network Policy Property	
Active	If the <b>Active</b> check box is selected, packets for the tunnel trigger the ZyWALL to build the tunnel. Clear the <b>Active</b> check box to turn the network policy off. The ZyWALL does not apply the policy. Packets for the tunnel do not trigger the tunnel.
Name	Type up to 32 characters to identify this VPN network policy. You may use any character, including spaces, but the ZyWALL drops trailing spaces.
Network Policy Setting	
Local Network	Local IP addresses must be static and correspond to the remote IPSec router's configured remote IP addresses. Select <b>Single</b> for a single IP address. Select <b>Range IP</b> for a specific range of IP addresses. Select <b>Subnet</b> to specify IP addresses on a network by their subnet mask.
Starting IP Address	When the <b>Local Network</b> field is configured to <b>Single</b> , enter a (static) IP address on the LAN behind your ZyWALL. When the <b>Local Network</b> field is configured to <b>Range IP</b> , enter the beginning (static) IP address, in a range of computers on the LAN behind your ZyWALL. When the <b>Local Network</b> field is configured to <b>Subnet</b> , this is a (static) IP address on the LAN behind your ZyWALL.
Ending IP Address/ Subnet Mask	When the <b>Local Network</b> field is configured to <b>Single</b> , this field is N/A. When the <b>Local Network</b> field is configured to <b>Range IP</b> , enter the end (static) IP address, in a range of computers on the LAN behind your ZyWALL. When the <b>Local Network</b> field is configured to <b>Subnet</b> , this is a subnet mask on the LAN behind your ZyWALL.

**Table 16** VPN Wizard : Network Setting

LABEL	DESCRIPTION
Remote Network	Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses. Select <b>Single</b> for a single IP address. Select <b>Range IP</b> for a specific range of IP addresses. Select <b>Subnet</b> to specify IP addresses on a network by their subnet mask.
Starting IP Address	When the <b>Remote Network</b> field is configured to <b>Single</b> , enter a (static) IP address on the network behind the remote IPSec router. When the <b>Remote Network</b> field is configured to <b>Range IP</b> , enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. When the <b>Remote Network</b> field is configured to <b>Subnet</b> , enter a (static) IP address on the network behind the remote IPSec router
Ending IP Address/ Subnet Mask	When the <b>Remote Network</b> field is configured to <b>Single</b> , this field is N/A. When the <b>Remote Network</b> field is configured to <b>Range IP</b> , enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the <b>Remote Network</b> field is configured to <b>Subnet</b> , enter a subnet mask on the network behind the remote IPSec router.
Back	Click <b>Back</b> to return to the previous screen.
Next	Click <b>Next</b> to continue.

### 3.5 VPN Wizard IKE Tunnel Setting (IKE Phase 1)

**Figure 28** VPN Wizard: IKE Tunnel Setting

**WIZARD - VPN**

**IKE Tunnel Setting (IKE Phase 1)**

Negotiation Mode  Main Mode  Aggressive Mode

Encryption Algorithm  DES  AES  3DES

Authentication Algorithm  SHA1  MD5

Key Group  DH1  DH2

SA Life Time  (Seconds)

Pre-Shared Key

The following table describes the labels in this screen.

**Table 17** VPN Wizard: IKE Tunnel Setting

LABEL	DESCRIPTION
Negotiation Mode	<p>Select <b>Main Mode</b> for identity protection. Select <b>Aggressive Mode</b> to allow more incoming connections from dynamic IP addresses to use separate passwords.</p> <p><b>Note:</b> Multiple SAs (security associations) connecting through a secure gateway must have the same negotiation mode.</p>
Encryption Algorithm	<p>When <b>DES</b> is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The <b>DES</b> encryption algorithm uses a 56-bit key. Triple DES (<b>3DES</b>) is a variation on <b>DES</b> that uses a 168-bit key. As a result, <b>3DES</b> is more secure than <b>DES</b>. It also requires more processing power, resulting in increased latency and decreased throughput. This implementation of <b>AES</b> uses a 128-bit key. <b>AES</b> is faster than <b>3DES</b>.</p>
Authentication Algorithm	<p><b>MD5</b> (Message Digest 5) and <b>SHA1</b> (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The <b>SHA1</b> algorithm is generally considered stronger than <b>MD5</b>, but is slower. Select <b>MD5</b> for minimal security and <b>SHA-1</b> for maximum security.</p>
Key Group	<p>You must choose a key group for phase 1 IKE setup. <b>DH1</b> (default) refers to Diffie-Hellman Group 1 a 768 bit random number. <b>DH2</b> refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number.</p>
SA Life Time (Seconds)	<p>Define the length of time before an IKE SA automatically renegotiates in this field. The minimum value is 180 seconds.</p> <p>A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.</p>
Pre-Shared Key	<p>Type your pre-shared key in this field. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection.</p> <p>Type from 8 to 31 case-sensitive ASCII characters or from 16 to 62 hexadecimal ("0-9", "A-F") characters. You must precede a hexadecimal key with a "0x (zero x)", which is not counted as part of the 16 to 62 character range for the key. For example, in "0x0123456789ABCDEF", 0x denotes that the key is hexadecimal and 0123456789ABCDEF is the key itself.</p> <p>Both ends of the VPN tunnel must use the same pre-shared key. You will receive a PYLD_MALFORMED (payload malformed) packet if the same pre-shared key is not used on both ends.</p>
Back	<p>Click <b>Back</b> to return to the previous screen.</p>
Next	<p>Click <b>Next</b> to continue.</p>

## 3.6 VPN Wizard IPsec Setting (IKE Phase 2)

**Figure 29** VPN Wizard: IPsec Setting

**WIZARD - VPN**

**IPsec Setting (IKE Phase 2)**

Encapsulation Mode  Tunnel  Transport

IPsec Protocol  ESP  AH

Encryption Algorithm  DES  AES  3DES  NULL

Authentication Algorithm  SHA1  MD5

SA Life Time  (Seconds)

Perfect Forward Secrecy (PFS)  None  DH1  DH2

The following table describes the labels in this screen.

**Table 18** VPN Wizard: IPsec Setting

LABEL	DESCRIPTION
Encapsulation Mode	<b>Tunnel</b> is compatible with NAT, <b>Transport</b> is not. Tunnel mode encapsulates the entire IP packet to transmit it securely. A Tunnel mode is required for gateway services to provide access to internal systems. Tunnel mode is fundamentally an IP tunnel with authentication and encryption. Transport mode is used to protect upper layer protocols and only affects the data in the IP packet. In Transport mode, the IP packet contains the security protocol (AH or ESP) located after the original IP header and options, but before any upper layer protocols contained in the packet (such as TCP and UDP).
IPsec Protocol	Select the security protocols used for an SA. Both <b>AH</b> and <b>ESP</b> increase ZyWALL processing requirements and communications latency (delay).
Encryption Algorithm	When <b>DES</b> is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES ( <b>3DES</b> ) is a variation on DES that uses a 168-bit key. As a result, <b>3DES</b> is more secure than <b>DES</b> . It also requires more processing power, resulting in increased latency and decreased throughput. This implementation of <b>AES</b> uses a 128-bit key. <b>AES</b> is faster than <b>3DES</b> . Select <b>NULL</b> to set up a tunnel without encryption. When you select <b>NULL</b> , you do not enter an encryption key.
Authentication Algorithm	<b>MD5</b> (Message Digest 5) and <b>SHA1</b> (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The <b>SHA1</b> algorithm is generally considered stronger than <b>MD5</b> , but is slower. Select <b>MD5</b> for minimal security and <b>SHA-1</b> for maximum security.

**Table 18** VPN Wizard: IPSec Setting (continued)

LABEL	DESCRIPTION
SA Life Time (Seconds)	Define the length of time before an IKE SA automatically renegotiates in this field. The minimum value is 180 seconds. A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Perfect Forward Secret (PFS)	Perfect Forward Secret (PFS) is disabled ( <b>None</b> ) by default in phase 2 IPSec SA setup. This allows faster IPSec setup, but is not so secure. Select <b>DH1</b> or <b>DH2</b> to enable PFS. <b>DH1</b> refers to Diffie-Hellman Group 1 a 768 bit random number. <b>DH2</b> refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number (more secure, yet slower).
Back	Click <b>Back</b> to return to the previous screen.
Next	Click <b>Next</b> to continue.

### 3.7 VPN Wizard Status Summary

This read-only screen shows the status of the current VPN setting. Use the summary table to check whether what you have configured is correct.

**Figure 30** VPN Wizard: VPN Status

**WIZARD - VPN**

**Status**

Gateway Policy Property	
Name	Test
Gateway Policy Setting	
My ZyWALL	0.0.0.0
Remote Gateway Address	BranchOffice.com
Network Policy Property	
Active	Yes
Name	Test
Network Policy Setting	
Local Network	
Starting IP Address	192.168.1.0
Subnet Mask	255.255.255.0
Remote Network	
Starting IP Address	10.0.0.0
Subnet Mask	255.0.0.0
IKE Tunnel Setting (IKE Phase 1)	
Authentication For Activating VPN	
Authenticated By	
User Name	
Password	
Negotiation Mode	Main Mode
Encryption Algorithm	DES
Authentication Algorithm	MD5
Key Group	DH1
SA Life Time	28800 (Seconds)
Pre-Shared Key	12345678
IPsec Setting (IKE Phase 2)	
Encapsulation Mode	Tunnel Mode
IPsec Protocol	ESP
Encryption Algorithm	DES
Authentication Algorithm	SHA1
SA Life Time	28800 (Seconds)
Perfect Forward Secrecy (PFS)	None

Back Finish

The following table describes the labels in this screen.

**Table 19** VPN Wizard: VPN Status

LABEL	DESCRIPTION
Gateway Policy Property	
Name	This is the name of this VPN gateway policy.
Gateway Policy Setting	
My ZyWALL	This is the WAN IP address or the domain name of your ZyWALL in router mode or the ZyWALL's IP address in bridge mode.
Remote Gateway Address	This is the IP address or the domain name used to identify the remote IPsec router.
Network Policy Property	
Active	This displays whether this VPN network policy is enabled or not.



**Table 19** VPN Wizard: VPN Status (continued)

LABEL	DESCRIPTION
Name	This is the name of this VPN network policy.
Network Policy Setting	
Local Network	
Starting IP Address	This is a (static) IP address on the LAN behind your ZyWALL.
Ending IP Address/ Subnet Mask	When the local network is configured for a single IP address, this field is N/A. When the local network is configured for a range IP address, this is the end (static) IP address, in a range of computers on the LAN behind your ZyWALL. When the local network is configured for a subnet, this is a subnet mask on the LAN behind your ZyWALL.
Remote Network	
Starting IP Address	This is a (static) IP address on the network behind the remote IPsec router.
Ending IP Address/ Subnet Mask	When the remote network is configured for a single IP address, this field is N/A. When the remote network is configured for a range IP address, this is the end (static) IP address, in a range of computers on the network behind the remote IPsec router. When the remote network is configured for a subnet, this is a subnet mask on the network behind the remote IPsec router.
IKE Tunnel Setting (IKE Phase 1)	
Negotiation Mode	This shows <b>Main Mode</b> or <b>Aggressive Mode</b> . Multiple SAs connecting through a secure gateway must have the same negotiation mode.
Encryption Algorithm	This is the method of data encryption. Options can be <b>DES</b> , <b>3DES</b> or <b>AES</b> .
Authentication Algorithm	<b>MD5</b> (Message Digest 5) and <b>SHA1</b> (Secure Hash Algorithm) are hash algorithms used to authenticate packet data.
Key Group	This is the key group you chose for phase 1 IKE setup.
SA Life Time (Seconds)	This is the length of time before an IKE SA automatically renegotiates.
Pre-Shared Key	This is a pre-shared key identifying a communicating party during a phase 1 IKE negotiation.
IPsec Setting (IKE Phase 2)	
Encapsulation Mode	This shows <b>Tunnel</b> mode or <b>Transport</b> mode.
IPsec Protocol	<b>ESP</b> or <b>AH</b> are the security protocols used for an SA.
Encryption Algorithm	This is the method of data encryption. Options can be <b>DES</b> , <b>3DES</b> , <b>AES</b> or <b>NULL</b> .
Authentication Algorithm	<b>MD5</b> (Message Digest 5) and <b>SHA1</b> (Secure Hash Algorithm) are hash algorithms used to authenticate packet data.
SA Life Time (Seconds)	This is the length of time before an IKE SA automatically renegotiates.
Perfect Forward Secret (PFS)	Perfect Forward Secret (PFS) is disabled ( <b>None</b> ) by default in phase 2 IPsec SA setup. Otherwise, <b>DH1</b> or <b>DH2</b> are selected to enable PFS.
Back	Click <b>Back</b> to return to the previous screen.
Finish	Click <b>Finish</b> to complete and save the wizard setup.

## 3.8 VPN Wizard Setup Complete

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

**Figure 31** VPN Wizard Setup Complete





# CHAPTER 4

## Registration

### 4.1 myZyXEL.com overview

myZyXEL.com is ZyXEL's online services center where you can register your ZyWALL and manage subscription services available for the ZyWALL.

**Note:** You need to create an account before you can register your device and activate the services at myZyXEL.com.

You can directly create a myZyXEL.com account, register your ZyWALL and activate a service using the **REGISTRATION** screen. Alternatively, go to <http://www.myZyXEL.com> with the ZyWALL's serial number and LAN MAC address to register it. Refer to the web site's on-line help for details.

**Note:** To activate a service on a ZyWALL, you need to access myZyXEL.com via that ZyWALL.

#### 4.1.1 Subscription Services Available on the ZyWALL

At the time of writing, the ZyWALL can use content filtering, anti-spam, anti-virus and IDP (Intrusion Detection and Prevention) subscription services.

Content filtering allows or blocks access to web sites. Subscribe to category-based content filtering to block access to categories of web sites based on content. Your ZyWALL accesses an external database that has millions of web sites categorized based on content. You can have the ZyWALL block, block and/or log access to web sites based on these categories.

Anti-spam identifies and marks or discards spam e-mail. An anti-spam subscription lets the ZyWALL check e-mail with an external anti-spam server.

Anti-virus allows the ZyWALL to scan packets for computer viruses and deletes the infected packets.

IDP allows the ZyWALL to detect malicious or suspicious packets and respond immediately.

The ID&P and anti-virus features use the same signature files on the ZyWALL to detect and scan for viruses. After the service is activated, the ZyWALL downloads the up-to-date signature files from the update server (<http://myupdate.zywall.zyxel.com>).

You will get automatic e-mail notification of new signature releases from mySecurityZone after you activate the IDP/Anti-virus service. You can also check for new signature or virus updates at <http://mysecurity.zyxel.com>.

See the chapters about content filtering, anti-virus, anti-spam and IDP for more information.

**Note:** To update the signature file or use a subscription service, you have to register and activate the corresponding service at myZyXEL.com (through the ZyWALL).

## 4.2 Registration

To register your ZyWALL with myXEL.com and activate a service, such as content filtering, anti-spam or anti-virus, click **REGISTRATION** in the navigation panel to open the screen as shown next.

**Note:** Make sure you have installed the ZyWALL Turbo extension card before you activate the IDP and anti-virus subscription services.

Turn the ZyWALL off before you install or remove the ZyWALL Turbo Card. See the ZyWALL Turbo Card guide for more information.

**Figure 32** Registration

The screenshot shows the 'REGISTRATION' screen with two tabs: 'Registration' and 'Service'. The 'Registration' tab is active, displaying the 'Device Registration' section. It has two radio buttons: 'New myZyXEL.com account' (selected) and 'Existing myZyXEL.com account'. Below are input fields for 'User Name' (containing 'ZyWALL'), 'Password' (masked with asterisks), 'Confirm Password' (masked with asterisks), 'E-Mail Address' (containing 'test@zyxel.com'), and 'Country' (a dropdown menu showing 'Taiwan'). A 'Check' button is next to the User Name field, with a note: '(Type username and password from 6 to 20 characters.)'. The 'Service Activation' section below has three checked checkboxes: 'Content Filtering 1-month Trial', 'Anti Spam 3-month Trial', and 'IDP/AV 3-month Trial'. A note at the bottom says: 'Note: For more device services management, please go to [myZyXEL.com](http://myZyXEL.com)'. At the very bottom are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

**Table 20** Registration

LABEL	DESCRIPTION
Device Registration	If you select <b>Existing myZyXEL.com account</b> , only the <b>User Name</b> and <b>Password</b> fields are available.
New myZyXEL.com account	If you haven't created an account at myZyXEL.com, select this option and configure the following fields to create an account and register your ZyWALL.
Existing myZyXEL.com account	If you already have an account at myZyXEL.com, select this option and enter your user name and password in the fields below to register your ZyWALL.
User Name	Enter a user name for your myZyXEL.com account. The name should be from six to 20 alphanumeric characters (and the underscore). Spaces are not allowed.
Check	Click this button to check with the myZyXEL.com database to verify the user name you entered has not been used.
Password	Enter a password of between six and 20 alphanumeric characters (and the underscore). Spaces are not allowed.
Confirm Password	Enter the password again for confirmation.
E-Mail Address	Enter your e-mail address. You can use up to 80 alphanumeric characters (periods and the underscore are also allowed) without spaces.
Country	Select your country from the drop-down box list.
Service Activation	You can try trial service subscription. After the trial expires, you can buy an iCard and enter the license key in the <b>REGISTRATION Service</b> screen to extend the service.
Content Filtering 1-month Trial	Select the check box to activate a trial. The trial period starts the day you activate the trial.
Anti Spam 3-month Trial	Select the check box to activate a trial. The trial period starts the day you activate the trial.
IDP/AV 3-month Trial	Select the check box to activate a trial. The trial period starts the day you activate the trial.
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

**Note:** If the ZyWALL is registered already, this screen is read-only and indicates whether trial services are activated. Use the **Service** screen to update your service subscription status.

**Figure 33** Registration: Registered Device

**REGISTRATION**

Registration Service

**Device Registration**

Existing myZyXEL.com account

User Name: jorynchen

Password: [REDACTED] (Type username and password from 6 to 20 characters.)

**Service Activation**

- Content Filtering 1-month Trial (Service has been activated.)
- Anti Spam 3-month Trial (Service has been activated.)
- IDP/AV 3-month Trial (Service has been activated.)

Note: For more device services management, please go to [myZyXEL.com](http://myZyXEL.com)

### 4.3 Service

After you activate a trial, you can also use the **Service** screen to register and enter your iCard's PIN number (license key). Click **REGISTRATION**, **Service** to open the screen as shown next.

**Note:** If you restore the ZyWALL to the default configuration file or upload a different configuration file after you register, click the **Service License Refresh** button to update license information.

**Figure 34** Registration: Service

**REGISTRATION**

Registration Service

**Service Management**

Service	Status	Registration Type	Expiration Day
Content Filter Service	Active	Trial	2005-08-24
Anti-Spam Service	Active	Trial	2005-10-23
IDP/Anti-Virus Service	Active	Standard	2007-01-22

**License Upgrade**

License Key: S-ZAS001-CE45BD86EA6DD5D [Update]

[Service License Refresh] (Sync with myZyXEL.com to download license Info.)

The following table describes the labels in this screen.

**Table 21** Service

LABEL	DESCRIPTION
Service Management	
Service	This field displays the service name available on the ZyWALL.
Status	This field displays whether a service is activated ( <b>Active</b> ) or not ( <b>Inactive</b> ).
Registration Type	This field displays whether you applied for a trial application ( <b>Trial</b> ) or registered a service with your iCard's PIN number ( <b>Standard</b> ).
Expiration Day	This field displays the date your service expires.
License Upgrade	
License Key	Enter your iCard's PIN number and click <b>Update</b> to activate or extend a standard service subscription. If a standard service subscription runs out, you need to buy a new iCard (specific to your ZyWALL) and enter the new PIN number to extend the service.
Service License Refresh	Click this button to renew service license information (such as the license key, registration status and expiration day).





# CHAPTER 5

## LAN Screens

This chapter describes how to configure LAN settings. This chapter is only applicable when the ZyWALL is in router mode. The **LAN Port Roles** screen is available on the ZyWALL 5 and ZyWALL 35.

### 5.1 LAN Overview

Local Area Network (LAN) is a shared communication system to which many computers are attached. The LAN screens can help you configure a LAN DHCP server, manage IP addresses, and partition your physical network into logical networks.

### 5.2 DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the ZyWALL as a DHCP server or disable it. When configured as a server, the ZyWALL provides the TCP/IP configuration for the clients. If DHCP service is disabled, you must have another DHCP server on your LAN, or else the computer must be manually configured.

#### 5.2.1 IP Pool Setup

The ZyWALL is pre-configured with a pool of IP addresses for the DHCP clients (DHCP Pool). See the product specifications in the appendices. Do not assign static IP addresses from the DHCP pool to your LAN computers.

### 5.3 LAN TCP/IP

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

#### 5.3.1 Factory LAN Defaults

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

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

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

### 5.3.2 IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number.

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the Network Address Translation (NAT) feature of the ZyWALL. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your ZyWALL, but make sure that no other device on your network is using that IP address.

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

### 5.3.3 RIP Setup

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

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

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

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

### 5.3.4 Multicast

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

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

The ZyWALL supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**). At start up, the ZyWALL queries all directly connected networks to gather group membership. After that, the ZyWALL periodically updates this information. IP multicasting can be enabled/disabled on the ZyWALL LAN and/or WAN interfaces in the web configurator (**LAN**; **WAN**). Select **None** to disable IP multicasting on these interfaces.

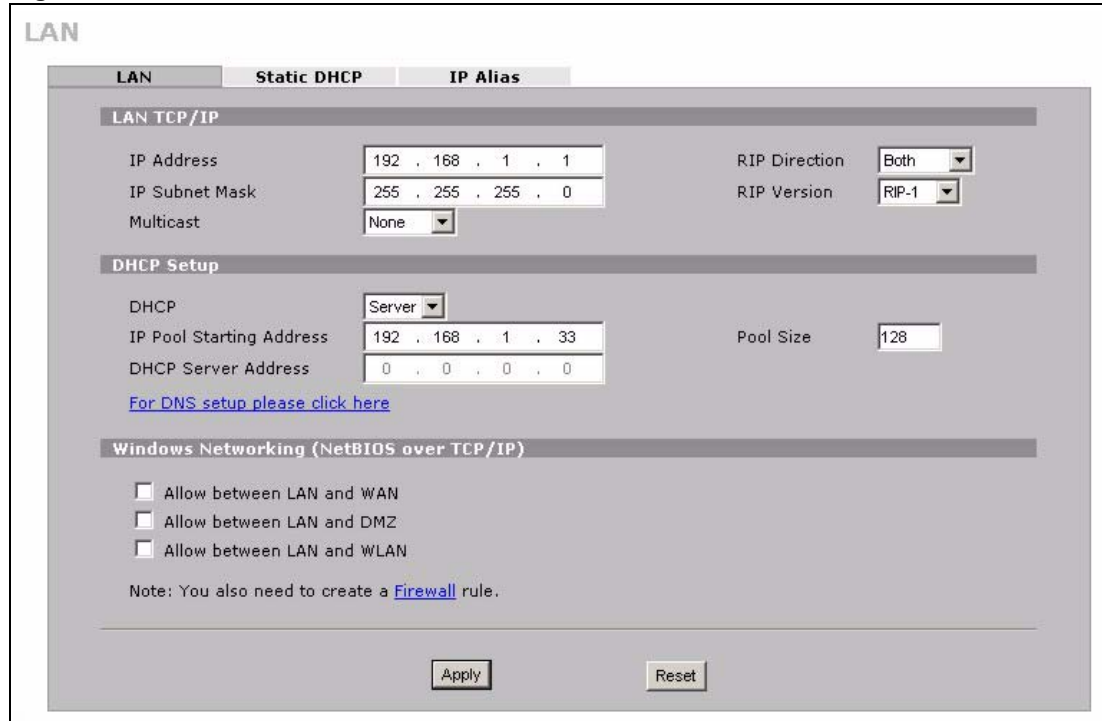
## 5.4 DNS Servers

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

## 5.5 LAN

Click **NETWORK**, **LAN** to open the **LAN** screen. Use this screen to configure the ZyWALL's IP address and other LAN TCP/IP settings as well as the built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

**Figure 35 LAN**



The following table describes the labels in this screen.

**Table 22 LAN**

LABEL	DESCRIPTION
LAN TCP/IP	
IP Address	Type the IP address of your ZyWALL in dotted decimal notation. 192.168.1.1 is the factory default. Alternatively, click the right mouse button to copy and/or paste the IP address.
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your ZyWALL automatically calculates the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyWALL.
RIP Direction	RIP (Routing Information Protocol, RFC1058 and RFC 1389) allows a router to exchange routing information with other routers. The <b>RIP Direction</b> field controls the sending and receiving of RIP packets. Select the RIP direction from <b>Both/In Only/Out Only/None</b> . When set to <b>Both</b> or <b>Out Only</b> , the ZyWALL will broadcast its routing table periodically. When set to <b>Both</b> or <b>In Only</b> , it will incorporate the RIP information that it receives; when set to <b>None</b> , it will not send any RIP packets and will ignore any RIP packets received. <b>Both</b> is the default.
RIP Version	The <b>RIP Version</b> field controls the format and the broadcasting method of the RIP packets that the ZyWALL sends (it recognizes both formats when receiving). <b>RIP-1</b> is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both <b>RIP-2B</b> and <b>RIP-2M</b> sends the routing data in RIP-2 format; the difference being that <b>RIP-2B</b> uses subnet broadcasting while <b>RIP-2M</b> uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to <b>Both</b> and the Version set to <b>RIP-1</b> .

**Table 22** LAN (continued)

LABEL	DESCRIPTION
Multicast	Select <b>IGMP V-1</b> or <b>IGMP V-2</b> or <b>None</b> . IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see <i>sections 4 and 5 of RFC 2236</i> .
DHCP Setup	
DHCP	DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (workstations) to obtain TCP/IP configuration at startup from a server. Unless you are instructed by your ISP, leave this field set to <b>Server</b> . When configured as a server, the ZyWALL provides TCP/IP configuration for the clients. When set as a server, fill in the <b>IP Pool Starting Address</b> and <b>Pool Size</b> fields. Select <b>Relay</b> to have the ZyWALL forward DHCP requests to another DHCP server. When set to <b>Relay</b> , fill in the <b>DHCP Server Address</b> field. Select <b>None</b> to stop the ZyWALL from acting as a DHCP server. When you select <b>None</b> , you must have another DHCP server on your LAN, or else the computers must be manually configured.
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Pool Size	This field specifies the size, or count of the IP address pool.
DHCP Server Address	Type the IP address of the DHCP server to which you want the ZyWALL to relay DHCP requests. Use dotted decimal notation. Alternatively, click the right mouse button to copy and/or paste the IP address.
Windows Networking (NetBIOS over TCP/IP)	NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls. However it may sometimes be necessary to allow NetBIOS packets to pass through to the WAN in order to find a computer on the WAN.
Allow between LAN and WAN	Select this check box to forward NetBIOS packets from the LAN to the WAN and from the WAN to the LAN. If your firewall is enabled with the default policy set to block WAN to LAN traffic, you also need to enable the default WAN to LAN firewall rule that forwards NetBIOS traffic. Clear this check box to block all NetBIOS packets going from the LAN to the WAN and from the WAN to the LAN.
Allow between LAN and DMZ	Select this check box to forward NetBIOS packets from the LAN to the DMZ and from the DMZ to the LAN. If your firewall is enabled with the default policy set to block DMZ to LAN traffic, you also need to enable the default DMZ to LAN firewall rule that forwards NetBIOS traffic. Clear this check box to block all NetBIOS packets going from the LAN to the DMZ and from the DMZ to the LAN.
Allow between LAN and WLAN	Select this check box to forward NetBIOS packets from the LAN to the WLAN and from the WLAN to the LAN. Clear this check box to block all NetBIOS packets going from the LAN to the WLAN and from the WLAN to the LAN.
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 5.6 LAN Static DHCP

This table allows you to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses.

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

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

**Figure 36** LAN Static DHCP

The screenshot shows the 'LAN Static DHCP' configuration interface. At the top, there are tabs for 'LAN', 'Static DHCP', and 'IP Alias'. Below the tabs is the 'Static DHCP Table' which is a table with three main columns: '#', 'MAC Address', and 'IP Address'. The 'MAC Address' column is further divided into six sub-columns for each hexadecimal pair. The 'IP Address' column is divided into four sub-columns for each octet. The first row (index 1) contains the MAC address 00:00:E8:7C:14:80 and the IP address 192.168.1.33. Rows 2 through 9 and 120 through 128 are empty. At the bottom of the table, there are 'Apply' and 'Reset' buttons.

#	MAC Address						IP Address			
1	00	00	E8	7C	14	80	192	168	1	33
2							0	0	0	0
3							0	0	0	0
4							0	0	0	0
5							0	0	0	0
6							0	0	0	0
7							0	0	0	0
8							0	0	0	0
9							0	0	0	0
120							0	0	0	0
121							0	0	0	0
122							0	0	0	0
123							0	0	0	0
124							0	0	0	0
125							0	0	0	0
126							0	0	0	0
127							0	0	0	0
128							0	0	0	0

The following table describes the labels in this screen.

**Table 23** LAN Static DHCP

LABEL	DESCRIPTION
#	This is the index number of the Static IP table entry (row).
MAC Address	Type the MAC address of a computer on your LAN.

**Table 23** LAN Static DHCP

LABEL	DESCRIPTION
IP Address	Type the IP address that you want to assign to the computer on your LAN. Alternatively, click the right mouse button to copy and/or paste the IP address.
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

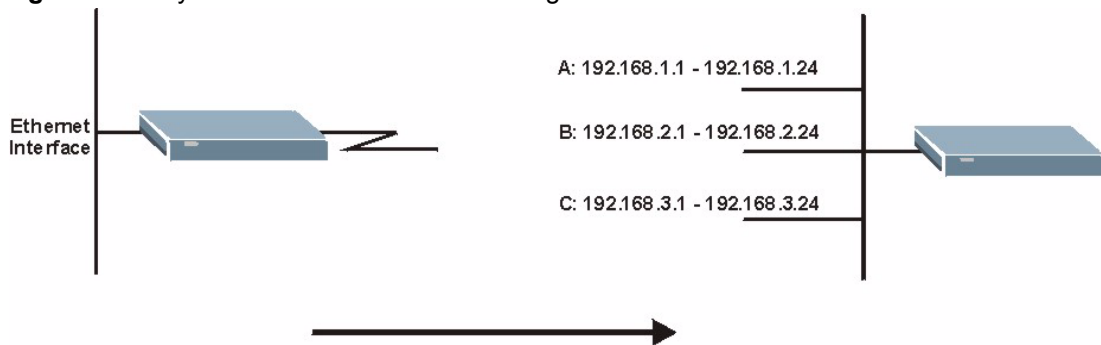
## 5.7 LAN IP Alias

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

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

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

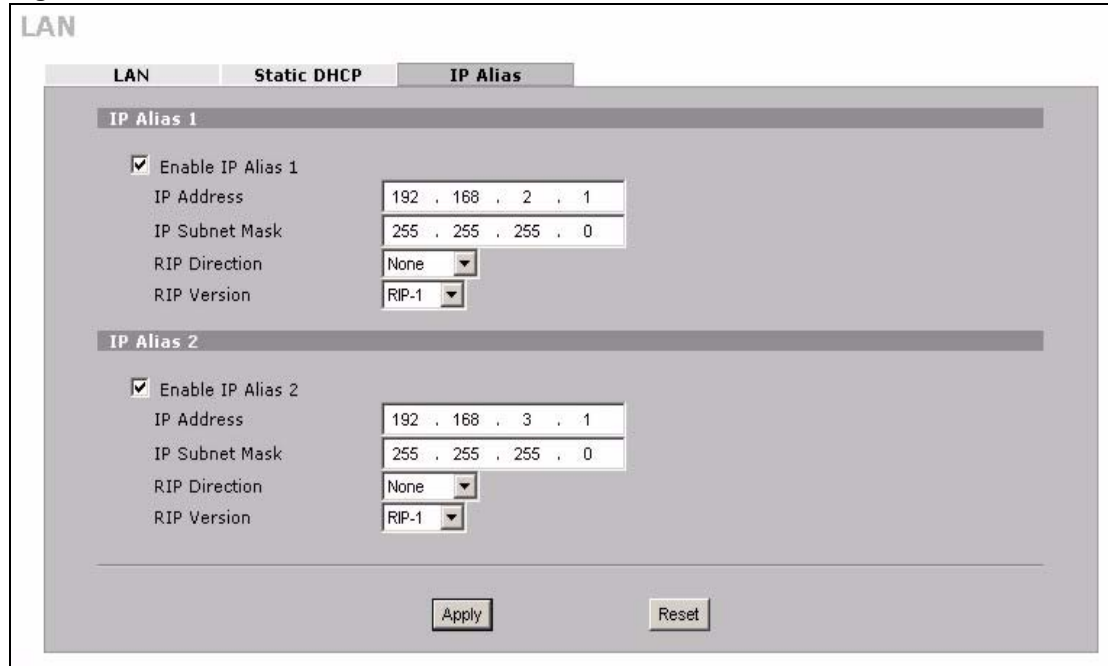
The following figure shows a LAN divided into subnets A, B, and C.

**Figure 37** Physical Network & Partitioned Logical Networks

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



**Figure 38** LAN IP Alias



The following table describes the labels in this screen.

**Table 24** LAN IP Alias

LABEL	DESCRIPTION
Enable IP Alias 1, 2	Select the check box to configure another LAN network for the ZyWALL.
IP Address	Enter the IP address of your ZyWALL in dotted decimal notation. Alternatively, click the right mouse button to copy and/or paste the IP address.
IP Subnet Mask	Your ZyWALL will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyWALL.
RIP Direction	RIP (Routing Information Protocol, RFC 1058 and RFC 1389) allows a router to exchange routing information with other routers. The <b>RIP Direction</b> field controls the sending and receiving of RIP packets. Select the RIP direction from <b>Both/In Only/Out Only/None</b> . When set to <b>Both</b> or <b>Out Only</b> , the ZyWALL will broadcast its routing table periodically. When set to <b>Both</b> or <b>In Only</b> , it will incorporate the RIP information that it receives; when set to <b>None</b> , it will not send any RIP packets and will ignore any RIP packets received.
RIP Version	The <b>RIP Version</b> field controls the format and the broadcasting method of the RIP packets that the ZyWALL sends (it recognizes both formats when receiving). <b>RIP-1</b> is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both <b>RIP-2B</b> and <b>RIP-2M</b> sends the routing data in RIP-2 format; the difference being that <b>RIP-2B</b> uses subnet broadcasting while <b>RIP-2M</b> uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to <b>Both</b> and the Version set to <b>RIP-1</b> .

**Table 24** LAN IP Alias

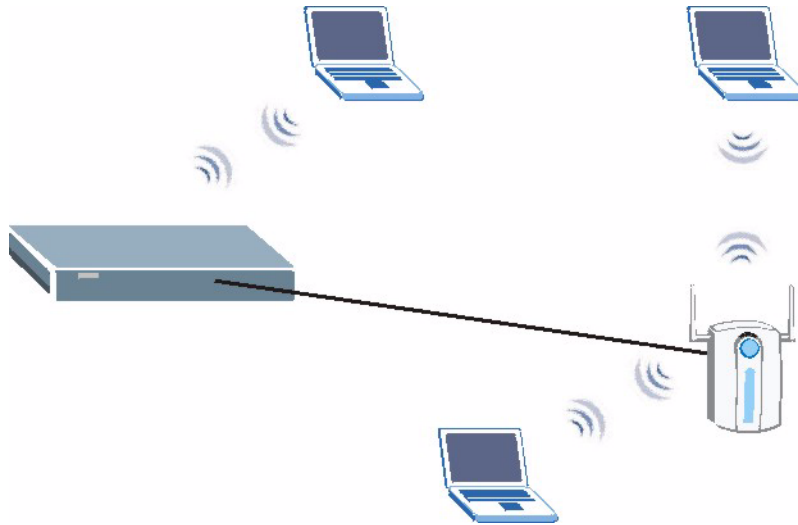
LABEL	DESCRIPTION
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 5.8 LAN Port Roles

Use the **Port Roles** screen to set ports as LAN, DMZ or WLAN interfaces. The LAN port role is not available on all models.

Connect wireless LAN Access Points (APs) to WLAN interfaces to extend the ZyWALL's wireless LAN coverage. The WLAN port role allows the ZyWALL's firewall to treat traffic from connected APs as part of the ZyWALL's WLAN. You can specify firewall rules for traffic going to or from the WLAN. The WLAN includes the ZyWALL's own WLAN and the Ethernet ports in the WLAN port role.

The following figure shows the ZyWALL with a wireless card installed and an AP connected to an Ethernet port in the WLAN port role.

**Figure 39** WLAN Port Role Example

**Note:** Do the following if you are configuring from a computer connected to a LAN, DMZ or WLAN port and changing the port's role:

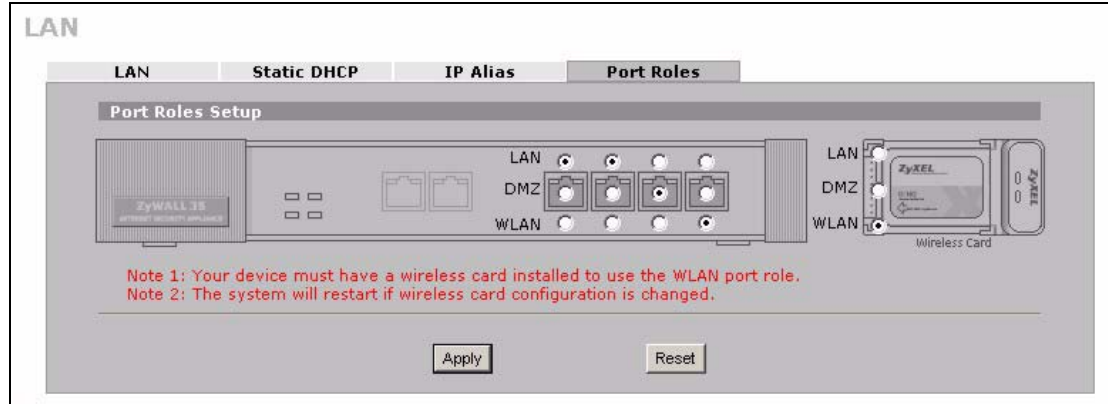
1. A port's IP address varies as its role changes, make sure your computer's IP address is in the same subnet as the ZyWALL's LAN, DMZ or WLAN IP address.
2. Use the appropriate LAN, DMZ or WLAN IP address to access the ZyWALL.

To change your ZyWALL's port role settings, click **NETWORK**, **LAN** and then the **Port Roles** tab. The screen appears as shown.

The radio buttons on the left correspond to Ethernet ports on the front panel of the ZyWALL. Ports 1 to 4 are all LAN ports by default. The radio buttons on the right are for the wireless card.

**Note:** Your changes are also reflected in the **DMZ Port Roles** and **WLAN Port Roles** screens.

**Figure 40** LAN Port Roles



The following table describes the labels in this screen.

**Table 25** LAN Port Roles

LABEL	DESCRIPTION
LAN	Select a port's LAN radio button to use the port as part of the LAN. The port will use the LAN IP address and MAC address.
DMZ	Select a port's DMZ radio button to use the port as part of the DMZ. The port will use the DMZ IP address and MAC address.
WLAN	When you have the wireless card set to <b>WLAN</b> , you can select a port's WLAN radio button to use the port as part of the WLAN. The port will use the ZyWALL's WLAN IP address and the MAC address of the WLAN card.  <b>Note:</b> You must install a wireless card to use the WLAN port role. See <a href="#">Appendix A on page 664</a> for how to install a WLAN card.
Wireless Card	Select <b>LAN</b> to use the wireless card as part of the LAN. Select <b>DMZ</b> to use the wireless card as part of the DMZ. Select <b>WLAN</b> to use the wireless card as part of the WLAN. The ZyWALL restarts after you change the wireless card setting.  <b>Note:</b> If you set the wireless card to be part of the LAN or DMZ, you can still use wireless access, but not the WLAN interface in the firewall. The firewall will treat the wireless card as part of the LAN or DMZ respectively.

**Table 25** LAN Port Roles (continued)

LABEL	DESCRIPTION
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

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

**Figure 41** Port Roles Change Complete



# CHAPTER 6

## Bridge Screens

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

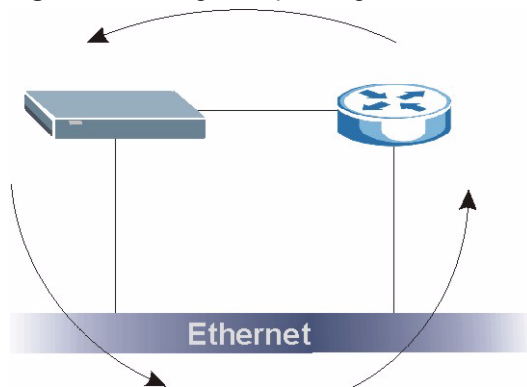
### 6.1 Bridge Loop

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

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

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

**Figure 42** Bridge Loop: Bridge Connected to Wired LAN



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

### 6.2 Spanning Tree Protocol (STP)

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

## 6.2.1 Rapid STP

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

## 6.2.2 STP Terminology

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

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

**Table 26** STP Path Costs

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

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

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

## 6.2.3 How STP Works

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

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

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

## 6.2.4 STP Port States

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

**Table 27** STP Port States

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

## 6.3 Bridge

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

Click **NETWORK, BRIDGE** to display the screen shown next. Use this screen to configure bridge and RSTP (Rapid Spanning Tree Protocol) settings.



**Figure 43** Bridge

The following table describes the labels in this screen.

**Table 28** Bridge

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

**Table 28** Bridge (continued)

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

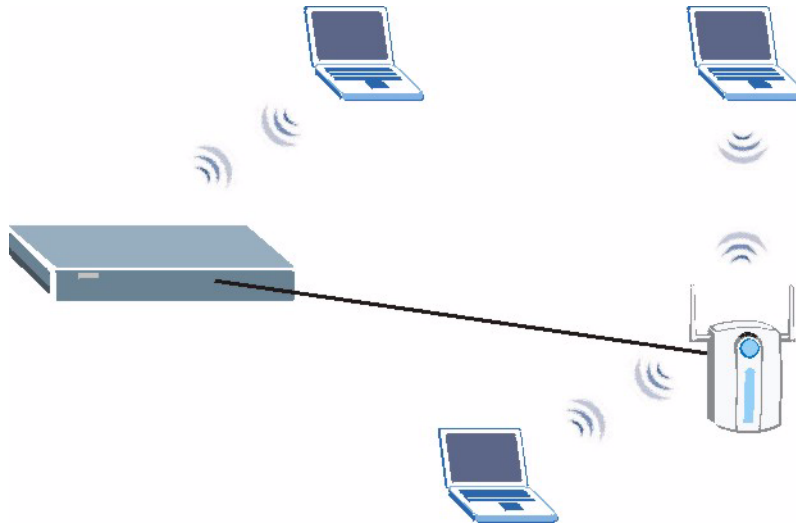
## 6.4 Bridge Port Roles

Use the **Port Roles** screen to set ports as LAN, DMZ or WLAN interfaces. The LAN port role is not available on all models.

Connect wireless LAN Access Points (APs) to WLAN interfaces to extend the ZyWALL's wireless LAN coverage. The WLAN port role allows the ZyWALL's firewall to treat traffic from connected APs as part of the ZyWALL's WLAN. You can specify firewall rules for traffic going to or from the WLAN. The WLAN includes the ZyWALL's own WLAN and the Ethernet ports in the WLAN port role.

The following figure shows the ZyWALL with a wireless card installed and an AP connected to an Ethernet port in the WLAN port role.

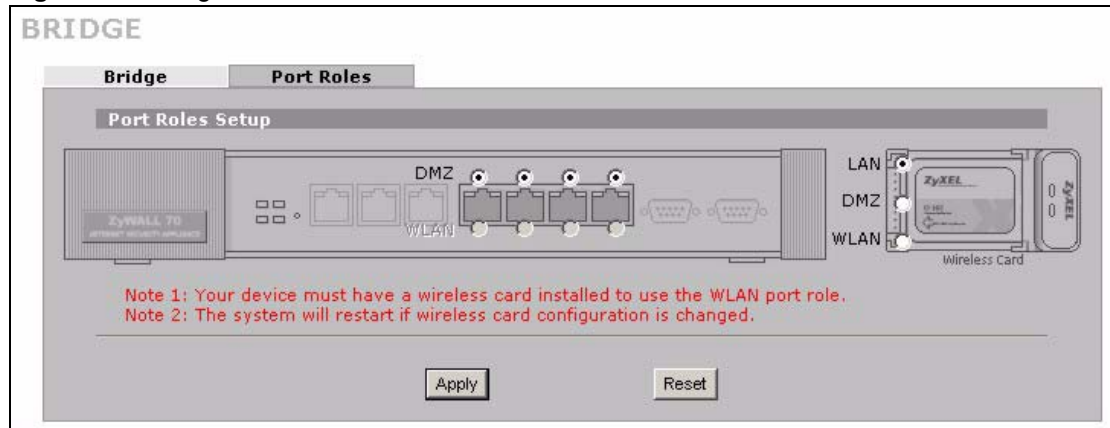
**Figure 44** WLAN Port Role Example



To change your ZyWALL's port role settings, click **NETWORK**, **BRIDGE** and then the **Port Roles** tab. The screen appears as shown.

The radio buttons on the left correspond to Ethernet ports on the front panel of the ZyWALL. Ports 1 to 4 are all DMZ ports on the ZyWALL 70 and all LAN ports on the ZyWALL 5 or ZyWALL 35 by default. The radio buttons on the right are for the WLAN card.

**Figure 45** Bridge Port Roles



The following table describes the labels in this screen.

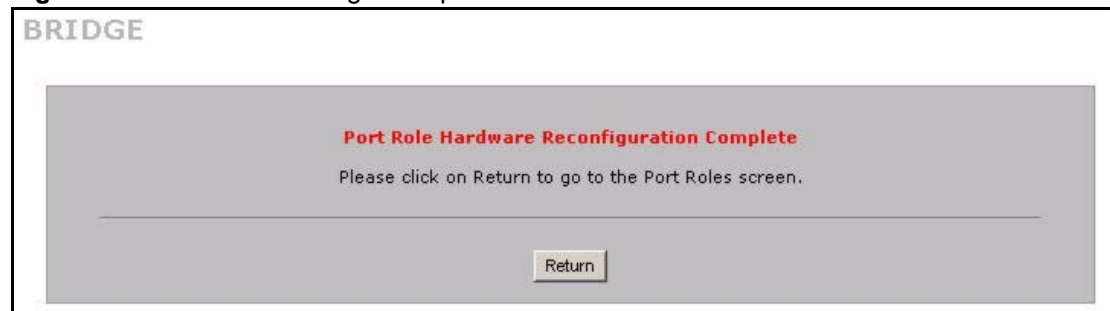
**Table 29** Bridge Port Roles

LABEL	DESCRIPTION
LAN	Select a port's LAN radio button to use the port as part of the LAN. The port will use the LAN IP address and MAC address.
DMZ	Select a port's DMZ radio button to use the port as part of the DMZ. The port will use the DMZ IP address and MAC address.

**Table 29** Bridge Port Roles (continued)

LABEL	DESCRIPTION
WLAN	<p>When you have the wireless card set to <b>WLAN</b>, you can select a port's WLAN radio button to use the port as part of the WLAN.</p> <p>The port will use the ZyWALL's WLAN IP address and the MAC address of the WLAN card.</p> <p><b>Note:</b> You must install a wireless card to use the WLAN port role. See <a href="#">Appendix A on page 664</a> for how to install a WLAN card.</p>
Wireless Card	<p>Select <b>LAN</b> to use the wireless card as part of the LAN.</p> <p>Select <b>DMZ</b> to use the wireless card as part of the DMZ.</p> <p>Select <b>WLAN</b> to use the wireless card as part of the WLAN.</p> <p>The ZyWALL restarts after you change the wireless card setting.</p> <p><b>Note:</b> If you set the wireless card to be part of the LAN or DMZ, you can still use wireless access, but not the WLAN interface in the firewall. The firewall will treat the wireless card as part of the LAN or DMZ respectively.</p>
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

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

**Figure 46** Port Roles Change Complete



# CHAPTER 7

## WAN Screens

This chapter describes how to configure WAN settings. Multiple WAN and load balancing are not available on the ZyWALL 5.

### 7.1 WAN Overview

- Use the **WAN General** screen to configure load balancing, route priority and traffic redirect properties for the ZyWALL 70 and ZyWALL 35.
- Use the **WAN Route** screen to configure route priority for the ZyWALL 5.
- Use the **WAN1** screen to configure the WAN1 port for Internet access on the ZyWALL 70 and ZyWALL 35.
- Use the **WAN2** screen to configure the WAN2 port for Internet access on the ZyWALL 70 and ZyWALL 35.
- Use the **WAN** screen to configure the WAN port for Internet access on the ZyWALL 5.
- Use the **Traffic Redirect** screen to configure your traffic redirect properties and parameters.
- Use the **Dial Backup** screen to configure the backup WAN dial-up connection.

### 7.2 Multiple WAN

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

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

The ZyWALL can balance the load between the two WAN ports (see [Section 7.3 on page 131](#)).

You can use policy routing to specify the WAN port that specific services go through. An ISP may give traffic from certain (more expensive) connections priority over the traffic from other accounts. You could route delay intolerant traffic (like voice over IP calls) through this kind of connection. Other traffic could be routed through a cheaper broadband Internet connection that does not provide priority service. If one WAN port's connection goes down, the ZyWALL can automatically send its traffic through the other WAN port. See [Chapter 24 on page 396](#) for details.

The ZyWALL's NAT feature allows you to configure sets of rules for one WAN port and separate sets of rules for the other WAN port. Refer to [Chapter 22 on page 374](#) for details.

You can select through which WAN port you want to send out traffic from UPnP-enabled applications (see [Chapter 28 on page 456](#)).

The ZyWALL's DDNS lets you select which WAN interface you want to use for each individual domain name. The DDNS high availability feature lets you have the ZyWALL use the other WAN interface for a domain name if the configured WAN interface's connection goes down. See [Section 26.10.2 on page 428](#) for details.

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

## 7.3 Load Balancing Introduction

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

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

## 7.4 Load Balancing Algorithms

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

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

### 7.4.1 Least Load First

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

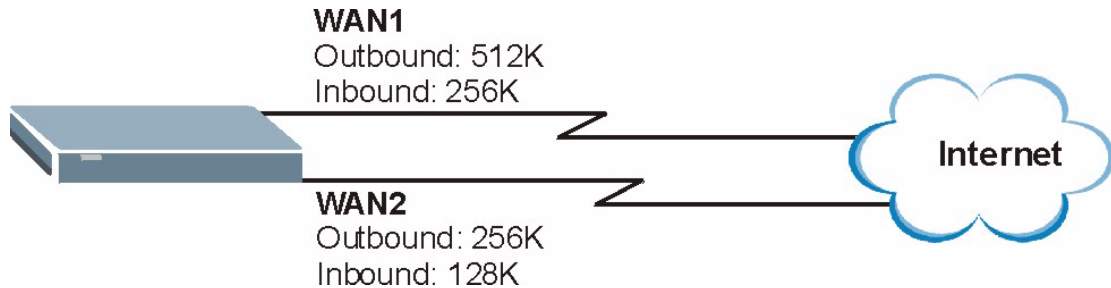
---

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

### 7.4.1.1 Example 1

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

**Figure 47** Least Load First Example



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

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

**Table 30** Least Load First: Example 1

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

### 7.4.1.2 Example 2

This example uses the same network scenario as in [Figure 47 on page 132](#), but uses both the outbound and inbound bandwidth utilization in calculating the load balancing index. If the measured inbound stream throughput for both WAN 1 and WAN 2 is 102K, the ZyWALL calculates the average load balancing indices as shown in the table below.

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

**Table 31** Least Load First: Example 2

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



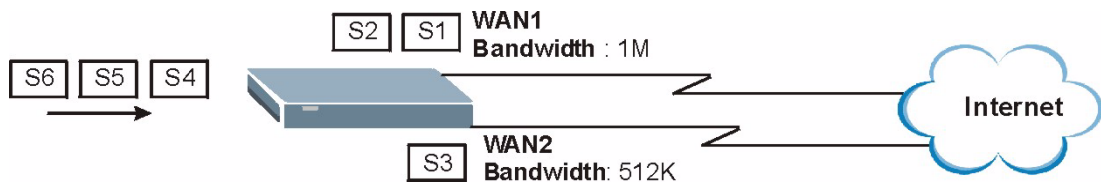
## 7.4.2 Weighted Round Robin

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

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

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

**Figure 48** Weighted Round Robin Algorithm Example

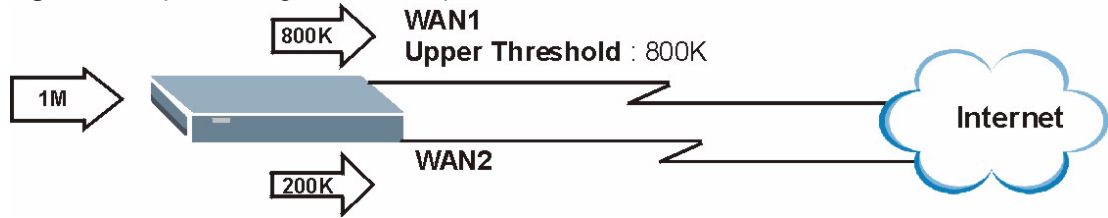


## 7.4.3 Spillover

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

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

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

**Figure 49** Spillover Algorithm Example

## 7.5 TCP/IP Priority (Metric)

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

- 1 The metric sets the priority for the ZyWALL's routes to the Internet. Each route must have a unique metric.
- 2 The priorities of the WAN port routes must always be higher than the dial-backup and traffic redirect route priorities.

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

For a ZyWALL with a single WAN port, if the WAN port route has a metric of "1" and the traffic-redirect route has a metric of "2" and dial-backup route has a metric of "3", then the WAN port route acts as the primary default route. If the WAN port route fails to connect to the Internet, the ZyWALL tries the traffic-redirect route next. In the same manner, the ZyWALL uses the dial-backup route if the traffic-redirect route also fails.

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

## 7.6 WAN General

Click **NETWORK**, **WAN** to open the **General** screen. Use this screen to configure load balancing, route priority and traffic redirect properties.

**Figure 50** WAN General

### WAN

**General**
**WAN 1**
**WAN 2**
**Traffic Redirect**
**Dial Backup**

**Operation Mode**

- Active/Passive (Fail Over) Mode
  - Fall Back to Primary WAN When Possible
- Active/Active Mode
  - Load Balancing Algorithm:

**Route Priority**

WAN 1	Priority (metric)	<input type="text" value="1"/>	1(Highest) ~ 15(Lowest)
WAN 2	Priority (metric)	<input type="text" value="2"/>	1(Highest) ~ 15(Lowest)
Traffic Redirect	Priority (metric)	<input type="text" value="14"/>	1(Highest) ~ 15(Lowest)
Dial Backup	Priority (metric)	<input type="text" value="15"/>	1(Highest) ~ 15(Lowest)

**Connectivity Check**

Check Period:  5 ~ 300 (Seconds)

Check Timeout:  1 ~ 10 (Seconds)

Check Fail Tolerance:  1 ~ 10 (Successive Checks)

- Check WAN 1 Connectivity
  - Ping Default Gateway: 172.23.19.254
  - Ping this Address:  (Domain Name or IP Address)
- Check WAN 2 Connectivity
  - Ping Default Gateway: 0.0.0.0
  - Ping this Address:  (Domain Name or IP Address)
- Check Traffic Redirection Connectivity
  - Ping Default Gateway: 0.0.0.0
  - Ping this Address:  (Domain Name or IP Address)

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

- Allow between WAN and LAN
- Allow between WAN and DMZ
- Allow between WAN and WLAN
- Allow Trigger Dial

Note: You also need to create a [Firewall](#) rule.

The following table describes the labels in this screen.

**Table 32** WAN General

LABEL	DESCRIPTION
Active/Passive (Fail Over) Mode	Select the Active/Passive (fail over) operation mode to have the ZyWALL use the second highest priority WAN port as a back up. This means that the ZyWALL will normally use the highest priority (primary) WAN port (depending on the priorities you configure in the <b>Route Priority</b> fields). The ZyWALL will switch to the secondary (second highest priority) WAN port when the primary WAN port's connection fails.
Fall Back to Primary WAN When Possible	This field determines the action the ZyWALL takes after the primary WAN port fails and the ZyWALL starts using the secondary WAN port. Select this check box to have the ZyWALL change back to using the primary WAN port when the ZyWALL can connect through the primary WAN port again. Clear this check box to have the ZyWALL continue using the secondary WAN port, even after the ZyWALL can connect through the primary WAN port again. The ZyWALL continues to use the secondary WAN port until it's connection fails (at which time it will change back to using the primary WAN port if its connection is up).
Active/Active Mode	Select <b>Active/Active Mode</b> to have the ZyWALL use both of the WAN ports at the same time and allow you to enable load balancing.
Load Balancing Algorithm	Select <b>Least Load First</b> , <b>Weighted Round Robin</b> or <b>Spillover</b> to activate load balancing and set the related fields. Otherwise, select <b>None</b> . Refer to <a href="#">Section 7.7 on page 137</a> for load balancing configuration.
Route Priority	
WAN1 WAN2 Traffic Redirect Dial Backup	The default WAN connection is "1" as your broadband connection via the WAN port should always be your preferred method of accessing the WAN. The ZyWALL switches from WAN port 1 to WAN port 2 if WAN port 1's connection fails and then back to WAN port 1 when WAN port 1's connection comes back up. The default priority of the routes is <b>WAN 1</b> , <b>WAN 2</b> , <b>Traffic Redirect</b> and then <b>Dial Backup</b> : You have three choices for an auxiliary connection ( <b>WAN 2</b> , <b>Traffic Redirect</b> and <b>Dial Backup</b> ) in the event that your regular WAN connection goes down. If <b>Dial Backup</b> is preferred to <b>Traffic Redirect</b> , then type "14" in the <b>Dial Backup Priority (metric)</b> field (and leave the <b>Traffic Redirect Priority (metric)</b> at the default of "15"). The <b>Dial Backup</b> field is available only when you enable the corresponding dial backup feature in the <b>Dial Backup</b> screen.
Connectivity Check	
Check Period	The ZyWALL tests a WAN connection by periodically sending a ping to either the default gateway or the address in the <b>Ping this Address</b> field. Type a number of seconds (5 to 300) to set the time interval between checks. Allow more time if your destination IP address handles lots of traffic.
Check Timeout	Type the number of seconds (1 to 10) for your ZyWALL to wait for a response to the ping before considering the check to have failed. This setting must be less than the <b>Check Period</b> . Use a higher value in this field if your network is busy or congested.
Check Fail Tolerance	Type how many WAN connection checks can fail (1-10) before the connection is considered "down" (not connected). The ZyWALL still checks a "down" connection to detect if it reconnects.

**Table 32** WAN General (continued)

LABEL	DESCRIPTION
Check WAN1/2 Connectivity	<p>Select the check box to have the ZyWALL periodically test the respective WAN port's connection.</p> <p>Select <b>Ping Default Gateway</b> to have the ZyWALL ping the WAN port's default gateway IP address.</p> <p>Select <b>Ping this Address</b> and enter a domain name or IP address of a reliable nearby computer (for example, your ISP's DNS server address) to have the ZyWALL ping that address. For a domain name, use up to 63 alphanumeric characters (hyphens, periods and the underscore are also allowed) without spaces.</p>
Check Traffic Redirection Connectivity	<p>Select the check box to have the ZyWALL periodically test the traffic redirect connection.</p> <p>Select <b>Ping Default Gateway</b> to have the ZyWALL ping the backup gateway's IP address.</p> <p>Select <b>Ping this Address</b> and enter a domain name or IP address of a reliable nearby computer (for example, your ISP's DNS server address) to have the ZyWALL ping that address. For a domain name, use up to 63 alphanumeric characters (hyphens, periods and the underscore are also allowed) without spaces.</p>
Windows Networking (NetBIOS over TCP/IP):	<p>NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls.</p>
Allow between WAN and LAN	<p>Select this check box to forward NetBIOS packets from the LAN to the WAN and from the WAN to the LAN. If your firewall is enabled with the default policy set to block WAN to LAN traffic, you also need to enable the default WAN to LAN firewall rule that forwards NetBIOS traffic.</p> <p>Clear this check box to block all NetBIOS packets going from the LAN to the WAN and from the WAN to the LAN.</p>
Allow between WAN and DMZ	<p>Select this check box to forward NetBIOS packets from the WAN to the DMZ and from the DMZ to the WAN.</p> <p>Clear this check box to block all NetBIOS packets going from the WAN to the DMZ and from the DMZ to the WAN.</p>
Allow between WAN and WLAN	<p>Select this check box to forward NetBIOS packets from the WLAN to the WAN and from the WAN to the WLAN.</p> <p>Clear this check box to block all NetBIOS packets going from the WLAN to the WAN and from the WAN to the WLAN.</p>
Allow Trigger Dial	<p>Select this option to allow NetBIOS packets to initiate calls.</p>
Apply	<p>Click <b>Apply</b> to save your changes back to the ZyWALL.</p>
Reset	<p>Click <b>Reset</b> to begin configuring this screen afresh.</p>

## 7.7 Configuring Load Balancing

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

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

## 7.7.1 Least Load First

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

**Figure 51** Load Balancing: Least Load First

The screenshot shows the WAN configuration interface with the following settings:

- Operation Mode:** Active/Active Mode (selected), with the checkbox **Fall Back to Primary WAN When Possible** checked.
- Load Balancing Algorithm:** Least Load First (selected in the dropdown).
- Time Frame:** 600 (with a range of 10(Seconds) - 600(Seconds)).
- Load Balancing Index(es):** Outbound Only (selected in the dropdown).

Interface	Available Inbound Bandwidth	Available Outbound Bandwidth
WAN 1	100 Kbps	100 Kbps
WAN 2	100 Kbps	100 Kbps

The following table describes the related fields in this screen.

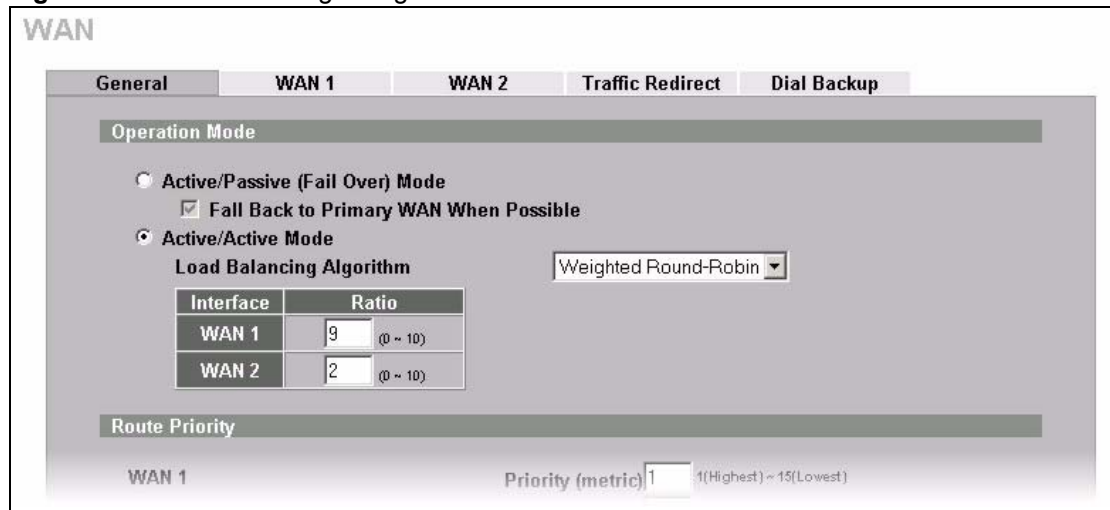
**Table 33** Load Balancing: Least Load First

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

## 7.7.2 Weighted Round Robin

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

**Figure 52** Load Balancing: Weighted Round Robin



The following table describes the related fields in this screen.

**Table 34** Load Balancing: Weighted Round Robin

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

## 7.7.3 Spillover

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

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

**Figure 53** Load Balancing: Spillover

The screenshot shows the 'WAN' configuration screen. The 'Operation Mode' section has two radio buttons: 'Active/Passive (Fail Over) Mode' (unselected) and 'Active/Active Mode' (selected). Under 'Active/Active Mode', there is a checked box for 'Fall Back to Primary WAN When Possible'. The 'Load Balancing Algorithm' is a dropdown menu set to 'Spillover'. The 'Time Frame' is a text input field containing '600', with a note '10(Seconds) ~ 600(Seconds)'. Below this, there is a text input field for 'Send traffic to secondary WAN when primary WAN bandwidth exceeds' set to '1000', followed by 'kbps'. At the bottom, there is a 'Route Priority' section.

The following table describes the related fields in this screen.

**Table 35** Load Balancing: Spillover

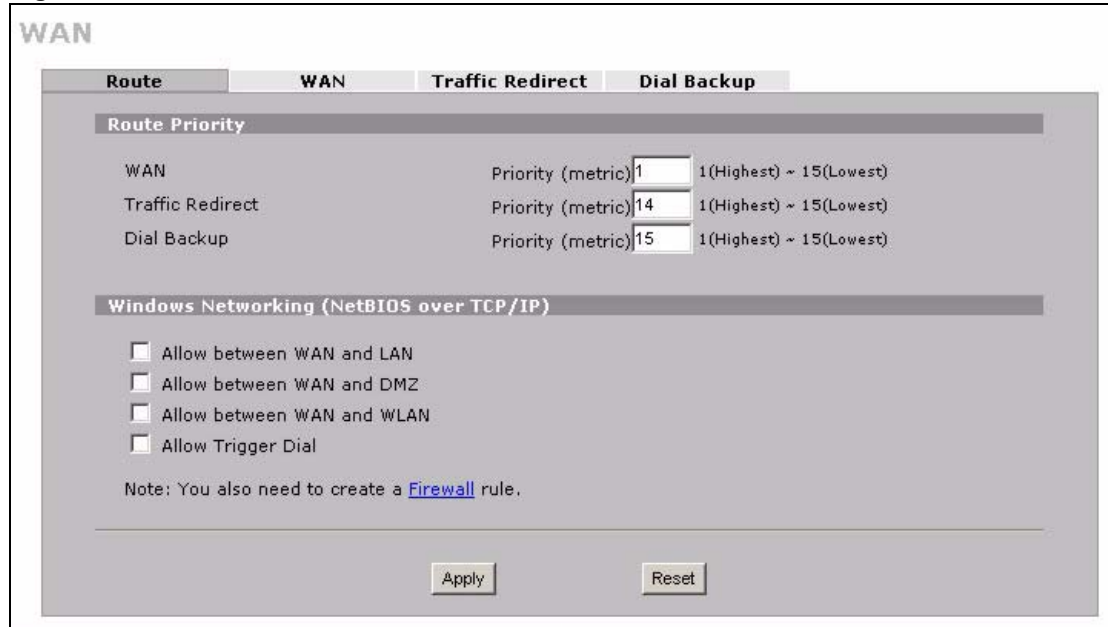
LABEL	DESCRIPTION
Active/Active Mode	Select <b>Active/Active Mode</b> and set the related fields to enable load balancing on the ZyWALL.
Load Balancing Algorithm	Select a load balancing method to use from the drop-down list box.
Time Frame	You can set the ZyWALL to get the measured bandwidth using the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

## 7.8 WAN Route

Click **NETWORK**, **WAN** to open the **Route** screen. Use this screen to configure route priority.



**Figure 54** WAN Route



The following table describes the labels in this screen.

**Table 36** WAN Route

LABEL	DESCRIPTION
Route Priority	
WAN Traffic Redirect Dial Backup	<p>The default WAN connection is "1" as your broadband connection via the WAN port should always be your preferred method of accessing the WAN. The default priority of the routes is <b>WAN</b>, <b>Traffic Redirect</b> and then <b>Dial Backup</b>:</p> <p>You have two choices for an auxiliary connection (<b>Traffic Redirect</b> and <b>Dial Backup</b>) in the event that your regular WAN connection goes down. If <b>Dial Backup</b> is preferred to <b>Traffic Redirect</b>, then type "14" in the <b>Dial Backup Priority (metric)</b> field (and leave the <b>Traffic Redirect Priority (metric)</b> at the default of "15").</p> <p>The <b>Dial Backup</b> field is available only when you enable the corresponding dial backup feature in the <b>Dial Backup</b> screen.</p>
Windows Networking (NetBIOS over TCP/IP):	<p>NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls.</p>
Allow between WAN and LAN	<p>Select this check box to forward NetBIOS packets from the LAN to the WAN and from the WAN to the LAN. If your firewall is enabled with the default policy set to block WAN to LAN traffic, you also need to enable the default WAN to LAN firewall rule that forwards NetBIOS traffic.</p> <p>Clear this check box to block all NetBIOS packets going from the LAN to the WAN and from the WAN to the LAN.</p>
Allow between WAN and DMZ	<p>Select this check box to forward NetBIOS packets from the WAN to the DMZ and from the DMZ to the WAN.</p> <p>Clear this check box to block all NetBIOS packets going from the WAN to the DMZ and from the DMZ to the WAN.</p>

**Table 36** WAN Route (continued)

LABEL	DESCRIPTION
Allow between WAN and WLAN	Select this check box to forward NetBIOS packets from the WLAN to the WAN and from the WAN to the WLAN. Clear this check box to block all NetBIOS packets going from the WLAN to the WAN and from the WAN to the WLAN.
Allow Trigger Dial	Select this option to allow NetBIOS packets to initiate calls.
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 7.9 WAN IP Address Assignment

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

**Table 37** Private IP Address Ranges

10.0.0.0	-	10.255.255.255
172.16.0.0	-	172.31.255.255
192.168.0.0	-	192.168.255.255

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

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

## 7.10 DNS Server Address Assignment

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa, for instance, the IP address of [www.zyxel.com](http://www.zyxel.com) is 204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

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

- 1 The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, manually enter them in the DNS server fields.
- 2 If your ISP dynamically assigns the DNS server IP addresses (along with the ZyWALL's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.
- 3 You can manually enter the IP addresses of other DNS servers. These servers can be public or private. A DNS server could even be behind a remote IPSec router (see [Section 26.5.1 on page 419](#)).

## 7.11 WAN MAC Address

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

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

**Table 38** 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)

## 7.12 WAN

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

**Note:** The WAN1 and WAN2 IP addresses of a ZyWALL with multiple WAN ports must be on different subnets.

### 7.12.1 WAN Ethernet Encapsulation

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

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

**Figure 55** WAN: Ethernet Encapsulation

The following table describes the labels in this screen.

**Table 39** WAN: Ethernet Encapsulation

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

**Table 39** WAN: Ethernet Encapsulation (continued)

LABEL	DESCRIPTION
Retype to Confirm	Type your password again to make sure that you have entered is correctly.
Login Server IP Address	Type the authentication server IP address here if your ISP gave you one. This field is not available for Telia Login.
Login Server (Telia Login only)	Type the domain name of the Telia login server, for example login1.telia.com.
Relogin Every(min) (Telia Login only)	The Telia server logs the ZyWALL out if the ZyWALL does not log in periodically. Type the number of minutes from 1 to 59 (30 default) for the ZyWALL to wait between logins.
WAN IP Address Assignment	
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
My WAN IP Address	Enter your WAN IP address in this field if you selected <b>Use Fixed IP Address</b> .
My WAN IP Subnet Mask	Enter the IP subnet mask (if your ISP gave you one) in this field if you selected <b>Use Fixed IP Address</b> .
Gateway IP Address	Enter the gateway IP address (if your ISP gave you one) in this field if you selected <b>Use Fixed IP Address</b> .
Advanced Setup	
Enable NAT (Network Address Translation)	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet). Select this check box to enable NAT.
RIP Direction	RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The <b>RIP Direction</b> field controls the sending and receiving of RIP packets. Choose <b>Both</b> , <b>None</b> , <b>In Only</b> or <b>Out Only</b> . When set to <b>Both</b> or <b>Out Only</b> , the ZyWALL will broadcast its routing table periodically. When set to <b>Both</b> or <b>In Only</b> , the ZyWALL will incorporate RIP information that it receives. When set to <b>None</b> , the ZyWALL will not send any RIP packets and will ignore any RIP packets received. By default, <b>RIP Direction</b> is set to <b>Both</b> .

**Table 39** WAN: Ethernet Encapsulation (continued)

LABEL	DESCRIPTION
RIP Version	<p>The <b>RIP Version</b> field controls the format and the broadcasting method of the RIP packets that the ZyWALL sends (it recognizes both formats when receiving).</p> <p>Choose <b>RIP-1</b>, <b>RIP-2B</b> or <b>RIP-2M</b>.</p> <p><b>RIP-1</b> is universally supported; but <b>RIP-2</b> carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both <b>RIP-2B</b> and <b>RIP-2M</b> sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, the <b>RIP Version</b> field is set to <b>RIP-1</b>.</p>
Enable Multicast	<p>Select this check box to turn on IGMP (Internet Group Multicast Protocol). IGMP is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data.</p>
Multicast Version	<p>Choose <b>None</b> (default), <b>IGMP-V1</b> or <b>IGMP-V2</b>. IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236.</p>
Spoof WAN MAC Address	<p>You can use the factory assigned default MAC Address or cloning the MAC address from a computer on your LAN.</p> <p>Otherwise, select the check box next to <b>Spoof WAN MAC Address</b> and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different ROM file.</p>
Clone the computer's MAC address - IP Address	<p>Enter the IP address of the computer on the LAN whose MAC you are cloning. It is recommended that you clone the MAC address prior to hooking up the WAN port.</p>
Apply	<p>Click <b>Apply</b> to save your changes back to the ZyWALL.</p>
Reset	<p>Click <b>Reset</b> to begin configuring this screen afresh.</p>

## 7.12.2 PPPoE Encapsulation

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

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example RADIUS).

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

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the ZyWALL (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the ZyWALL does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

Refer to [Appendix F on page 702](#) for more information on PPPoE.

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

**Figure 56** WAN: PPPoE Encapsulation

**WAN**

General **WAN 1** WAN 2 Traffic Redirect Dial Backup

**ISP Parameters for Internet Access**

Encapsulation: PPP over Ethernet

Service Name: (Optional)

User Name: [ ]

Password: [ ]

Retype to Confirm: [ ]

Authentication Type: CHAP/PAP

Nailed-Up

Idle Timeout: 0 (Seconds)

**WAN IP Address Assignment**

Get Automatically from ISP

Use Fixed IP Address

My WAN IP Address: 0 . 0 . 0 . 0

**Advanced Setup**

Enable NAT (Network Address Translation)

RIP Direction: None

RIP Version: RIP-1

Enable Multicast

Multicast Version: IGMP-v1

Spoof WAN MAC Address

Clone the computer's MAC address - IP Address: 192 . 168 . 1 . 33

Apply Reset

The following table describes the labels in this screen.

**Table 40** WAN: PPPoE Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	The PPPoE choice is for a dial-up connection using PPPoE. The router supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (i.e. DSL, cable, wireless, etc.) connection. Operationally, PPPoE saves significant effort for both the end user and ISP/carrier, as it requires no specific configuration of the broadband modem at the customer site. By implementing PPPoE directly on the router rather than individual computers, the computers on the LAN do not need PPPoE software installed, since the router does that part of the task. Further, with NAT, all of the LAN's computers will have access.
Service Name	Type the PPPoE service name provided to you. PPPoE uses a service name to identify and reach the PPPoE server.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.
Authentication Type	Use the drop-down list box to select an authentication protocol for outgoing calls. Options are: <b>CHAP/PAP</b> - Your ZyWALL accepts either CHAP or PAP when requested by this remote node. <b>CHAP</b> - Your ZyWALL accepts CHAP only. <b>PAP</b> - Your ZyWALL accepts PAP only.
Nailed-Up	Select <b>Nailed-Up</b> if you do not want the connection to time out.
Idle Timeout	This value specifies the time in seconds that elapses before the ZyWALL automatically disconnects from the PPPoE server.
WAN IP Address Assignment	
Get automatically from ISP	Select this option if your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option if the ISP assigned a fixed IP address.
My WAN IP Address	Enter your WAN IP address in this field if you selected <b>Use Fixed IP Address</b> .
Advanced Setup	
Enable NAT (Network Address Translation)	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet). Select this checkbox to enable NAT. For more information about NAT see <a href="#">Chapter 22 on page 374</a> .



**Table 40** WAN: PPPoE Encapsulation

LABEL	DESCRIPTION
RIP Direction	<p>RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The <b>RIP Direction</b> field controls the sending and receiving of RIP packets.</p> <p>Choose <b>Both</b>, <b>None</b>, <b>In Only</b> or <b>Out Only</b>.</p> <p>When set to <b>Both</b> or <b>Out Only</b>, the ZyWALL will broadcast its routing table periodically.</p> <p>When set to <b>Both</b> or <b>In Only</b>, the ZyWALL will incorporate RIP information that it receives.</p> <p>When set to <b>None</b>, the ZyWALL will not send any RIP packets and will ignore any RIP packets received.</p> <p>By default, <b>RIP Direction</b> is set to <b>Both</b>.</p>
RIP Version	<p>The <b>RIP Version</b> field controls the format and the broadcasting method of the RIP packets that the ZyWALL sends (it recognizes both formats when receiving).</p> <p>Choose <b>RIP-1</b>, <b>RIP-2B</b> or <b>RIP-2M</b>.</p> <p><b>RIP-1</b> is universally supported; but <b>RIP-2</b> carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both <b>RIP-2B</b> and <b>RIP-2M</b> sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, the <b>RIP Version</b> field is set to <b>RIP-1</b>.</p>
Enable Multicast	<p>Select this check box to turn on IGMP (Internet Group Multicast Protocol). IGMP is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data.</p>
Multicast Version	<p>Choose <b>None</b> (default), <b>IGMP-V1</b> or <b>IGMP-V2</b>. IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group – it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236.</p>
Spoof WAN MAC Address	<p>You can use the factory assigned default MAC Address or cloning the MAC address from a computer on your LAN.</p> <p>Otherwise, select the check box next to <b>Spoof WAN MAC Address</b> and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different ROM file.</p>
Clone the computer's MAC address – IP Address	<p>Enter the IP address of the computer on the LAN whose MAC you are cloning. It is recommended that you clone the MAC address prior to hooking up the WAN port.</p>
Apply	<p>Click <b>Apply</b> to save your changes back to the ZyWALL.</p>
Reset	<p>Click <b>Reset</b> to begin configuring this screen afresh.</p>

## 7.12.3 PPTP Encapsulation

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

PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet. The screen shown next is for **PPTP** encapsulation.

Refer to [Appendix G on page 704](#) for more information on PPTP.

**Figure 57** WAN: PPTP Encapsulation

**WAN**

General | **WAN 1** | WAN 2 | Traffic Redirect | Dial Backup

**ISP Parameters for Internet Access**

Encapsulation: PPTP

User Name: [ ]

Password: [ ]

Retype to Confirm: [ ]

Authentication Type: CHAP/PAP

Nailed-Up

Idle Timeout: 0 (Seconds)

**PPTP Configuration**

My IP Address: 0 . 0 . 0 . 0

My IP Subnet Mask: 0 . 0 . 0 . 0

Server IP Address: 0 . 0 . 0 . 0

Connection ID/Name: [ ]

**WAN IP Address Assignment**

Get Automatically from ISP

Use Fixed IP Address

My WAN IP Address: 0 . 0 . 0 . 0

**Advanced Setup**

Enable NAT (Network Address Translation)

RIP Direction: None

RIP Version: RIP-1

Enable Multicast

Multicast Version: IGMP-v1

Spoof WAN MAC Address

Clone the computer's MAC address - IP Address: 192 . 168 . 1 . 33

Apply | Reset

The following table describes the labels in this screen.

**Table 41** WAN: PPTP Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks. PPTP supports on-demand, multi-protocol, and virtual private networking over public networks, such as the Internet. The ZyWALL supports only one PPTP server connection at any given time. To configure a PPTP client, you must configure the <b>User Name</b> and <b>Password</b> fields for a PPP connection and the PPTP parameters for a PPTP connection.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.
Authentication Type	Use the drop-down list box to select an authentication protocol for outgoing calls. Options are: <b>CHAP/PAP</b> - Your ZyWALL accepts either CHAP or PAP when requested by this remote node. <b>CHAP</b> - Your ZyWALL accepts CHAP only. <b>PAP</b> - Your ZyWALL accepts PAP only.
Nailed-up	Select <b>Nailed-Up</b> if you do not want the connection to time out.
Idle Timeout	This value specifies the time in seconds that elapses before the ZyWALL automatically disconnects from the PPTP server.
PPTP Configuration	
My IP Address	Type the (static) IP address assigned to you by your ISP.
My IP Subnet Mask	Your ZyWALL will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyWALL.
Server IP Address	Type the IP address of the PPTP server.
Connection ID/ Name	Type your identification name for the PPTP server.
WAN IP Address Assignment	
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use Fixed IP Address	Select this option If the ISP assigned a fixed IP address.
My WAN IP Address	Enter your WAN IP address in this field if you selected <b>Use Fixed IP Address</b> .
Advanced Setup	

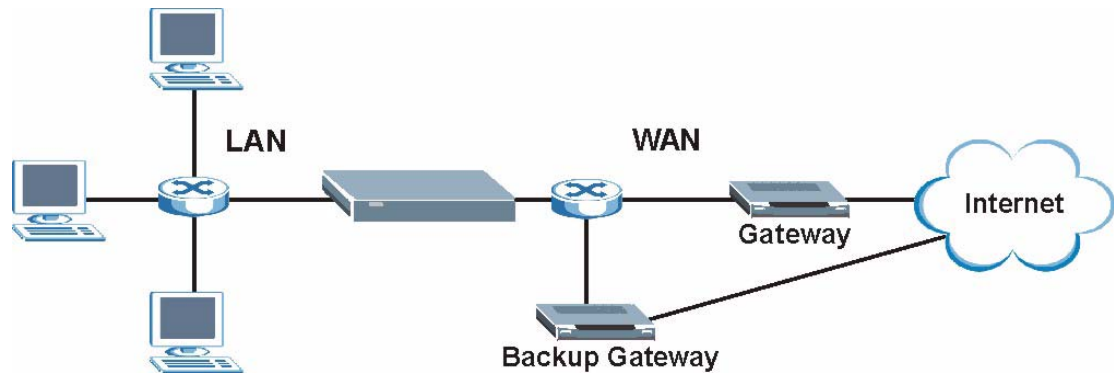
**Table 41** WAN: PPTP Encapsulation

LABEL	DESCRIPTION
Enable NAT (Network Address Translation)	<p>Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet).</p> <p>Select this checkbox to enable NAT.</p> <p>For more information about NAT see <a href="#">Chapter 22 on page 374</a>.</p>
RIP Direction	<p>RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The <b>RIP Direction</b> field controls the sending and receiving of RIP packets.</p> <p>Choose <b>Both</b>, <b>None</b>, <b>In Only</b> or <b>Out Only</b>.</p> <p>When set to <b>Both</b> or <b>Out Only</b>, the ZyWALL will broadcast its routing table periodically.</p> <p>When set to <b>Both</b> or <b>In Only</b>, the ZyWALL will incorporate RIP information that it receives.</p> <p>When set to <b>None</b>, the ZyWALL will not send any RIP packets and will ignore any RIP packets received.</p> <p>By default, <b>RIP Direction</b> is set to <b>Both</b>.</p>
RIP Version	<p>The <b>RIP Version</b> field controls the format and the broadcasting method of the RIP packets that the ZyWALL sends (it recognizes both formats when receiving).</p> <p>Choose <b>RIP-1</b>, <b>RIP-2B</b> or <b>RIP-2M</b>.</p> <p><b>RIP-1</b> is universally supported; but <b>RIP-2</b> carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both <b>RIP-2B</b> and <b>RIP-2M</b> sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, the <b>RIP Version</b> field is set to <b>RIP-1</b>.</p>
Enable Multicast	<p>Select this check box to turn on IGMP (Internet Group Multicast Protocol). IGMP is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data.</p>
Multicast Version	<p>Choose <b>None</b> (default), <b>IGMP-V1</b> or <b>IGMP-V2</b>. IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group – it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236.</p>
Spoof WAN MAC Address	<p>You can use the factory assigned default MAC Address or cloning the MAC address from a computer on your LAN.</p> <p>Otherwise, select the check box next to <b>Spoof WAN MAC Address</b> and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different ROM file.</p>
Clone the computer's MAC address – IP Address	<p>Enter the IP address of the computer on the LAN whose MAC you are cloning. It is recommended that you clone the MAC address prior to hooking up the WAN port.</p>
Apply	<p>Click <b>Apply</b> to save your changes back to the ZyWALL.</p>
Reset	<p>Click <b>Reset</b> to begin configuring this screen afresh.</p>

## 7.13 Traffic Redirect

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

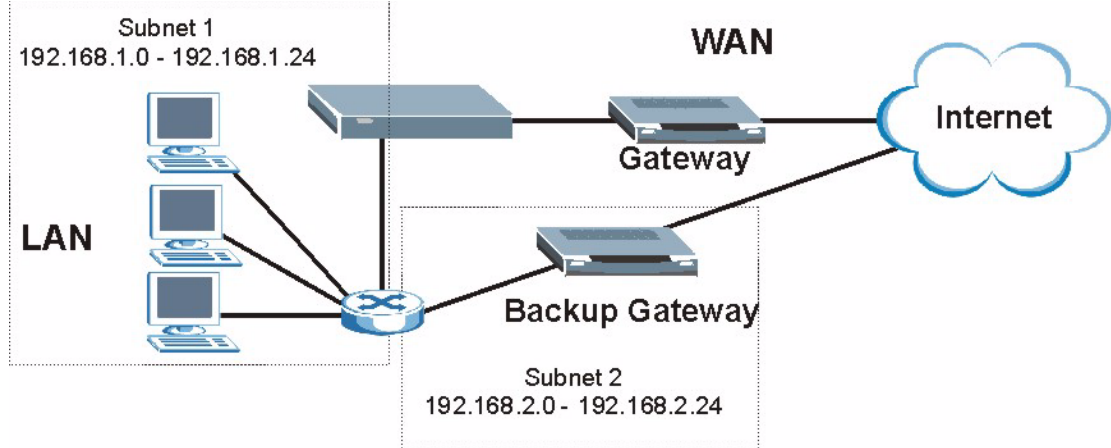
**Figure 58** Traffic Redirect WAN Setup



The following network topology allows you to avoid triangle route security issues (see [Appendix I on page 722](#)) when the backup gateway is connected to the LAN or DMZ. Use IP alias to configure the LAN into two or three logical networks with the ZyWALL itself as the gateway for each LAN network. Put the protected LAN in one subnet (Subnet 1 in the following figure) and the backup gateway in another subnet (Subnet 2). Configure a LAN to LAN/ZyWALL firewall rule that forwards packets from the protected LAN (Subnet 1) to the backup gateway (Subnet 2).

The following network topology allows you to avoid triangle route security issues (see [Appendix I on page 722](#)) when the backup gateway is connected to the LAN or DMZ. Use IP alias to configure the LAN into two or three logical networks with the ZyWALL itself as the gateway for each LAN network. Put the protected LAN in one subnet (Subnet 1 in the following figure) and the backup gateway in another subnet (Subnet 2). Configure a LAN to LAN/ZyWALL firewall rule that forwards packets from the protected LAN (Subnet 1) to the backup gateway (Subnet 2).

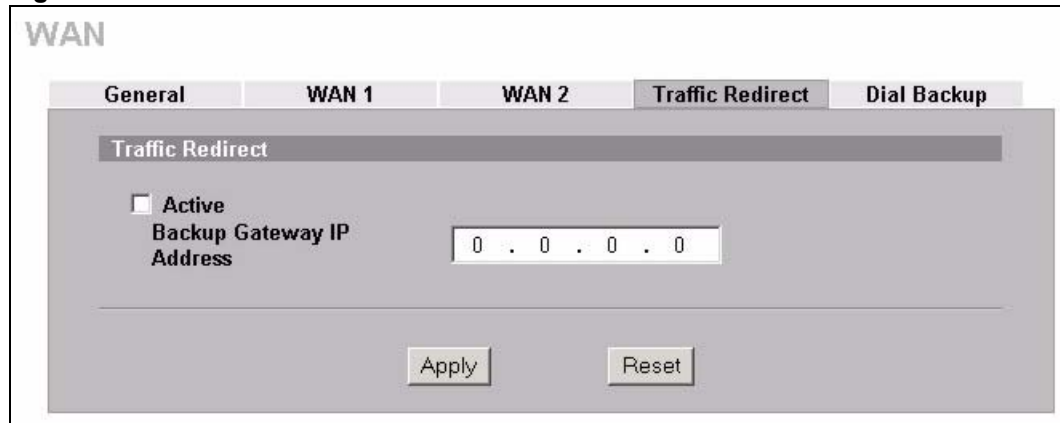
**Figure 59** Traffic Redirect LAN Setup



## 7.14 Configuring Traffic Redirect

To change your ZyWALL's traffic redirect settings, click **NETWORK**, **WAN** and then the **Traffic Redirect** tab. The screen appears as shown. Not all fields are available on all models.

**Figure 60** Traffic Redirect



The following table describes the labels in this screen.

**Table 42** Traffic Redirect

LABEL	DESCRIPTION
Active	Select this check box to have the ZyWALL use traffic redirect if the normal WAN connection goes down.
Backup Gateway IP Address	Type the IP address of your backup gateway in dotted decimal notation. The ZyWALL automatically forwards traffic to this IP address if the ZyWALL's Internet connection terminates.
Check WAN IP Address	Configuration of this field is optional. If you do not enter an IP address here, the ZyWALL will use the default gateway IP address. Configure this field to test your ZyWALL's WAN accessibility. Type the IP address of a reliable nearby computer (for example, your ISP's DNS server address).

**Table 42** Traffic Redirect (continued)

<b>LABEL</b>	<b>DESCRIPTION</b>
Fail Tolerance	Type how many WAN connection checks can fail (1 to 10) before the connection is considered "down" (not connected). The ZyWALL still checks a "down" connection to detect if it reconnects.
Period	The ZyWALL tests a WAN connection by periodically sending a ping to either the default gateway or the address in the <b>Check WAN IP Address</b> field. Type a number of seconds (5 to 300) to set the time interval between checks. Allow more time if your destination IP address handles lots of traffic.
Timeout	Type the number of seconds (1 to 10) for your ZyWALL to wait for a response to the ping before considering the check to have failed. This setting must be less than the <b>Period</b> . Use a higher value in this field if your network is busy or congested.
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 7.15 Configuring Dial Backup

Click **NETWORK**, **WAN** and then the **Dial Backup** tab to display the **Dial Backup** screen. Use this screen to configure the backup WAN dial-up connection.

Figure 61 Dial Backup

**WAN**

General    **WAN 1**    WAN 2    Traffic Redirect    **Dial Backup**

---

**Dial Backup Setup**

Enable Dial Backup

---

**Basic Settings**

Login Name:

Password:

Retype to Confirm:

Authentication Type:

Primary Phone Number:

Secondary Phone Number:  (Optional)

Dial Backup Port Speed:

AT Command Initial String:

Advanced Modem Setup:

---

**TCP/IP Options**

Get IP Address Automatically from Remote Server

Use Fixed IP Address

My WAN IP Address:

Remote IP Subnet Mask:

Remote Node IP Address:

Enable NAT (Network Address Translation)

Enable RIP

RIP Version:

RIP Direction:

Broadcast Dial Backup Route

Enable Multicast

Multicast Version:

---

**PPP Options**

PPP Encapsulation:

Enable Compression

---

**Budget**

Always On

Configure Budget

Allocated Budget:  (Minutes)

Period:  (Hours)

Idle Timeout:  (Seconds)

---



The following table describes the labels in this screen.

**Table 43** Dial Backup

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

**Table 43** Dial Backup (continued)

LABEL	DESCRIPTION
Enable RIP	Select this check box to turn on RIP (Routing Information Protocol), which allows a router to exchange routing information with other routers.
RIP Version	<p>The <b>RIP Version</b> field controls the format and the broadcasting method of the RIP packets that the ZyWALL sends (it recognizes both formats when receiving). Choose <b>RIP-1</b>, <b>RIP-2B</b> or <b>RIP-2M</b>.</p> <p><b>RIP-1</b> is universally supported; but <b>RIP-2</b> carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both <b>RIP-2B</b> and <b>RIP-2M</b> sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also.</p>
RIP Direction	<p>RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The <b>RIP Direction</b> field controls the sending and receiving of RIP packets.</p> <p>Choose <b>Both</b>, <b>In Only</b> or <b>Out Only</b>.</p> <p>When set to <b>Both</b> or <b>Out Only</b>, the ZyWALL will broadcast its routing table periodically.</p> <p>When set to <b>Both</b> or <b>In Only</b>, the ZyWALL will incorporate RIP information that it receives.</p>
Broadcast Dial Backup Route	Select this check box to forward the backup route broadcasts to the WAN.
Enable Multicast	Select this check box to turn on IGMP (Internet Group Multicast Protocol). IGMP is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data.
Multicast Version	Select <b>IGMP-v1</b> or <b>IGMP-v2</b> . 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 <i>sections 4 and 5 of RFC 2236</i> .
PPP Options	
PPP Encapsulation	Select <b>CISCO PPP</b> from the drop-down list box if your dial backup WAN device uses Cisco PPP encapsulation, otherwise select <b>Standard PPP</b> .
Enable Compression	Select this check box to turn on stac compression.
Budget	
Always On	Select this check box to have the dial backup connection on all of the time.
Configure Budget	Select this check box to have the dial backup connection on during the time that you select.
Allocated Budget	Type the amount of time (in minutes) that the dial backup connection can be used during the time configured in the <b>Period</b> field. Set an amount that is less than the time period configured in the <b>Period</b> field.
Period	Type the time period (in hours) for how often the budget should be reset. For example, to allow calls to this remote node for a maximum of 10 minutes every hour, set the <b>Allocated Budget</b> to 10 (minutes) and the <b>Period</b> to 1 (hour).
Idle Timeout	Type the number of seconds of idle time (when there is no traffic from the ZyWALL to the remote node) for the ZyWALL to wait before it automatically disconnects the dial backup connection. This option applies only when the ZyWALL initiates the call. The dial backup connection never times out if you set this field to "0" (it is the same as selecting <b>Always On</b> ).

**Table 43** Dial Backup (continued)

LABEL	DESCRIPTION
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 7.16 Advanced Modem Setup

### 7.16.1 AT Command Strings

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

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

### 7.16.2 DTR Signal

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

### 7.16.3 Response Strings

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

## 7.17 Configuring Advanced Modem Setup

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

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

**Figure 62** Advanced Setup

**WAN - ADVANCED MODEM SETUP**

**AT Command Strings**

Dial

Drop

Answer

Drop DTR When Hang Up

**AT Response Strings**

CLID

Called ID

Speed

**Call Control**

Dial Timeout (sec)

Retry Count

Retry Interval (sec)

Drop Timeout (sec)

Call Back Delay (sec)

The following table describes the labels in this screen.

**Table 44** Advanced Setup

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

**Table 44** Advanced Setup (continued)

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

# CHAPTER 8

## DMZ Screens

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

### 8.1 DMZ

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

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

It is highly recommended that you connect all of your public servers to the DMZ port(s).

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

### 8.2 Configuring DMZ

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

When the DMZ uses public IP addresses, the WAN and DMZ ports must use public IP addresses that are on separate subnets. See [Appendix E on page 694](#) for information on IP subnetting. If you do not configure SUA NAT or any full feature NAT mapping rules for the public IP addresses on the DMZ, the ZyWALL will route traffic to the public IP addresses on the DMZ without performing NAT. This may be useful for hosting servers for NAT unfriendly applications (see [Chapter 22 on page 374](#) for more information).

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

Like the LAN, the ZyWALL can also assign TCP/IP configuration via DHCP to computers connected to the DMZ ports.

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

**Figure 63** DMZ

The screenshot shows the DMZ configuration interface. At the top, there are four tabs: DMZ, Static DHCP, IP Alias, and Port Roles. The DMZ tab is selected. Below the tabs, there are three main sections:

- DMZ TCP/IP:** Contains fields for IP Address (172 . 25 . 10 . 1), IP Subnet Mask (255 . 255 . 0 . 0), Multicast (None), RIP Direction (Both), and RIP Version (RIP-1).
- DHCP Setup:** Contains a dropdown for DHCP (Server), IP Pool Starting Address (172 . 25 . 10 . 5), DHCP Server Address (0 . 0 . 0 . 0), and Pool Size (128).
- Windows Networking (NetBIOS over TCP/IP):** Contains three checkboxes: Allow between DMZ and LAN, Allow between DMZ and WAN, and Allow between DMZ and WLAN. A note below states: "Note: You also need to create a [Firewall](#) rule."

At the bottom of the screen, there are two buttons: Apply and Reset.

The following table describes the labels in this screen.

**Table 45** DMZ

LABEL	DESCRIPTION
DMZ TCP/IP	
IP Address	Type the IP address of your ZyWALL's DMZ port in dotted decimal notation.  <b>Note:</b> Make sure the IP addresses of the LAN, WAN, WLAN and DMZ are on separate subnets.
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your ZyWALL will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyWALL 255.255.255.0.
RIP Direction	RIP (Routing Information Protocol, RFC1058 and RFC 1389) allows a router to exchange routing information with other routers. The <b>RIP Direction</b> field controls the sending and receiving of RIP packets. Select the RIP direction from <b>Both/In Only/Out Only/None</b> . When set to <b>Both</b> or <b>Out Only</b> , the ZyWALL will broadcast its routing table periodically. When set to <b>Both</b> or <b>In Only</b> , it will incorporate the RIP information that it receives; when set to <b>None</b> , it will not send any RIP packets and will ignore any RIP packets received. <b>Both</b> is the default.

**Table 45** DMZ (continued)

LABEL	DESCRIPTION
RIP Version	The <b>RIP Version</b> field controls the format and the broadcasting method of the RIP packets that the ZyWALL sends (it recognizes both formats when receiving). <b>RIP-1</b> is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both <b>RIP-2B</b> and <b>RIP-2M</b> sends the routing data in RIP-2 format; the difference being that <b>RIP-2B</b> uses subnet broadcasting while <b>RIP-2M</b> uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to <b>Both</b> and the Version set to <b>RIP-1</b> .
Multicast	Select <b>IGMP V-1</b> or <b>IGMP V-2</b> or <b>None</b> . IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see <i>sections 4 and 5 of RFC 2236</i> .
DHCP Setup	
DHCP	DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (workstations) to obtain TCP/IP configuration at startup from a server. Unless you are instructed by your ISP, leave this field set to <b>Server</b> . When configured as a server, the ZyWALL provides TCP/IP configuration for the clients. When set as a server, fill in the <b>IP Pool Starting Address</b> and <b>Pool Size</b> fields.  Select <b>Relay</b> to have the ZyWALL forward DHCP requests to another DHCP server. When set to <b>Relay</b> , fill in the <b>DHCP Server Address</b> field.  Select <b>None</b> to stop the ZyWALL from acting as a DHCP server. When you select <b>None</b> , you must have another DHCP server on your LAN, or else the computers must be manually configured.
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Pool Size	This field specifies the size, or count of the IP address pool.
DHCP Server Address	Type the IP address of the DHCP server to which you want the ZyWALL to relay DHCP requests. Use dotted decimal notation. Alternatively, click the right mouse button to copy and/or paste the IP address.
Windows Networking (NetBIOS over TCP/IP)	
Allow between DMZ and LAN	Select this check box to forward NetBIOS packets from the LAN to the DMZ and from the DMZ to the LAN. If your firewall is enabled with the default policy set to block DMZ to LAN traffic, you also need to enable the default DMZ to LAN firewall rule that forwards NetBIOS traffic.  Clear this check box to block all NetBIOS packets going from the LAN to the DMZ and from the DMZ to the LAN.
Allow between DMZ and WAN	Select this check box to forward NetBIOS packets from the WAN to the DMZ and from the DMZ to the WAN.  Clear this check box to block all NetBIOS packets going from the WAN to the DMZ and from the DMZ to the WAN.



**Table 45** DMZ (continued)

LABEL	DESCRIPTION
Allow between DMZ and WLAN	Select this check box to forward NetBIOS packets from the WLAN to the DMZ and from the DMZ to the WLAN. Clear this check box to block all NetBIOS packets going from the WLAN to the DMZ and from the DMZ to the WLAN.
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 8.3 DMZ Static DHCP

This table allows you to assign IP addresses on the DMZ to specific individual computers based on their MAC Addresses.

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

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

**Figure 64** DMZ Static DHCP

The screenshot shows the 'DMZ Static DHCP' configuration interface. At the top, there are tabs for 'DMZ', 'Static DHCP', 'IP Alias', and 'Port Roles'. The 'Static DHCP Table' is the main area, containing a table with 128 rows. The first 118 rows are partially obscured by a wavy line. Each row has a '#' column, a 'MAC Address' column (6 hex digits), and an 'IP Address' column (4 octets). Below the table are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

**Table 46** DMZ Static DHCP

LABEL	DESCRIPTION
#	This is the index number of the Static IP table entry (row).
MAC Address	Type the MAC address of a computer on your DMZ.
IP Address	Type the IP address that you want to assign to the computer on your DMZ. Alternatively, click the right mouse button to copy and/or paste the IP address.
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 8.4 DMZ IP Alias

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

The IP alias IP addresses can be either private or public regardless of whether the physical DMZ interface is set to use a private or public IP address. Use NAT if you want to make DMZ computers with private IP addresses publicly accessible (see [Chapter 22 on page 374](#) for more information). When you use IP alias, you can have the DMZ use both public and private IP addresses at the same time.

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

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

**Figure 65** DMZ: IP Alias

The following table describes the labels in this screen.

**Table 47** DMZ: IP Alias

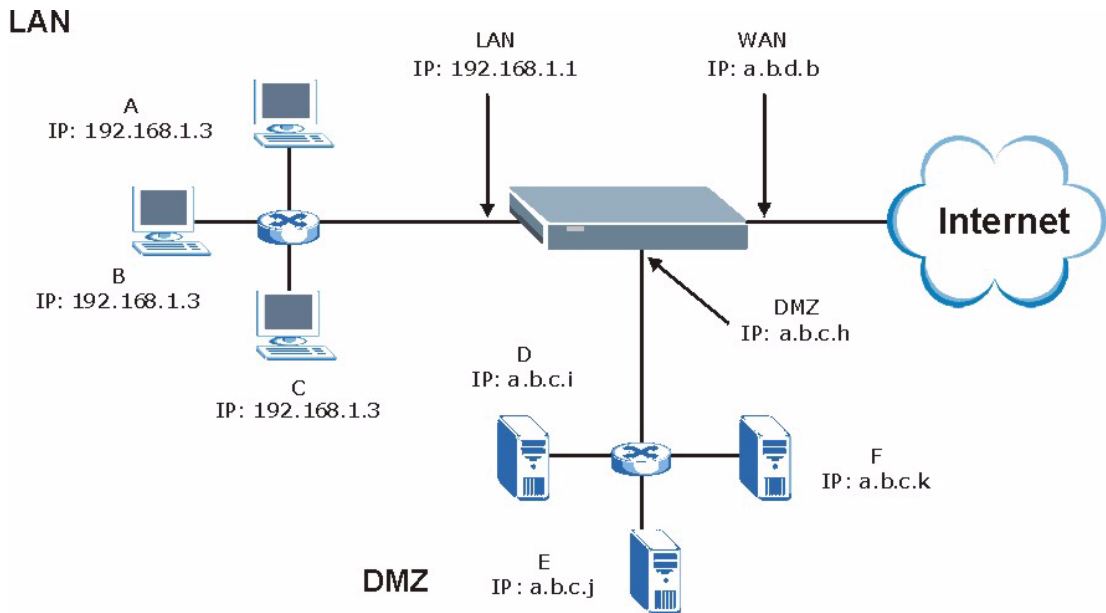
LABEL	DESCRIPTION
Enable IP Alias 1, 2	Select the check box to configure another DMZ network for the ZyWALL.
IP Address	Enter the IP address of your ZyWALL in dotted decimal notation.  <b>Note:</b> Make sure the IP addresses of the LAN, WAN, WLAN and DMZ are on separate subnets.

**Table 47** DMZ: IP Alias (continued)

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

## 8.5 DMZ Public IP Address Example

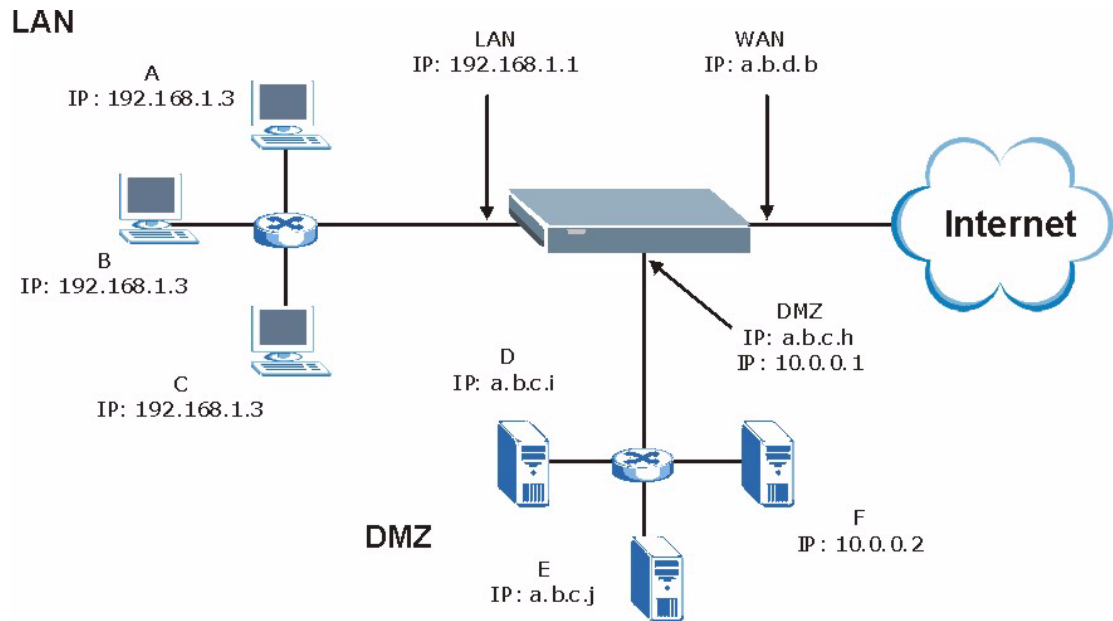
The following figure shows a simple network setup with public IP addresses on the WAN and DMZ and private IP addresses on the LAN. Lower case letters represent public IP addresses (like a.b.c.d for example). The LAN port and connected computers (A through C) use private IP addresses that are in one subnet.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

**Figure 66** DMZ Public Address Example

## 8.6 DMZ Private and Public IP Address Example

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

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

**Figure 67** DMZ Private and Public Address Example

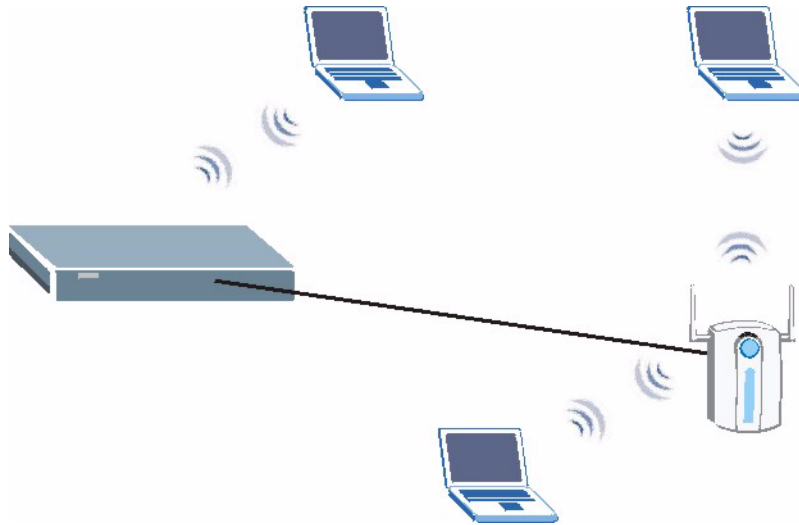
## 8.7 DMZ Port Roles

Use the **Port Roles** screen to set ports as LAN, DMZ or WLAN interfaces. The LAN port role is not available on all models.

Connect wireless LAN Access Points (APs) to WLAN interfaces to extend the ZyWALL's wireless LAN coverage. The WLAN port role allows the ZyWALL's firewall to treat traffic from connected APs as part of the ZyWALL's WLAN. You can specify firewall rules for traffic going to or from the WLAN. The WLAN includes the ZyWALL's own WLAN and the Ethernet ports in the WLAN port role.

The following figure shows the ZyWALL with a wireless card installed and an AP connected to an Ethernet port in the WLAN port role.

**Figure 68** WLAN Port Role Example



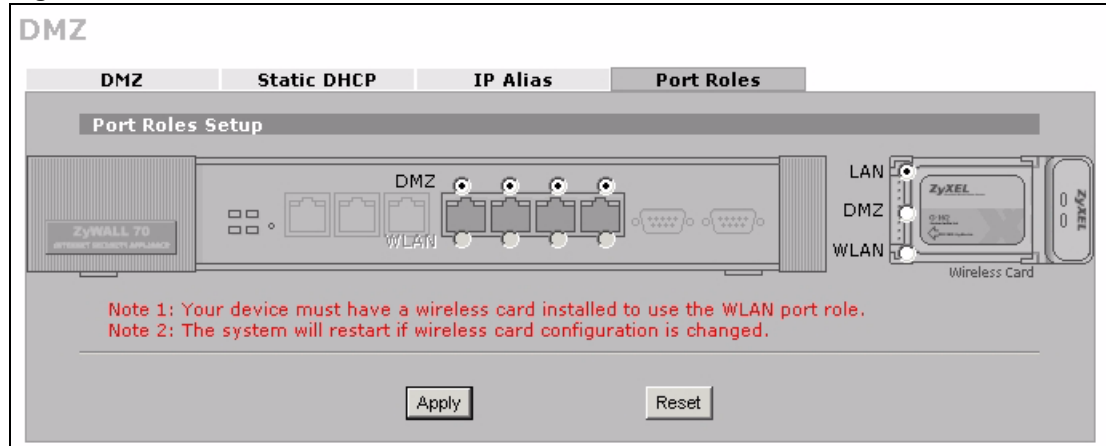
**Note:** Do the following if you are configuring from a computer connected to a LAN, DMZ or WLAN port and changing the port's role:

1. A port's IP address varies as its role changes, make sure your computer's IP address is in the same subnet as the ZyWALL's LAN, DMZ or WLAN IP address.
2. Use the appropriate LAN, DMZ or WLAN IP address to access the ZyWALL.

To change your ZyWALL's port role settings, click **NETWORK, DMZ** and then the **Port Roles** tab. The screen appears as shown.

The radio buttons on the left correspond to Ethernet ports on the front panel of the ZyWALL. Ports 1 to 4 are all DMZ ports on the ZyWALL 70 and all LAN ports on the ZyWALL 5 or ZyWALL 35 by default. The radio buttons on the right are for the WLAN card.

**Note:** Your changes are also reflected in the **LAN** and/or **WLAN Port Roles** screens.

**Figure 69** DMZ: Port Roles

The following table describes the labels in this screen.

**Table 48** DMZ: Port Roles

LABEL	DESCRIPTION
LAN	Select a port's LAN radio button to use the port as part of the LAN. The port will use the LAN IP address and MAC address.
DMZ	Select a port's DMZ radio button to use the port as part of the DMZ. The port will use the DMZ IP address and MAC address.
WLAN	When you have the wireless card set to <b>WLAN</b> , you can select a port's WLAN radio button to use the port as part of the WLAN. The port will use the ZyWALL's WLAN IP address and the MAC address of the WLAN card.  <b>Note:</b> You must install a wireless card to use the WLAN port role. See <a href="#">Appendix A on page 664</a> for how to install a WLAN card.
Wireless Card	Select <b>LAN</b> to use the wireless card as part of the LAN. Select <b>DMZ</b> to use the wireless card as part of the DMZ. Select <b>WLAN</b> to use the wireless card as part of the WLAN. The ZyWALL restarts after you change the wireless card setting.  <b>Note:</b> If you set the wireless card to be part of the LAN or DMZ, you can still use wireless access, but not the WLAN interface in the firewall. The firewall will treat the wireless card as part of the LAN or DMZ respectively.
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.





# CHAPTER 9

## Wireless LAN

This chapter discusses how to configure wireless LAN on the ZyWALL.

### 9.1 Wireless LAN Introduction

A wireless LAN can be as simple as two computers with wireless LAN adapters communicating in a peer-to-peer network or as complex as a number of computers with wireless LAN adapters communicating through access points which bridge network traffic to the wired LAN.

**Note:** See [Appendix A on page 664](#) for how to install a WLAN card.

See the WLAN appendix for more detailed information on WLANs.

#### 9.1.1 Additional Installation Requirements for Using 802.1x

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

### 9.2 Configuring WLAN

The WLAN interface uses the ZyWALL's WLAN IP address and the MAC address of the WLAN card. You need to insert a compatible wireless LAN card and enable the card in the **Wireless Card** screen (see [Figure 80 on page 191](#)) to have wireless functionality. You can also use the **Port Roles** screen to set a port to be part of the WLAN and connect an access point (AP) to the WLAN interface to extend the ZyWALL's wireless LAN coverage.

There is a WLAN interface in the firewall. You can specify firewall rules for traffic going to or from the WLAN.

Click **NETWORK**, **WLAN** to open the **WLAN** screen to configure the IP address for ZyWALL's WLAN interface, other TCP/IP and DHCP settings.

**Figure 70** WLAN

The screenshot shows the ZyWALL configuration interface for the WLAN section. At the top, there are four tabs: **WLAN**, **Static DHCP**, **IP Alias**, and **Port Roles**. The **WLAN** tab is selected. Below the tabs, there are three main sections:

- WLAN TCP/IP:** Contains fields for IP Address (10 . 12 . 5 . 1), IP Subnet Mask (255 . 255 . 255 . 0), Multicast (IGMP-v2), RIP Direction (None), and RIP Version (RIP-1).
- DHCP Setup:** Contains a DHCP dropdown menu (Server), IP Pool Starting Address (10 . 12 . 5 . 33), DHCP Server Address (0 . 0 . 0 . 0), and Pool Size (64).
- Windows Networking (NetBIOS over TCP/IP):** Contains three checkboxes:
  - Allow between WLAN and LAN
  - Allow between WLAN and WAN
  - Allow between WLAN and DMZ
 A note below states: "Note: You also need to create a [Firewall](#) rule."

At the bottom of the configuration area, there are two buttons: **Apply** and **Reset**.

The following table describes the labels in this screen.

**Table 49** WLAN

LABEL	DESCRIPTION
WLAN TCP/IP	
IP Address	Type the IP address of your ZyWALL's WLAN interface in dotted decimal notation. Alternatively, click the right mouse button to copy and/or paste the IP address.  <b>Note:</b> Make sure the IP addresses of the LAN, WAN, WLAN and DMZ are on separate subnets.
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your ZyWALL automatically calculates the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyWALL.
RIP Direction	RIP (Routing Information Protocol, RFC1058 and RFC 1389) allows a router to exchange routing information with other routers. The <b>RIP Direction</b> field controls the sending and receiving of RIP packets. Select the RIP direction from <b>Both/In Only/Out Only/None</b> . When set to <b>Both</b> or <b>Out Only</b> , the ZyWALL will broadcast its routing table periodically. When set to <b>Both</b> or <b>In Only</b> , it will incorporate the RIP information that it receives; when set to <b>None</b> , it will not send any RIP packets and will ignore any RIP packets received. <b>Both</b> is the default.

**Table 49** WLAN (continued)

LABEL	DESCRIPTION
RIP Version	The <b>RIP Version</b> field controls the format and the broadcasting method of the RIP packets that the ZyWALL sends (it recognizes both formats when receiving). <b>RIP-1</b> is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both <b>RIP-2B</b> and <b>RIP-2M</b> sends the routing data in RIP-2 format; the difference being that <b>RIP-2B</b> uses subnet broadcasting while <b>RIP-2M</b> uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to <b>Both</b> and the Version set to <b>RIP-1</b> .
Multicast	Select <b>IGMP V-1</b> or <b>IGMP V-2</b> or <b>None</b> . IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see <i>sections 4 and 5 of RFC 2236</i> .
DHCP Setup	
DHCP	DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (workstations) to obtain TCP/IP configuration at startup from a server. Unless you are instructed by your ISP, leave this field set to <b>Server</b> . When configured as a server, the ZyWALL provides TCP/IP configuration for the clients. When set as a server, fill in the <b>IP Pool Starting Address</b> and <b>Pool Size</b> fields.  Select <b>Relay</b> to have the ZyWALL forward DHCP requests to another DHCP server. When set to <b>Relay</b> , fill in the <b>DHCP Server Address</b> field.  Select <b>None</b> to stop the ZyWALL from acting as a DHCP server. When you select <b>None</b> , you must have another DHCP server on your LAN, or else the computers must be manually configured.
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Pool Size	This field specifies the size, or count of the IP address pool.
DHCP Server Address	Type the IP address of the DHCP server to which you want the ZyWALL to relay DHCP requests. Use dotted decimal notation. Alternatively, click the right mouse button to copy and/or paste the IP address.
Windows Networking (NetBIOS over TCP/IP)	NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls. However it may sometimes be necessary to allow NetBIOS packets to pass through to the WAN in order to find a computer on the WAN.
Allow between WLAN and LAN	Select this check box to forward NetBIOS packets from the LAN to the WLAN and from the WLAN to the LAN. If your firewall is enabled with the default policy set to block WLAN to LAN traffic, you also need to enable the default WLAN to LAN firewall rule that forwards NetBIOS traffic. Clear this check box to block all NetBIOS packets going from the LAN to the WLAN and from the WLAN to the LAN.
Allow between WLAN and WAN	Select this check box to forward NetBIOS packets from the WLAN to the WAN and from the WAN to the WLAN. Clear this check box to block all NetBIOS packets going from the WLAN to the WAN and from the WAN to the WLAN.

**Table 49** WLAN (continued)

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

## 9.3 WLAN Static DHCP

This table allows you to assign IP addresses on the WLAN to specific individual computers based on their MAC addresses.

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

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

**Figure 71** WLAN Static DHCP

The screenshot shows the 'WLAN Static DHCP' configuration page. At the top, there are four tabs: 'WLAN', 'Static DHCP', 'IP Alias', and 'Port Roles'. The 'Static DHCP' tab is selected. Below the tabs is a 'Static DHCP Table' header. The table has three main columns: '#', 'MAC Address', and 'IP Address'. The 'MAC Address' column is divided into six sub-columns, and the 'IP Address' column is divided into four sub-columns. The table contains 128 rows, numbered 1 to 128. The first 10 rows are visible, and a wavy line indicates that rows 11 through 119 are hidden. Each row has input fields for the MAC address and IP address, with the IP address field pre-filled with '0 . 0 . 0 . 0'. Below the table are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

**Table 50** WLAN Static DHCP

LABEL	DESCRIPTION
#	This is the index number of the Static IP table entry (row).
MAC Address	Type the MAC address of a computer on your WLAN.
IP Address	Type the IP address that you want to assign to the computer on your WLAN. Alternatively, click the right mouse button to copy and/or paste the IP address.
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 9.4 WLAN IP Alias

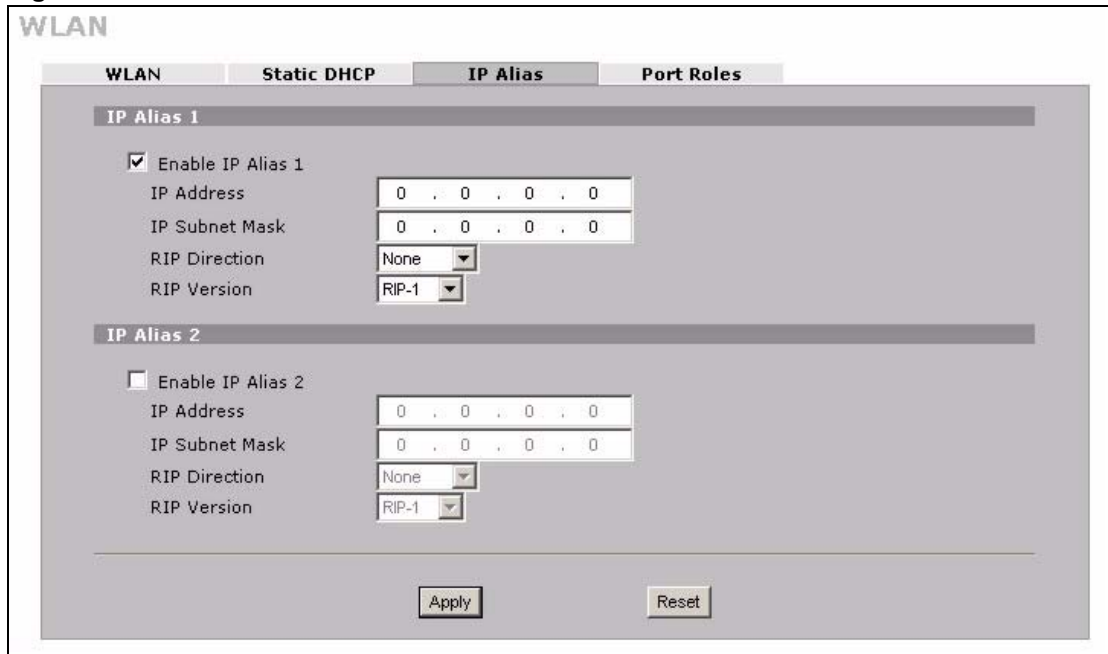
IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The ZyWALL supports three logical WLAN interfaces via its single physical Ethernet interface with the ZyWALL itself as the gateway for each WLAN network.

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

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

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

**Figure 72** WLAN IP Alias



The following table describes the labels in this screen.

**Table 51** WLAN IP Alias

LABEL	DESCRIPTION
Enable IP Alias 1, 2	Select the check box to configure another WLAN network for the ZyWALL.
IP Address	Enter the IP address of your ZyWALL in dotted decimal notation. Alternatively, click the right mouse button to copy and/or paste the IP address.
IP Subnet Mask	Your ZyWALL will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyWALL.
RIP Direction	RIP (Routing Information Protocol, RFC 1058 and RFC 1389) allows a router to exchange routing information with other routers. The <b>RIP Direction</b> field controls the sending and receiving of RIP packets. Select the RIP direction from <b>Both/In Only/Out Only/None</b> . When set to <b>Both</b> or <b>Out Only</b> , the ZyWALL will broadcast its routing table periodically. When set to <b>Both</b> or <b>In Only</b> , it will incorporate the RIP information that it receives; when set to <b>None</b> , it will not send any RIP packets and will ignore any RIP packets received.

**Table 51** WLAN IP Alias

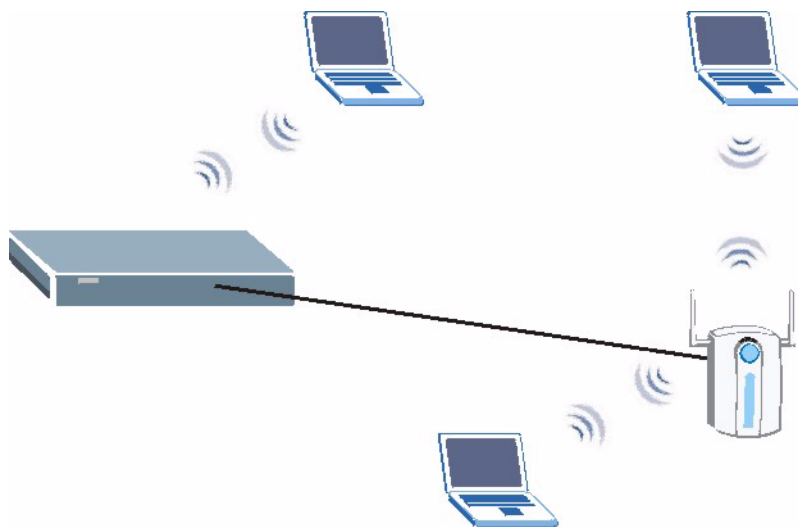
LABEL	DESCRIPTION
RIP Version	The <b>RIP Version</b> field controls the format and the broadcasting method of the RIP packets that the ZyWALL sends (it recognizes both formats when receiving). <b>RIP-1</b> is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most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

## 9.5 WLAN Port Roles

Use the **Port Roles** screen to set ports as LAN, DMZ or WLAN interfaces. The LAN port role is not available on all models.

Connect wireless LAN Access Points (APs) to WLAN interfaces to extend the ZyWALL's wireless LAN coverage. The WLAN port role allows the ZyWALL's firewall to treat traffic from connected APs as part of the ZyWALL's WLAN. You can specify firewall rules for traffic going to or from the WLAN. The WLAN includes the ZyWALL's own WLAN and the Ethernet ports in the WLAN port role.

The following figure shows the ZyWALL with a wireless card installed and an AP connected to an Ethernet port in the WLAN port role.

**Figure 73** WLAN Port Role Example



**Note:** Do the following if you are configuring from a computer connected to a LAN, DMZ or WLAN port and changing the port's role:

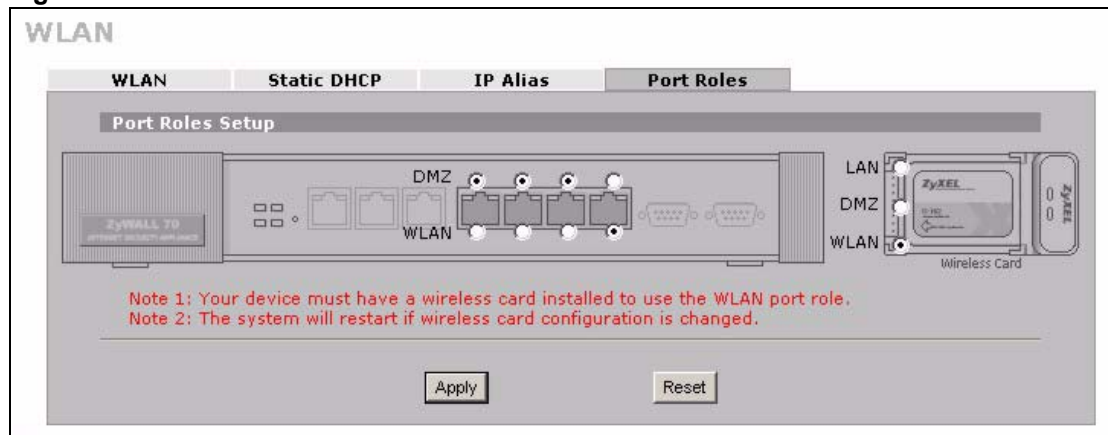
1. A port's IP address varies as its role changes, make sure your computer's IP address is in the same subnet as the ZyWALL's LAN, DMZ or WLAN IP address.
2. Use the appropriate LAN, DMZ or WLAN IP address to access the ZyWALL.

To change your ZyWALL's port role settings, click **NETWORK**, **WLAN** and then the **Port Roles** tab. The screen appears as shown.

The radio buttons on the left correspond to Ethernet ports on the front panel of the ZyWALL. Ports 1 to 4 are all DMZ ports on the ZyWALL 70 and all LAN ports on the ZyWALL 5 or ZyWALL 35 by default. The radio buttons on the right are for the WLAN card.

**Note:** Your changes are also reflected in the **LAN** and/or **DMZ Port Roles** screen.

**Figure 74** WLAN Port Roles



The following table describes the labels in this screen.

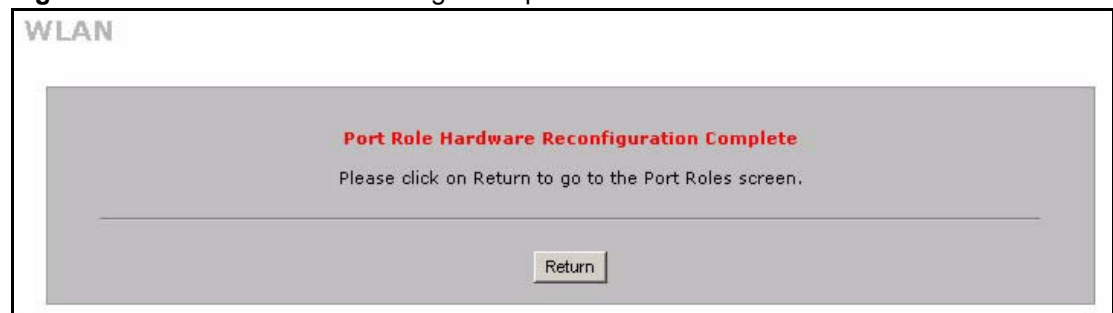
**Table 52** WLAN Port Roles

LABEL	DESCRIPTION
LAN	Select a port's LAN radio button to use the port as part of the LAN. The port will use the LAN IP address and MAC address.
DMZ	Select a port's DMZ radio button to use the port as part of the DMZ. The port will use the DMZ IP address and MAC address.
WLAN	When you have the wireless card set to <b>WLAN</b> , you can select a port's WLAN radio button to use the port as part of the WLAN. The port will use the ZyWALL's WLAN IP address and the MAC address of the WLAN card.  <b>Note:</b> You must install a wireless card to use the WLAN port role. See <a href="#">Appendix A on page 664</a> for how to install a WLAN card.

**Table 52** WLAN Port Roles (continued)

LABEL	DESCRIPTION
Wireless Card	Select <b>LAN</b> to use the wireless card as part of the LAN. Select <b>DMZ</b> to use the wireless card as part of the DMZ. Select <b>WLAN</b> to use the wireless card as part of the WLAN. The ZyWALL restarts after you change the wireless card setting.  <b>Note:</b> If you set the wireless card to be part of the LAN or DMZ, you can still use wireless access, but not the WLAN interface in the firewall. The firewall will treat the wireless card as part of the LAN or DMZ respectively.
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

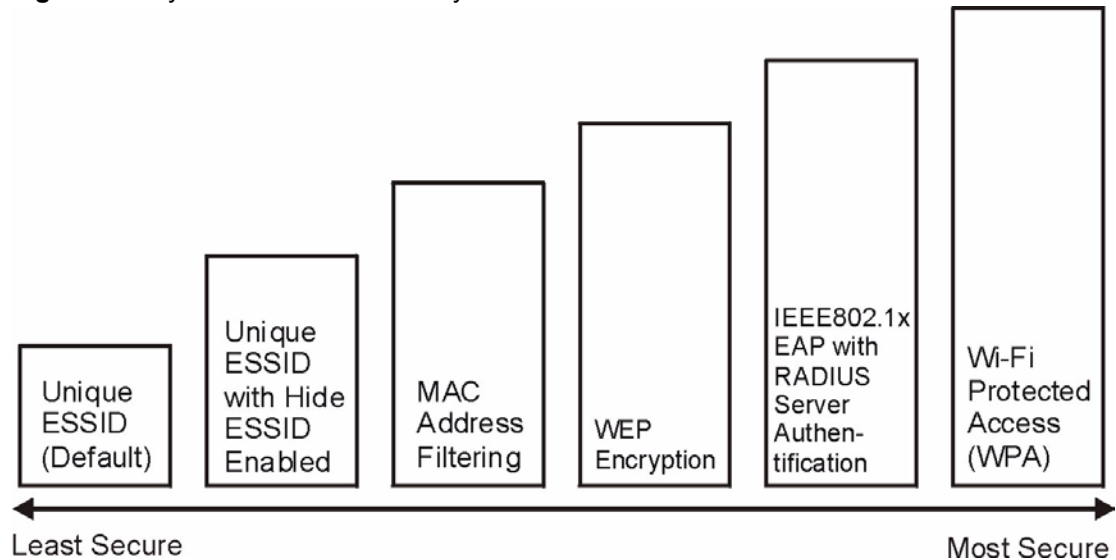
After you change the LAN/DMZ/WLAN port roles and click **Apply**, please wait for few seconds until the following screen appears. Click **Return** to go back to the **Port Roles** screen.

**Figure 75** WLAN Port Roles Change Complete

## 9.6 Wireless Security

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

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

**Figure 76** ZyWALL Wireless Security Levels

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

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

## 9.6.1 Encryption

- Use WPA security if you have WPA-aware wireless clients and a RADIUS server. WPA has user authentication and improved data encryption over WEP.
- Use WPA-PSK if you have WPA-aware wireless clients but no RADIUS server.
- If you don't have WPA-aware wireless clients, then use WEP key encrypting. A higher bit key offers better security at a throughput trade-off. You can use Passphrase to automatically generate 64-bit or 128-bit WEP keys or manually enter 64-bit, 128-bit or 256-bit WEP keys.

## 9.6.2 Authentication

Use a RADIUS server with WPA or IEEE 802.1x key management protocol. You can also configure IEEE 802.1x to use the built-in database (Local User Database) to authenticate wireless clients before joining your network.

- Use RADIUS authentication if you have a RADIUS server. See the appendices for information on protocols used when a client authenticates with a RADIUS server via the ZyWALL.
- Use the Local User Database if you have less than 32 wireless clients in your network. The ZyWALL uses MD5 encryption when a client authenticates with the Local User Database.

### 9.6.3 Restricted Access

The **MAC Filter** screen allows you to configure the AP to give exclusive access to devices (**Allow Association**) or exclude them from accessing the AP (**Deny Association**).

### 9.6.4 Hide ZyWALL Identity

If you hide the ESSID, then the ZyWALL cannot be seen when a wireless client scans for local APs. The trade-off for the extra security of “hiding” the ZyWALL may be inconvenience for some valid WLAN clients.

## 9.7 Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each authentication method/ key management protocol type. You enter manual keys when using WEP encryption or WPA-PSK. MAC address filters are not dependent on how you configure these security features.

**Table 53** Wireless Security Relational Matrix

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

## 9.8 WEP Encryption

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

## 9.9 802.1x Overview

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

### 9.9.1 Introduction to RADIUS

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

- **Authentication**  
Determines the identity of the users.
- **Accounting**  
Keeps track of the client's network activity.

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

#### 9.9.1.1 Types of RADIUS Messages

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

- **Access-Request**  
Sent by an access point requesting authentication.
- **Access-Reject**  
Sent by a RADIUS server rejecting access.
- **Access-Accept**  
Sent by a RADIUS server allowing access.
- **Access-Challenge**  
Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

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

- **Accounting-Request**  
Sent by the access point requesting accounting.
- **Accounting-Response**

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

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

## 9.9.2 EAP Authentication Overview

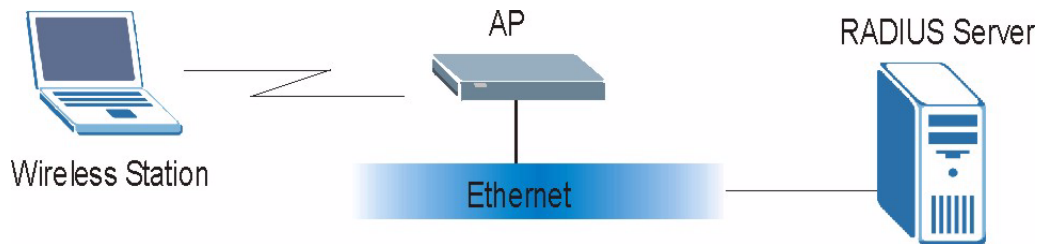
EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, the access point helps a wireless station and a RADIUS server perform authentication.

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

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

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

**Figure 77** EAP Authentication



The details below provide a general description of how IEEE 802.1x EAP authentication works.

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

## 9.10 Dynamic WEP Key Exchange

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

If this feature is enabled, it is not necessary to configure a default encryption key in the **Wireless Card** screen (see [Section 9.16.4 on page 196](#)). You may still configure and store keys here, but they will not be used while dynamic WEP is enabled.

To use dynamic WEP, enable and configure dynamic WEP key exchange in the **Wireless Card** screen and configure RADIUS server settings in the **AUTH SERVER RADIUS** screen (see [Section 21.3 on page 372](#)). Ensure that the wireless station's EAP type is configured to one of the following:

- EAP-TLS
- EAP-TTLS
- PEAP

**Note:** EAP-MD5 cannot be used with dynamic WEP key exchange.

## 9.11 Introduction to WPA

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

### 9.11.1 User Authentication

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

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

### 9.11.2 Encryption

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

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

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

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

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

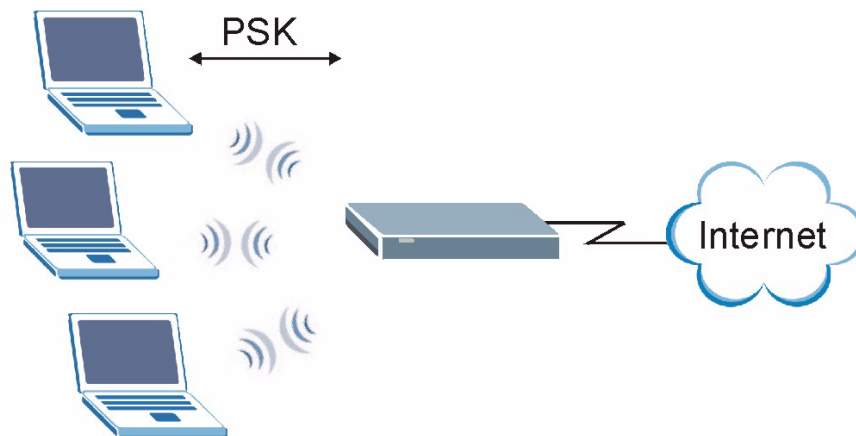
The encryption mechanisms used for WPA and WPA-PSK are the same. The only difference between the two is that WPA-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA-PSK susceptible to brute-force password-guessing attacks but it's still an improvement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

## 9.12 WPA-PSK Application Example

A WPA-PSK application looks as follows.

- 1** First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters (including spaces and symbols).
- 2** The AP checks each client's password and (only) allows it to join the network if it matches its password.
- 3** The AP derives and distributes keys to the wireless clients.
- 4** The AP and wireless clients use the TKIP encryption process to encrypt data exchanged between them.



**Figure 78** WPA-PSK Authentication

## 9.13 Introduction to RADIUS

The ZyWALL can use an external RADIUS server to authenticate an unlimited number of users. RADIUS is based on a client-server model that supports authentication and accounting, where access point is the client and the server is the RADIUS server.

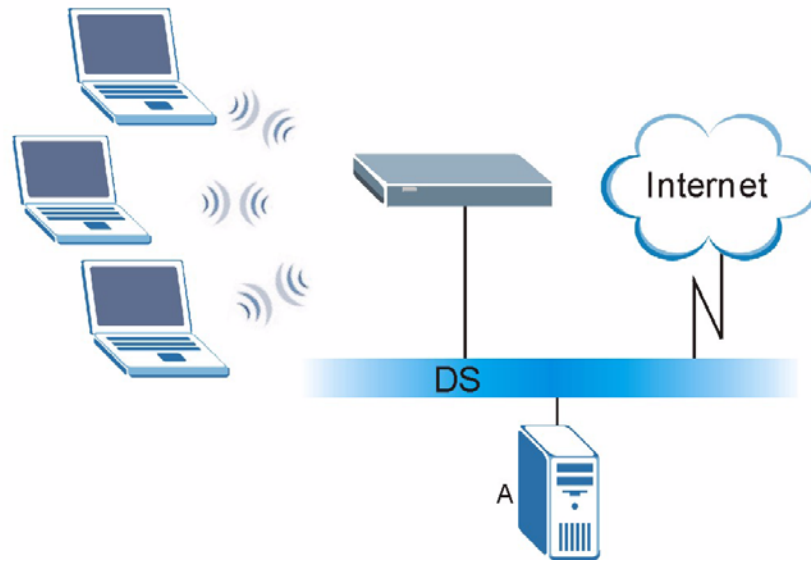
- Authentication
  - Determines the identity of the users.
- Accounting
  - Keeps track of the client's network activity.

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

## 9.14 WPA with RADIUS Application Example

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

- 1** The AP passes the wireless client's authentication request to the RADIUS server.
- 2** The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
- 3** The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

**Figure 79** WPA with RADIUS Application Example

## 9.15 Wireless Client WPA Supplicants

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

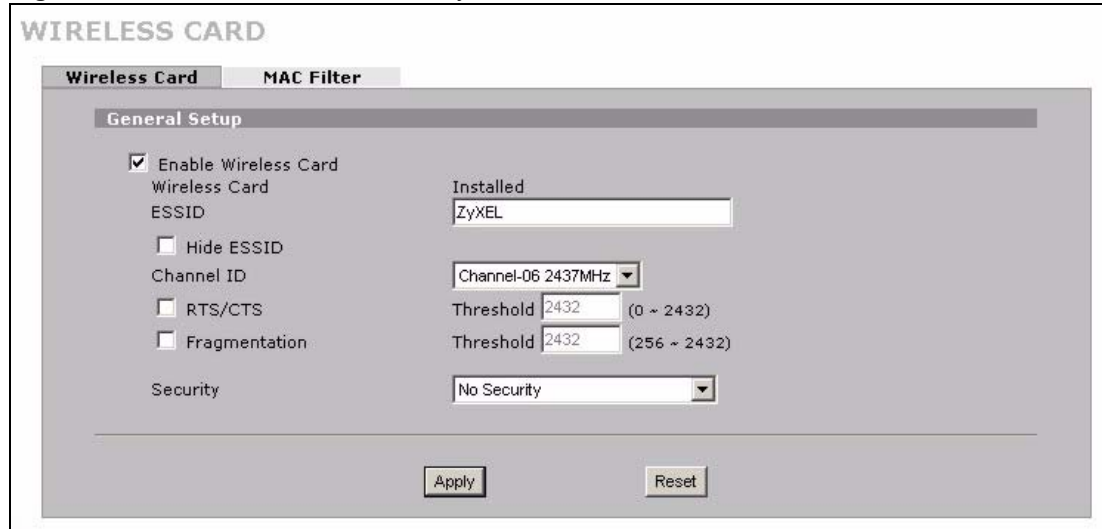
The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

## 9.16 Wireless Card

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

Click **NETWORK** and **WIRELESS CARD** to open the **Wireless Card** screen. The screen varies according to the security features you select.

**Figure 80** Wireless Card: No Security



The following table describes the labels in this screen.

**Table 54** Wireless Card: No Security

LABEL	DESCRIPTION
Enable Wireless Card	The wireless LAN is turned off by default, before you enable the wireless LAN you should configure some security by setting MAC filters and/or 802.1x security; otherwise your wireless LAN will be vulnerable upon enabling it. Select the check box to enable the wireless LAN.
Wireless Card	This field displays whether or not a compatible ZyXEL wireless LAN card is installed. You can only use the wireless LAN feature if a compatible ZyXEL wireless LAN card is installed.  <b>Note:</b> Turn the ZyWALL off before you install or remove the wireless LAN card. See the product specifications appendix for a table of compatible ZyXEL WLAN cards (and the WLAN security features each card supports) and how to install a WLAN card.
ESSID	(Extended Service Set IDentity) The ESSID identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same ESSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN.
Hide ESSID	Select to hide the ESSID in the outgoing beacon frame so a station cannot obtain the ESSID through scanning.
Channel ID	This allows you to set the operating frequency/channel depending on your particular region. Select a channel from the drop-down list box.
RTS/CTS Threshold	The RTS (Request To Send) threshold (number of bytes) is for enabling RTS/CTS. Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this value to be larger than the maximum MSDU (MAC service data unit) size turns off RTS/CTS. Setting this value to zero turns on RTS/CTS.  Select the check box to change the default value and enter a new value between <b>0</b> and <b>2432</b> .

**Table 54** Wireless Card: No Security (continued)

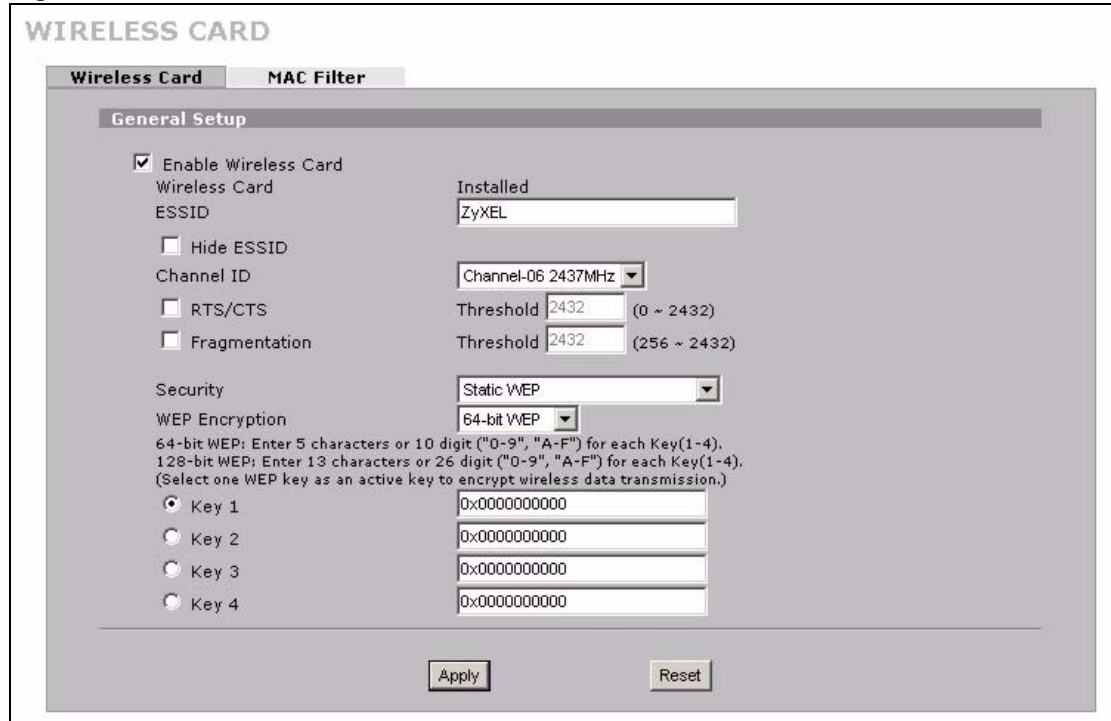
LABEL	DESCRIPTION
Fragmentation Threshold	<p>This is the threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent.</p> <p>Select the check box to change the default value and enter a value between <b>256</b> and <b>2432</b>.</p>
Security	<p>Choose from one of the security settings listed in the drop-down box.</p> <ul style="list-style-type: none"> <li>• No Security</li> <li>• Static WEP</li> <li>• WPA-PSK</li> <li>• WPA</li> <li>• 802.1x + Dynamic WEP</li> <li>• 802.1x + Static WEP</li> <li>• 802.1x + No WEP</li> <li>• No Access 802.1x + Static WEP</li> <li>• No Access 802.1x + No WEP</li> </ul> <p>Select <b>No Security</b> to allow wireless stations to communicate with the access points without any data encryption. Otherwise, select the security you need and see the following sections for more information.</p> <p><b>Note:</b> The installed ZyXEL WLAN card may not support all of the WLAN security features you can configure in the ZyWALL.</p> <p>Please see the product specifications appendix for a table of compatible ZyXEL WLAN cards and the WLAN security features each card supports.</p>
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

### 9.16.1 Static WEP

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

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

**Figure 81** Wireless Card: Static WEP



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

**Table 55** Wireless Card: Static WEP

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

### 9.16.2 WPA-PSK

Click the **NETWORK** and **WIRELESS CARD** to display the **Wireless Card** screen. Select **WPA-PSK** from the **Security** list.

**Figure 82** Wireless Card: WPA-PSK

**WIRELESS CARD**

**Wireless Card** | **MAC Filter**

**General Setup**

Enable Wireless Card  
Wireless Card: Installed

ESSID: ZyXEL

Hide ESSID

Channel ID: Channel-06 2437MHz

RTS/CTS

Fragmentation

Security: WPA-PSK

Pre-Shared Key: qwer1234

ReAuthentication Timer: 1800 (Seconds)

Idle Timeout: 3600 (Seconds)

WPA Group Key Update Timer: 1800 (Seconds)

Threshold: 2432 (0 ~ 2432)

Threshold: 2432 (256 ~ 2432)

Apply | Reset

The following wireless LAN security fields become available when you select **WPA-PSK** in the **Security** drop down list-box.

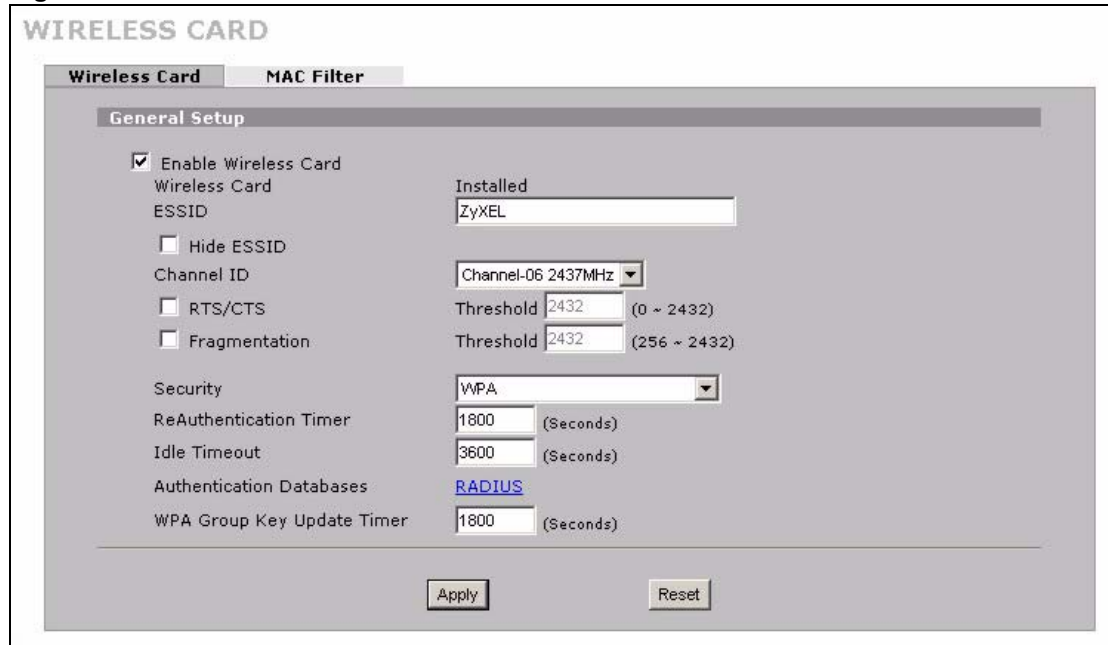
**Table 56** Wireless Card: WPA-PSK

LABEL	DESCRIPTION
Security	Select <b>WPA-PSK</b> from the drop-down list.
Pre-Shared Key	The encryption mechanisms used for <b>WPA</b> and <b>WPA-PSK</b> are the same. The only difference between the two is that <b>WPA-PSK</b> uses a simple common password, instead of user-specific credentials. Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).
ReAuthentication Timer (Seconds)	Specify how often wireless stations have to resend user names and passwords in order to stay connected. Enter a time interval between 10 and 65535 seconds. If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout (Seconds)	The ZyWALL automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the user name and password again before access to the wired network is allowed.
WPA Group Key Update Timer (Seconds)	The <b>WPA Group Key Update Timer</b> is the rate at which the AP (if using <b>WPA-PSK</b> key management) or RADIUS server (if using <b>WPA</b> key management) sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the <b>WPA Group Key Update Timer</b> is also supported in <b>WPA-PSK</b> mode.
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

### 9.16.3 WPA

Click the **NETWORK** and **WIRELESS CARD** to display the **Wireless Card** screen. Select **WPA** from the **Security** list.

**Figure 83** Wireless Card: WPA



The following wireless LAN security fields become available when you select **WPA** in the **Security** drop down list-box.

**Table 57** Wireless Card: WPA

LABEL	DESCRIPTION
Security	Select <b>WPA</b> from the drop-down list.
ReAuthentication Timer (Seconds)	Specify how often wireless stations have to resend user names and passwords in order to stay connected. Enter a time interval between 10 and 65535 seconds. If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout (Seconds)	The ZyWALL automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the user name and password again before access to the wired network is allowed.
Authentication Databases	Click <b>RADIUS</b> to go to the <b>RADIUS</b> screen where you can configure the ZyWALL to check an external RADIUS server.
WPA Group Key Update Timer (Seconds)	The <b>WPA Group Key Update Timer</b> is the rate at which the AP (if using <b>WPA-PSK</b> key management) or RADIUS server (if using <b>WPA</b> key management) sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the <b>WPA Group Key Update Timer</b> is also supported in <b>WPA-PSK</b> mode.
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 9.16.4 IEEE 802.1x + Dynamic WEP

Click the **NETWORK** and **WIRELESS CARD** to display the **Wireless Card** screen. Select **802.1x + Dynamic WEP** from the **Security** list.

**Figure 84** Wireless Card: 802.1x + Dynamic WEP

The screenshot shows the 'WIRELESS CARD' configuration page with the 'General Setup' tab selected. The 'Wireless Card' sub-tab is active. The 'Enable Wireless Card' checkbox is checked. The 'Wireless Card' status is 'Installed' and the 'ESSID' is 'ZyXEL'. The 'Hide ESSID' checkbox is unchecked. The 'Channel ID' is set to 'Channel-06 2437MHz'. The 'RTS/CTS' and 'Fragmentation' checkboxes are unchecked. The 'Security' dropdown is set to '802.1x + Dynamic WEP'. The 'ReAuthentication Timer' is set to 1800 seconds, and the 'Idle Timeout' is set to 3600 seconds. The 'Authentication Databases' link is labeled 'RADIUS'. The 'Dynamic WEP Key Exchange' dropdown is set to '64-bit'. There are 'Apply' and 'Reset' buttons at the bottom.

The following wireless LAN security fields become available when you select **802.1x + Dynamic WEP** in the **Security** drop down list-box.

**Table 58** Wireless Card: 802.1x + Dynamic WEP

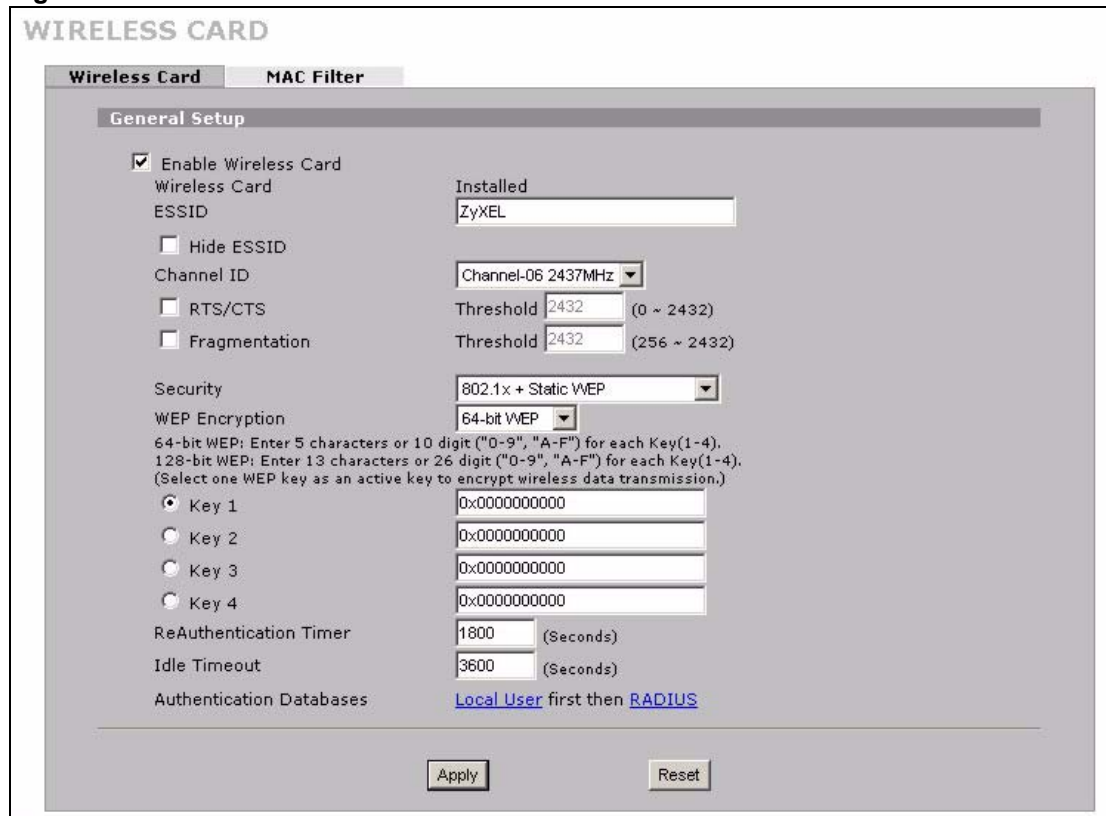
LABEL	DESCRIPTION
Security	Select <b>802.1x + Dynamic WEP</b> from the drop-down list.
ReAuthentication Timer (Seconds)	Specify how often wireless stations have to resend user names and passwords in order to stay connected. Enter a time interval between 10 and 65535 seconds. If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout (Seconds)	The ZyWALL automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the user name and password again before access to the wired network is allowed.
Authentication Databases	Click <b>RADIUS</b> to go to the <b>RADIUS</b> screen where you can configure the ZyWALL to check an external RADIUS server.
Dynamic WEP Key Exchange	Select <b>64-bit WEP</b> or <b>128-bit WEP</b> to enable data encryption.
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.



### 9.16.5 IEEE 802.1x + Static WEP

Click the **NETWORK** and **WIRELESS CARD** to display the **Wireless Card** screen. Select **802.1x + Static WEP** from the **Security** list.

**Figure 85** Wireless Card: 802.1x + Static WEP



The following wireless LAN security fields become available when you select **802.1x + Static WEP** in the **Security** drop down list-box.

**Table 59** Wireless Card: 802.1x + Static WEP

LABEL	DESCRIPTION
Security	Select <b>802.1x + Static WEP</b> from the drop-down list.
WEP Encryption	WEP (Wired Equivalent Privacy) provides data encryption to prevent unauthorized wireless stations from accessing data transmitted over the wireless network. Select <b>64-bit WEP</b> or <b>128-bit WEP</b> to enable data encryption.
Key 1 to Key 4	If you chose <b>64-bit WEP</b> in the <b>WEP Encryption</b> field, then enter any 5 characters (ASCII string) or 10 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key. If you chose <b>128-bit WEP</b> in the <b>WEP Encryption</b> field, then enter 13 characters (ASCII string) or 26 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key. There are four data encryption keys to secure your data from eavesdropping by unauthorized wireless users. The values for the keys must be set up exactly the same on the access points as they are on the wireless stations.

**Table 59** Wireless Card: 802.1x + Static WEP (continued)

LABEL	DESCRIPTION
ReAuthentication Timer (Seconds)	Specify how often wireless stations have to resend user names and passwords in order to stay connected. Enter a time interval between 10 and 65535 seconds. If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout (Seconds)	The ZyWALL automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the user name and password again before access to the wired network is allowed.
Authentication Databases	Click <b>Local User</b> to go to the <b>Local User Database</b> screen where you can view and/or edit the list of users and passwords. Click <b>RADIUS</b> to go to the <b>RADIUS</b> screen where you can configure the ZyWALL to check an external RADIUS server.
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

### 9.16.6 IEEE 802.1x + No WEP

Click the **NETWORK** and **WIRELESS CARD** to display the **Wireless Card** screen. Select **802.1x + No WEP** from the **Security** list.

**Figure 86** Wireless Card: 802.1x + No WEP

The screenshot shows the 'WIRELESS CARD' configuration page with the 'Wireless Card' tab selected. Under 'General Setup', the 'Enable Wireless Card' checkbox is checked. The 'Wireless Card' status is 'Installed'. The 'ESSID' is 'ZyXEL'. The 'Hide ESSID' checkbox is unchecked. The 'Channel ID' is set to 'Channel-06 2437MHz'. There are two 'Threshold' fields, both set to '2432', with ranges '(0 ~ 2432)' and '(256 ~ 2432)' respectively. The 'Security' dropdown is set to '802.1x + No WEP'. The 'ReAuthentication Timer' is '1800 (Seconds)' and the 'Idle Timeout' is '3600 (Seconds)'. The 'Authentication Databases' section shows a link for 'Local User' and a link for 'RADIUS'. At the bottom, there are 'Apply' and 'Reset' buttons.

The following wireless LAN security fields become available when you select **802.1x + No WEP** in the **Security** drop down list-box.

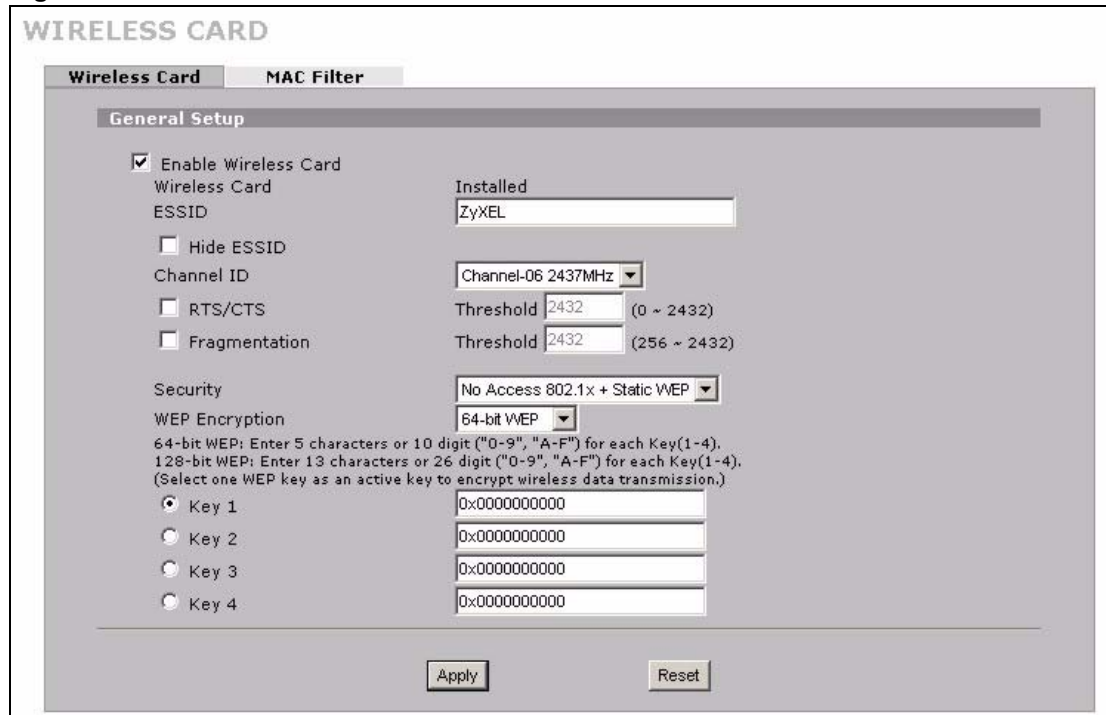
**Table 60** Wireless Card: 802.1x + No WEP

LABEL	DESCRIPTION
Security	Select <b>802.1x + No WEP</b> from the drop-down list.
ReAuthentication Timer (Seconds)	Specify how often wireless stations have to resend user names and passwords in order to stay connected. Enter a time interval between 10 and 65535 seconds. If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout (Seconds)	The ZyWALL automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the user name and password again before access to the wired network is allowed.
Authentication Databases	Click <b>Local User</b> to go to the <b>Local User Database</b> screen where you can view and/or edit the list of users and passwords. Click <b>RADIUS</b> to go to the <b>RADIUS</b> screen where you can configure the ZyWALL to check an external RADIUS server.
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

### 9.16.7 No Access 802.1x + Static WEP

Click the **NETWORK** and **WIRELESS CARD** to display the **Wireless Card** screen. Select **No Access 802.1x + Static WEP** to deny all wireless stations access to your wired network and allow wireless stations to communicate with the ZyWALL using static WEP keys for data encryption.

**Figure 87** Wireless Card: No Access 802.1x + Static WEP



The following wireless LAN security fields become available when you select **No Access 802.1x + Static WEP** in the **Security** drop down list-box.

**Table 61** Wireless Card: No Access 802.1x + Static WEP

LABEL	DESCRIPTION
Security	Select <b>No Access 802.1x + Static WEP</b> from the drop-down list.
WEP Encryption	WEP (Wired Equivalent Privacy) provides data encryption to prevent unauthorized wireless stations from accessing data transmitted over the wireless network. Select <b>64-bit WEP</b> or <b>128-bit WEP</b> to enable data encryption.
Key 1 to Key 4	If you chose <b>64-bit WEP</b> in the <b>WEP Encryption</b> field, then enter any 5 characters (ASCII string) or 10 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key. If you chose <b>128-bit WEP</b> in the <b>WEP Encryption</b> field, then enter 13 characters (ASCII string) or 26 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key.  There are four data encryption keys to secure your data from eavesdropping by unauthorized wireless users. The values for the keys must be set up exactly the same on the access points as they are on the wireless stations.
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

### 9.16.8 No Access 802.1x + No WEP

Click the **NETWORK** and **WIRELESS CARD** to display the **Wireless Card** screen. Select **No Access 802.1x + No WEP** to deny all wireless stations access to your wired network and block all wireless stations from communicating with the ZyWALL.

## 9.17 MAC Filter

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

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

**Figure 88** Wireless Card: MAC Address Filter

The screenshot shows the 'MAC Address Filter' configuration interface. It includes an 'Active' checkbox, an 'Association' label, and radio buttons for 'Allow' and 'Deny'. A table with 12 rows is present, each with a '#', a 'User Name' field, and a 'MAC Address' field. The 'MAC Address' field is divided into six sub-fields, each containing '00'. At the bottom, there are 'Apply' and 'Reset' buttons.

The following table describes the labels in this menu.

**Table 62** Wireless Card: MAC Address Filter

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

# CHAPTER 10

## Firewalls

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

### 10.1 Firewall Overview

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

### 10.2 Types of Firewalls

There are three main types of firewalls:

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

#### 10.2.1 Packet Filtering Firewalls

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

#### 10.2.2 Application-level Firewalls

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

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

### 10.2.3 Stateful Inspection Firewalls

Stateful inspection firewalls restrict access by screening data packets against defined access rules. They make access control decisions based on IP address and protocol. They also "inspect" the session data to assure the integrity of the connection and to adapt to dynamic protocols. These firewalls generally provide the best speed and transparency; however, they may lack the granular application level access control or caching that some proxies support. See [Section 10.5 on page 208](#) for more information on Stateful Inspection.

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

## 10.3 Introduction to ZyXEL's Firewall

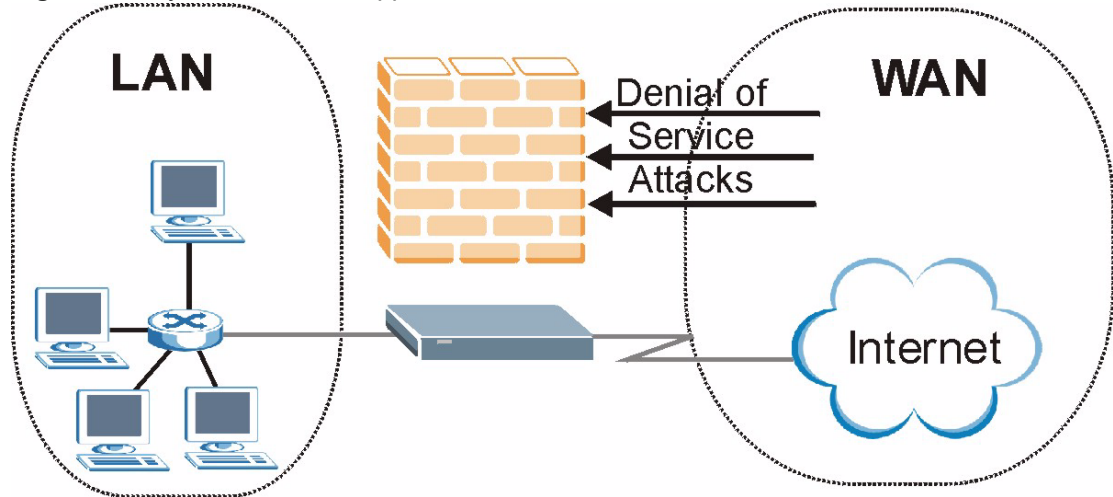
The ZyWALL firewall is a stateful inspection firewall and is designed to protect against Denial of Service attacks when activated (in SMT menu 21.2 or in the web configurator). The ZyWALL's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The ZyWALL can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

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

The ZyWALL allows you to physically separate the network into the following areas:

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

Figure 89 ZyWALL Firewall Application



## 10.4 Denial of Service

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

### 10.4.1 Basics

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

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

Some of the most common IP ports are:

**Table 63** Common IP Ports

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

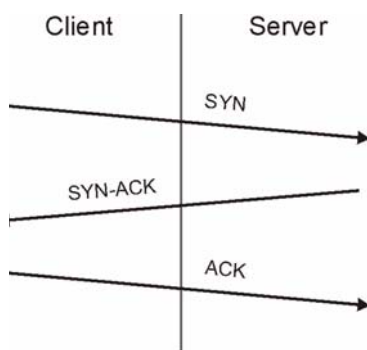


## 10.4.2 Types of DoS Attacks

There are four types of DoS attacks:

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

**Figure 90** Three-Way Handshake

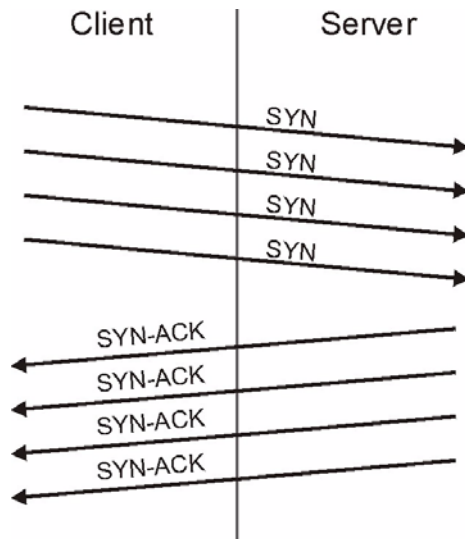


Under normal circumstances, the application that initiates a session sends a SYN (synchronize) packet to the receiving server. The receiver sends back an ACK (acknowledgment) packet and its own SYN, and then the initiator responds with an ACK (acknowledgment). After this handshake, a connection is established.

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

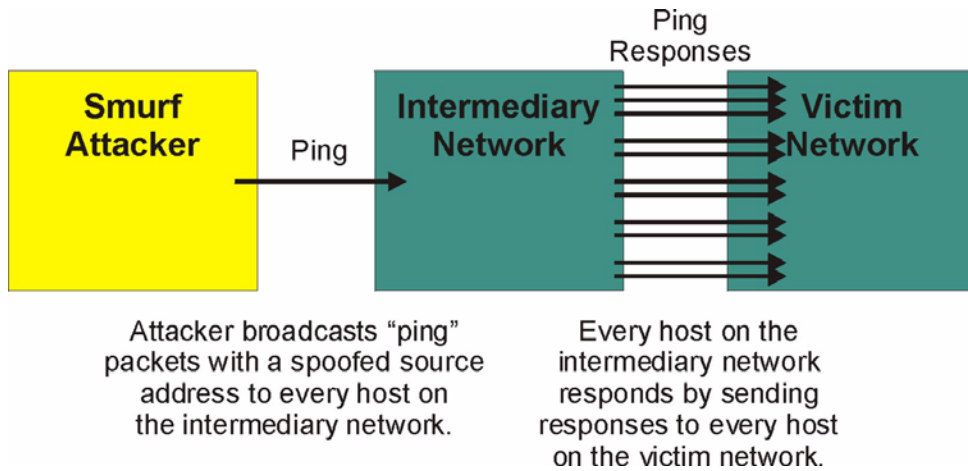
response. While the targeted system waits for the ACK that follows the SYN-ACK, it queues up all outstanding SYN-ACK responses on what is known as a backlog queue. SYN-ACKs are moved off the queue only when an ACK comes back or when an internal timer (which is set at relatively long intervals) terminates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

**Figure 91** SYN Flood



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

**Figure 92** Smurf Attack



### 10.4.2.1 ICMP Vulnerability

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

**Table 64** ICMP Commands That Trigger Alerts

5	REDIRECT
13	TIMESTAMP_REQUEST
14	TIMESTAMP_REPLY
17	ADDRESS_MASK_REQUEST
18	ADDRESS_MASK_REPLY

### 10.4.2.2 Illegal Commands (NetBIOS and SMTP)

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

**Table 65** Legal NetBIOS Commands

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

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

**Table 66** Legal SMTP Commands

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

### 10.4.2.3 Traceroute

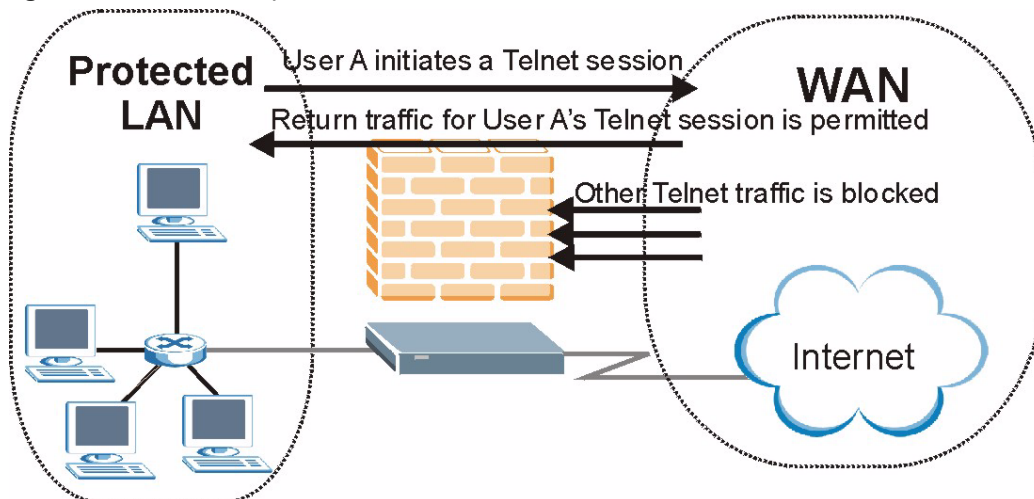
Traceroute is a utility used to determine the path a packet takes between two endpoints. Sometimes when a packet filter firewall is configured incorrectly an attacker can traceroute the firewall gaining knowledge of the network topology inside the firewall.

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

## 10.5 Stateful Inspection

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

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

**Figure 93** 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.

### 10.5.1 Stateful Inspection Process

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

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

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

- 8 Any additional inbound or outbound packets that belong to the connection are inspected to update the state table entry and to modify the temporary inbound access list entries as required, and are forwarded through the interface.
- 9 When the connection terminates or times out, the connection's state table entry is deleted and the connection's temporary inbound access list entries are deleted.

## 10.5.2 Stateful Inspection and the ZyWALL

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

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

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

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

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

## 10.5.3 TCP Security

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

If an initiation packet originates on the WAN, this means that someone is trying to make a connection from the Internet into the LAN. Except in a few special cases (see "Upper Layer Protocols" shown next), these packets are dropped and logged.

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

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

#### **10.5.4 UDP/ICMP Security**

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

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

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

#### **10.5.5 Upper Layer Protocols**

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

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

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

Any protocol that operates in this way must be supported on a case-by-case basis. You can use the web configurator's **Custom Services** feature to do this.

## 10.6 Guidelines For Enhancing Security With Your Firewall

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

## 10.7 Packet Filtering Vs Firewall

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

### 10.7.1 Packet Filtering:

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

#### 10.7.1.1 When To Use Filtering

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



## 10.7.2 Firewall

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

### 10.7.2.1 When To Use The Firewall

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

# CHAPTER 11

## Firewall Screens

This chapter shows you how to configure your ZyWALL firewall.

### 11.1 Access Methods

The web configurator is, by far, the most comprehensive firewall configuration tool your ZyWALL has to offer. For this reason, it is recommended that you configure your firewall using the web configurator. SMT screens allow you to activate the firewall. CLI commands provide limited configuration options and are only recommended for advanced users, please refer to [Appendix N on page 756](#) for firewall CLI commands.

### 11.2 Firewall Policies Overview

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

- LAN to LAN/ZyWALL
- LAN to WAN
- LAN to DMZ
- LAN to WLAN
- WLAN to LAN
- WLAN to WLAN/ZyWALL
- WAN to LAN
- WAN to WAN/ZyWALL
- WAN to DMZ
- WAN to WLAN
- WLAN to WAN
- DMZ to LAN
- DMZ to WAN
- DMZ to DMZ/ZyWALL
- DMZ to WLAN
- WLAN to DMZ

**Note:** You can only use the wireless LAN feature if a compatible ZyXEL wireless LAN card is installed.

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

- LAN to LAN/ZyWALL

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

- LAN to WAN
- LAN to DMZ
- LAN to WLAN
- WAN to DMZ
- DMZ to WAN

- WLAN to WAN

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

- WAN to LAN
- WAN to WAN/ZyWALL

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

- WAN to WLAN

This drops any packets travelling from the WAN to the WLAN and creates a log.

- DMZ to LAN
- DMZ to DMZ/ZyWALL

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

- DMZ to WLAN
- WLAN to LAN
- WLAN to DMZ
- WLAN to WLAN/ZyWALL

This prevents computers on the WLAN from communicating between networks or subnets connected to the WLAN interface and/or managing the ZyWALL.

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

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

For example, you may create rules to:

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

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

## 11.3 Rule Logic Overview

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

### 11.3.1 Rule Checklist

- 1 State the intent of the rule. For example, This restricts all IRC access from the LAN to the Internet. Or, This allows a remote Lotus Notes server to synchronize over the Internet to an inside Notes server.
- 2 Is the intent of the rule to forward or block traffic?
- 3 What direction of traffic does the rule apply to (see [Section 10.2 on page 202](#))?
- 4 What IP services will be affected?
- 5 What computers on the LAN or DMZ are to be affected (if any)?
- 6 What computers on the Internet will be affected? The more specific, the better. For example, if traffic is being allowed from the Internet to the LAN, it is better to allow only certain machines on the Internet to access the LAN.

### 11.3.2 Security Ramifications

Once the logic of the rule has been defined, it is critical to consider the security ramifications created by the rule:

- 1 Does this rule stop LAN users from accessing critical resources on the Internet? For example, if IRC is blocked, are there users that require this service?
- 2 Is it possible to modify the rule to be more specific? For example, if IRC is blocked for all users, will a rule that blocks just certain users be more effective?
- 3 Does a rule that allows Internet users access to resources on the LAN create a security vulnerability? For example, if FTP ports (TCP 20, 21) are allowed from the Internet to the LAN, Internet users may be able to connect to computers with running FTP servers.
- 4 Does this rule conflict with any existing rules?

Once these questions have been answered, adding rules is simply a matter of plugging the information into the correct fields in the web configurator screens.

### 11.3.3 Key Fields For Configuring Rules

#### 11.3.3.1 Action

Should the action be to **Drop**, **Reject** or **Permit**?

**Note:** “Drop” means the firewall silently discards the packet. “Reject” means the firewall discards packets and sends an ICMP destination-unreachable message to the sender.

### 11.3.3.2 Service

Select the service from the **Service** scrolling list box. If the service is not listed, it is necessary to first define it. See [Section 11.11.2 on page 233](#) for more information on predefined services.

### 11.3.3.3 Source Address

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

### 11.3.3.4 Destination Address

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

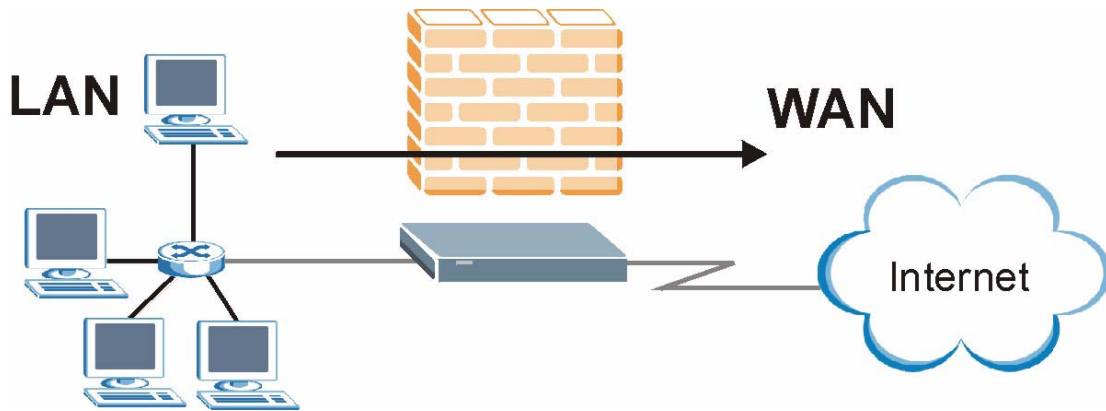
## 11.4 Connection Direction Examples

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

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

### 11.4.1 LAN To WAN Rules

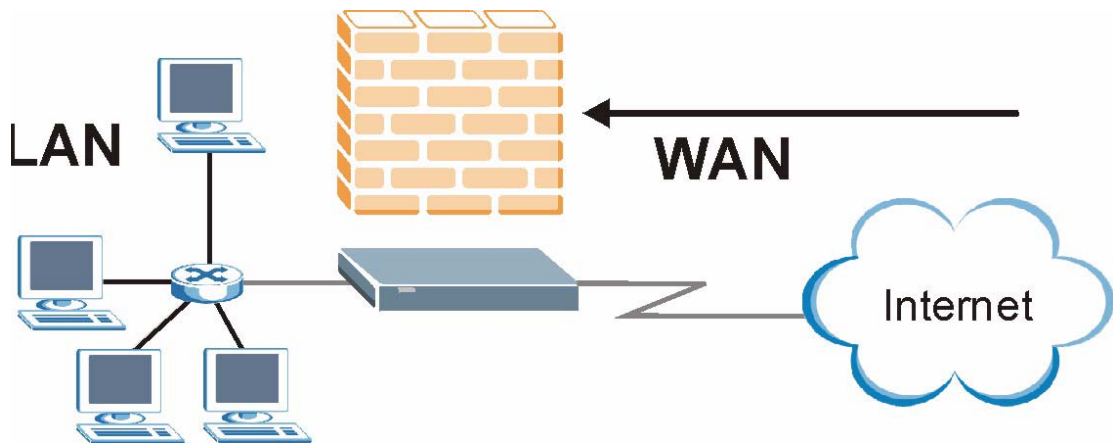
The default rule for LAN to WAN traffic is that all users on the LAN are allowed non-restricted access to the WAN. When you configure a LAN to WAN rule, you in essence want to limit some or all users from accessing certain services on the WAN. See the following figure.

**Figure 94** LAN to WAN Traffic

## 11.4.2 WAN To LAN Rules

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

See the following figure.

**Figure 95** WAN to LAN Traffic

## 11.5 Alerts

Alerts are reports on events, such as attacks, that you may want to know about right away. You can choose to generate an alert when a rule is matched in the **Edit Rule** screen (see [Figure 99 on page 224](#)). Configure the **Log Settings** screen to have the ZyWALL send an immediate e-mail message to you when an event generates an alert. Refer to the chapter on logs for details.

## 11.6 Firewall Default Rule (Router Mode)

Click **SECURITY, FIREWALL** to open the **Default Rule** screen. Enable (or activate) the firewall by selecting the **Enable Firewall** check box.

Use this screen to configure general firewall settings when the ZyWALL is set to router mode.

**Figure 96** Default Rule (Router Mode)

**FIREWALL**

**Default Rule** | **Rule Summary** | **Anti-Probing** | **Threshold** | **Service**

**Default Rule Setup**

Enable Firewall

Allow Asymmetrical Route (Warning: When this box is checked, all LAN to LAN, WAN to WAN, DMZ to DMZ and WLAN to WLAN packets will bypass the Firewall check.)

Packet Direction	Default Action	Log
LAN to LAN / ZyWALL	Permit	<input type="checkbox"/>
LAN to WAN	Permit	<input type="checkbox"/>
LAN to DMZ	Permit	<input type="checkbox"/>
LAN to WLAN	Drop	<input checked="" type="checkbox"/>
WAN to LAN	Drop	<input checked="" type="checkbox"/>
WAN to WAN / ZyWALL	Drop	<input type="checkbox"/>
WAN to DMZ	Permit	<input type="checkbox"/>
WAN to WLAN	Permit	<input type="checkbox"/>
DMZ to LAN	Permit	<input type="checkbox"/>
DMZ to WAN	Permit	<input type="checkbox"/>
DMZ to DMZ / ZyWALL	Permit	<input type="checkbox"/>
DMZ to WLAN	Drop	<input checked="" type="checkbox"/>
WLAN to LAN	Drop	<input checked="" type="checkbox"/>
WLAN to WAN	Permit	<input type="checkbox"/>
WLAN to DMZ	Drop	<input checked="" type="checkbox"/>
WLAN to WLAN / ZyWALL	Drop	<input checked="" type="checkbox"/>

Apply      Reset

The following table describes the labels in this screen.

**Table 67** Default Rule (Router Mode)

LABEL	DESCRIPTION
Enable Firewall	Select this check box to activate the firewall. The ZyWALL performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Allow Asymmetrical Route	Select this check box to have the ZyWALL firewall permit the use of triangle route topology on the network.  <b>Note:</b> Allowing asymmetrical routes may let traffic from the WAN go directly to a LAN computer without passing through the ZyWALL. See <a href="#">Appendix I on page 722</a> for more on triangle route topology and how to deal with this problem.

**Table 67** Default Rule (Router Mode) (continued)

LABEL	DESCRIPTION
Packet Direction	<p>This is the direction of travel of packets (<b>LAN to LAN/ZyWALL, LAN to WAN, LAN to DMZ, LAN to WLAN, WAN to LAN, WAN to WAN/ZyWALL, WAN to DMZ, WAN to WLAN, DMZ to LAN, DMZ to WAN, DMZ to DMZ/ZyWALL, DMZ to WLAN, WLAN to LAN, WLAN to WAN, WLAN to DMZ or WLAN to WLAN/ZyWALL</b>).</p> <p>Firewall rules are grouped based on the direction of travel of packets to which they apply. For example, <b>LAN to LAN/ZyWALL</b> means packets traveling from a computer/subnet on the LAN to either another computer/subnet on the LAN interface of the ZyWALL or the ZyWALL itself.</p>
Default Action	<p>Use the drop-down list boxes to select whether to <b>Drop</b> (silently discard), <b>Reject</b> (discard and send an ICMP destination-unreachable message to the sender) or <b>Permit</b> (allow the passage of) packets that are traveling in the selected direction.</p>
Log	<p>Select the check box to create a log (when the above action is taken) for packets that are traveling in the selected direction and do not match any of your customized rules.</p>
Apply	<p>Click <b>Apply</b> to save your changes back to the ZyWALL.</p>
Reset	<p>Click <b>Reset</b> to begin configuring this screen afresh.</p>

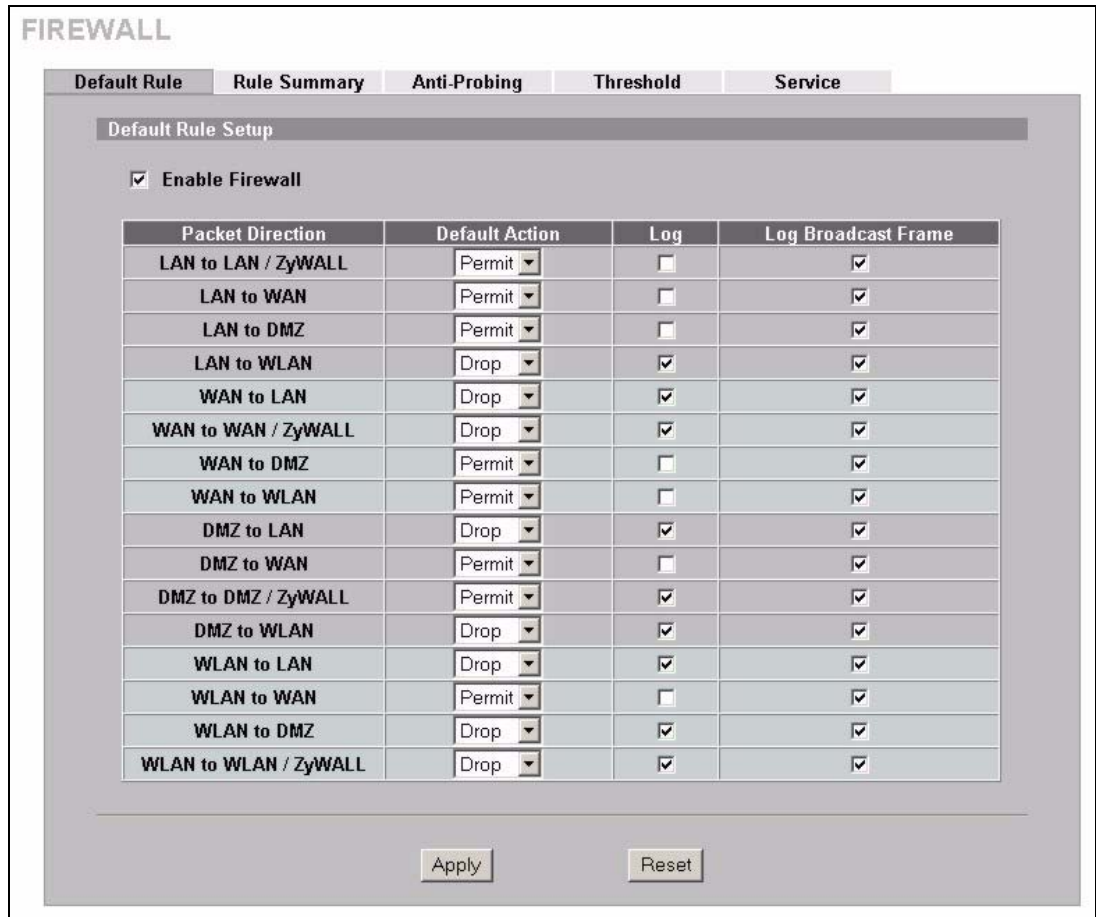
## 11.7 Firewall Default Rule (Bridge Mode)

Click **SECURITY, FIREWALL** to open the **Default Rule** screen. Enable (or activate) the firewall by selecting the **Enable Firewall** check box.

Use this screen to configure general firewall settings when the ZyWALL is set to bridge mode.



**Figure 97** Default Rule (Bridge Mode)



The following table describes the labels in this screen.

**Table 68** Default Rule (Bridge Mode)

LABEL	DESCRIPTION
Enable Firewall	Select this check box to activate the firewall. The ZyWALL performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Packet Direction	This is the direction of travel of packets ( <b>LAN to LAN/ZyWALL, LAN to WAN, LAN to DMZ, LAN to WLAN, WAN to LAN, WAN to WAN/ZyWALL, WAN to DMZ, WAN to WLAN, DMZ to LAN, DMZ to WAN, DMZ to DMZ/ZyWALL, DMZ to WLAN, WLAN to LAN, WLAN to WAN, WLAN to DMZ or WLAN to WLAN/ZyWALL</b> ).  Firewall rules are grouped based on the direction of travel of packets to which they apply. For example, <b>LAN to LAN/ZyWALL</b> means packets traveling from a computer/subnet on the LAN to either another computer/subnet on the LAN interface of the ZyWALL or the ZyWALL itself.
Default Action	Use the drop-down list boxes to select whether to <b>Drop</b> (silently discard), <b>Reject</b> (discard and send an ICMP destination-unreachable message to the sender) or <b>Permit</b> (allow the passage of) packets that are traveling in the selected direction.
Log	Select the check box to create a log (when the above action is taken) for packets that are traveling in the selected direction and do not match any of your customized rules.

**Table 68** Default Rule (Bridge Mode)

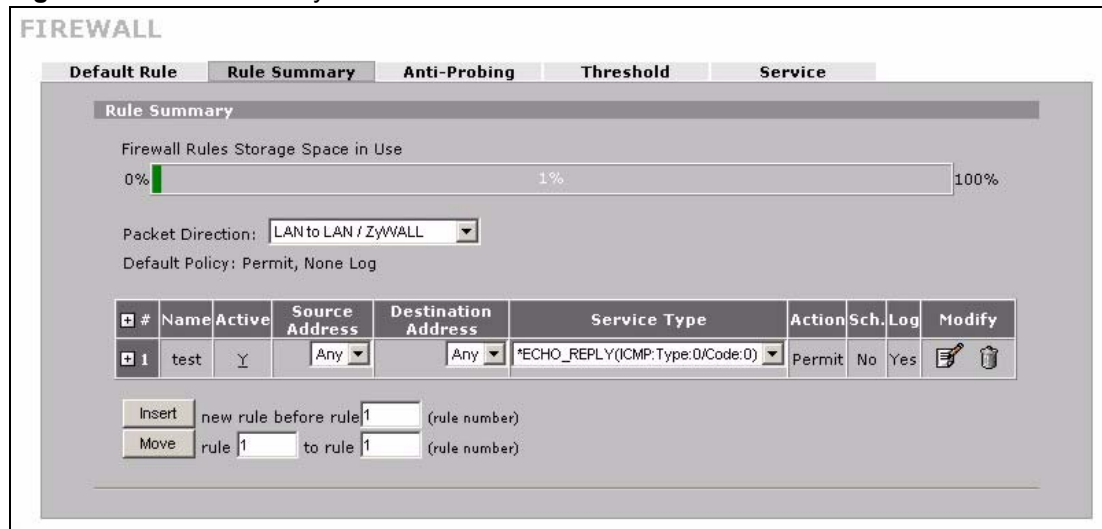
LABEL	DESCRIPTION
Log Broadcast Frame	Select the check box to create a log for any Layer 2 broadcast frames that are traveling in the selected direction.
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 11.8 Firewall Rule Summary

Click **SECURITY, FIREWALL**, then the **Rule Summary** tab to open the screen. This screen displays a list of the configured firewall rules.

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

**Figure 98** Rule Summary



The following table describes the labels in this screen.

**Table 69** Rule Summary

LABEL	DESCRIPTION
Firewall Rules Storage Space in Use	This bar displays the percentage of the ZyWALL's firewall rules storage space that is currently in use. The bar turns from green to red when the maximum is being approached. When the bar is red, you should consider deleting unnecessary firewall rules before adding more firewall rules.
Packet Direction	Use the drop-down list box to select a direction of travel of packets ( <b>LAN to LAN/ ZyWALL, LAN to WAN, LAN to DMZ, LAN to WLAN, WAN to LAN, WAN to WAN/ ZyWALL, WAN to DMZ, WAN to WLAN, DMZ to LAN, DMZ to WAN, DMZ to DMZ/ZyWALL, DMZ to WLAN, WLAN to LAN, WLAN to WAN, WLAN to DMZ or WLAN to WLAN/ZyWALL</b> ) for which you want to configure firewall rules.
Default Policy	This field displays the default action and log policy you selected in the <b>Default Rule</b> screen for the packet direction shown in the field above.

**Table 69** Rule Summary

LABEL	DESCRIPTION
	The following read-only fields summarize the rules you have created that apply to traffic traveling in the selected packet direction. The firewall rules that you configure (summarized below) take priority over the general firewall action settings above.
#	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn. Click + to expand or - to collapse the <b>Source Address</b> , <b>Destination Address</b> and <b>Service Type</b> drop down lists.
Name	This is the name of the firewall rule.
Active	This field displays whether a firewall is turned on ( <b>Y</b> ) or not ( <b>N</b> ).
Source Address	This drop-down list box displays the source addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to <b>Any</b> .
Destination Address	This drop-down list box displays the destination addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to <b>Any</b> .
Service Type	This drop-down list box displays the services to which this firewall rule applies. See <a href="#">Table 75 on page 233</a> for more information.
Action	This field displays whether the firewall silently discards packets ( <b>Drop</b> ), discards packets and sends an ICMP destination-unreachable message to the sender ( <b>Reject</b> ) or allow the passage of packets ( <b>Permit</b> ).
Sch.	This field tells you whether a schedule is specified ( <b>Yes</b> ) or not ( <b>No</b> ).
Log	This field shows you whether a log is created when packets match this rule ( <b>Yes</b> ) or not ( <b>No</b> ).
Modify	Click the edit icon to go to the screen where you can edit the rule. Click the delete icon to delete an existing firewall rule. A window display asking you to confirm that you want to delete the firewall rule. Note that subsequent firewall rules move up by one when you take this action.
Insert	Type the index number for where you want to put a rule. For example, if you type 6, your new rule becomes number 6 and the previous rule 6 (if there is one) becomes rule 7. Click <b>Insert</b> to display this screen and refer to the following table for information on the fields.
Move	Type a rule's index number and the number for where you want to put that rule. Click <b>Move</b> to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering.

## 11.8.1 Firewall Edit Rule

Follow these directions to create a new rule.

- 1** In the **Rule Summary** screen, type the index number for where you want to put the rule. For example, if you type 6, your new rule becomes number 6 and the previous rule 6 (if there is one) becomes rule 7.
- 2** Click **Insert** to display the **Firewall Edit Rule** screen and refer to the following table for information on the labels.

Figure 99 Firewall Edit Rule

### FIREWALL - EDIT RULE

**Rule Name**

---

**Edit Source Address**

<b>Address Editor</b>	<b>Source Address(es)</b>
<b>Address Type</b> <span style="border: 1px solid gray; padding: 2px;">Any Address</span>	<div style="border: 1px solid gray; padding: 5px; min-height: 40px;">Any</div>
<b>Start IP Address</b> <span style="border: 1px solid gray; padding: 2px;">0 . 0 . 0 . 0</span>	
<b>End IP Address</b> <span style="border: 1px solid gray; padding: 2px;">0 . 0 . 0 . 0</span>	
<b>Subnet Mask</b> <span style="border: 1px solid gray; padding: 2px;">0 . 0 . 0 . 0</span>	
<input type="button" value="Add"/> <input type="button" value="Modify"/>	<input type="button" value="Delete"/>

---

**Edit Destination Address**

<b>Address Editor</b>	<b>Destination Address(es)</b>
<b>Address Type</b> <span style="border: 1px solid gray; padding: 2px;">Any Address</span>	<div style="border: 1px solid gray; padding: 5px; min-height: 40px;">Any</div>
<b>Start IP Address</b> <span style="border: 1px solid gray; padding: 2px;">0 . 0 . 0 . 0</span>	
<b>End IP Address</b> <span style="border: 1px solid gray; padding: 2px;">0 . 0 . 0 . 0</span>	
<b>Subnet Mask</b> <span style="border: 1px solid gray; padding: 2px;">0 . 0 . 0 . 0</span>	
<input type="button" value="Add"/> <input type="button" value="Modify"/>	<input type="button" value="Delete"/>

---

**Edit Service**

<b>Available Services (See <a href="#">Service</a>)</b>	<b>Selected Service(s)</b>	
<div style="border: 1px solid gray; padding: 5px; min-height: 100px;"> <ul style="list-style-type: none"> <li>*CNM(IP:234)</li> <li>Any(All)</li> <li>Any(TCP)</li> <li>Any(UDP)</li> <li>Any(ICMP)</li> <li>AIM/NEW_ICQ(TCP:5190)</li> <li>AUTH(TCP:113)</li> <li>BGP(TCP:179)</li> <li>BOOTP_CLIENT(UDP:68)</li> <li>BOOTP_SERVER(UDP:67)</li> <li>CU-SEEME(TCP/UDP:7648,24032)</li> <li>DNS(TCP/UDP:53)</li> <li>FINGER(TCP:79)</li> <li>FTP(TCP:20,21)</li> <li>H.323(TCP:1720)</li> </ul> </div>	<div style="display: flex; justify-content: center; gap: 10px;"> <span style="font-size: 24px;">&lt;&lt;</span> <span style="font-size: 24px;">&gt;&gt;</span> </div>	<div style="border: 1px solid gray; padding: 5px; min-height: 100px;"></div>

---

**Edit Schedule**

**Day to Apply:**  
 Sun  Mon  Tue  Wed  Thu  Fri  Sat

**Time of Day to Apply: (24-Hour Format)**  
 All day

**Start:**  (Hour)  (Minute)    **End:**  (Hour)  (Minute)

---

**Actions When Matched**

Log Packet Information When Matched

Send Alert Message to Administrator When Matched

**Action for Matched Packets** Permit

The following table describes the labels in this screen.

**Table 70** Firewall Edit Rule

LABEL	DESCRIPTION
Rule Name	Enter a descriptive name of up to 31 printable ASCII characters (except Extended ASCII characters) for the firewall rule. Spaces are allowed.
Edit Source/ Destination Address	
Address Type	Do you want your rule to apply to packets with a particular (single) IP, a range of IP addresses (for example 192.168.1.10 to 192.169.1.50), a subnet or any IP address? Select an option from the drop-down list box that includes: <b>Single Address, Range Address, Subnet Address</b> and <b>Any Address</b> . You can configure up to 20 source or destination IP address entries in a rule.
Start IP Address	Enter the single IP address or the starting IP address in a range here.
End IP Address	Enter the ending IP address in a range here.
Subnet Mask	Enter the subnet mask here, if applicable.
Add	Click <b>Add</b> to add a new address to the <b>Source</b> or <b>Destination Address(es)</b> box. You can add multiple addresses, ranges of addresses, and/or subnets.
Modify	To edit an existing source or destination address, select it from the box and click <b>Modify</b> .
Delete	Highlight an existing source or destination address from the <b>Source</b> or <b>Destination Address(es)</b> box above and click <b>Delete</b> to remove it.
Edit Service	
Available/ Selected Services	Please see <a href="#">Section 11.11 on page 230</a> for more information on services available. Highlight a service from the <b>Available Services</b> box on the left, then click >> to add it to the <b>Selected Service(s)</b> box on the right. To remove a service, highlight it in the <b>Selected Service(s)</b> box on the right, then click <<.
Edit Schedule	
Day to Apply	Select everyday or the day(s) of the week to apply the rule.
Time of Day to Apply (24-Hour Format)	Select <b>All Day</b> or enter the start and end times in the hour-minute format to apply the rule.
Actions When Matched	
Log Packet Information When Matched	This field determines if a log for packets that match the rule is created ( <b>Yes</b> ) or not ( <b>No</b> ). Go to the <b>Log Settings</b> page and select the <b>Access Control</b> logs category to have the ZyWALL record these logs.
Send Alert Message to Administrator When Matched	Select the check box to have the ZyWALL generate an alert when the rule is matched.
Action for Matched Packets	Use the drop-down list box to select whether to discard ( <b>Drop</b> ), deny and send an ICMP destination-unreachable message to the sender of ( <b>Reject</b> ) or allow the passage of ( <b>Permit</b> ) packets that match this rule.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

## 11.9 Anti-Probing

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

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

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

**Figure 100** Anti-Probing

The following table describes the labels in this screen.

**Table 71** Anti-Probing

LABEL	DESCRIPTION
Respond to PING on	The ZyWALL does not respond to any incoming Ping requests when <b>Disable</b> is selected. Select <b>LAN</b> to reply to incoming LAN Ping requests. Select <b>WAN</b> to reply to incoming WAN Ping requests. Select <b>DMZ</b> to reply to incoming DMZ Ping requests. Select <b>WLAN</b> to reply to incoming WLAN Ping requests. Otherwise select <b>ALL</b> to reply to both incoming LAN and WAN and DMZ and WLAN Ping requests.
Do not respond to requests for unauthorized services.	Select this option to prevent hackers from finding the ZyWALL by probing for unused ports. If you select this option, the ZyWALL will not respond to port request(s) for unused ports, thus leaving the unused ports and the ZyWALL unseen. By default this option is not selected and the ZyWALL will reply with an ICMP Port Unreachable packet for a port probe on its unused UDP ports, and a TCP Reset packet for a port probe on its unused TCP ports.  Note that the probing packets must first traverse the ZyWALL's firewall mechanism before reaching this anti-probing mechanism. Therefore if the firewall mechanism blocks a probing packet, the ZyWALL reacts based on the corresponding firewall policy to send a TCP reset packet for a blocked TCP packet or an ICMP port-unreachable packet for a blocked UDP packets or just drop the packets without sending a response packet.
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 11.10 Firewall Threshold

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

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

### 11.10.1 Threshold Values

Tune these parameters when the ZyWALL is under DoS attacks and after you have checked the firewall logs. 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.

If you use P2P applications such as file sharing with eMule or eDonkey quite often, it's recommended that you increase the threshold values since lots of sessions will be established during a small period of time and the ZyWALL may take them as DoS attacks.

### 11.10.2 Half-Open Sessions

For TCP, half-open means that the session has not reached the established state-the TCP three-way handshake has not yet been completed (see [Figure 90 on page 205](#)). For UDP, half-open means that the firewall has detected no return traffic. An unusually high number of half-open sessions (either an absolute number or measured as the arrival rate) could indicate that a Denial of Service attack is occurring.

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

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

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

### 11.10.2.1 TCP Maximum Incomplete and Blocking Time

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

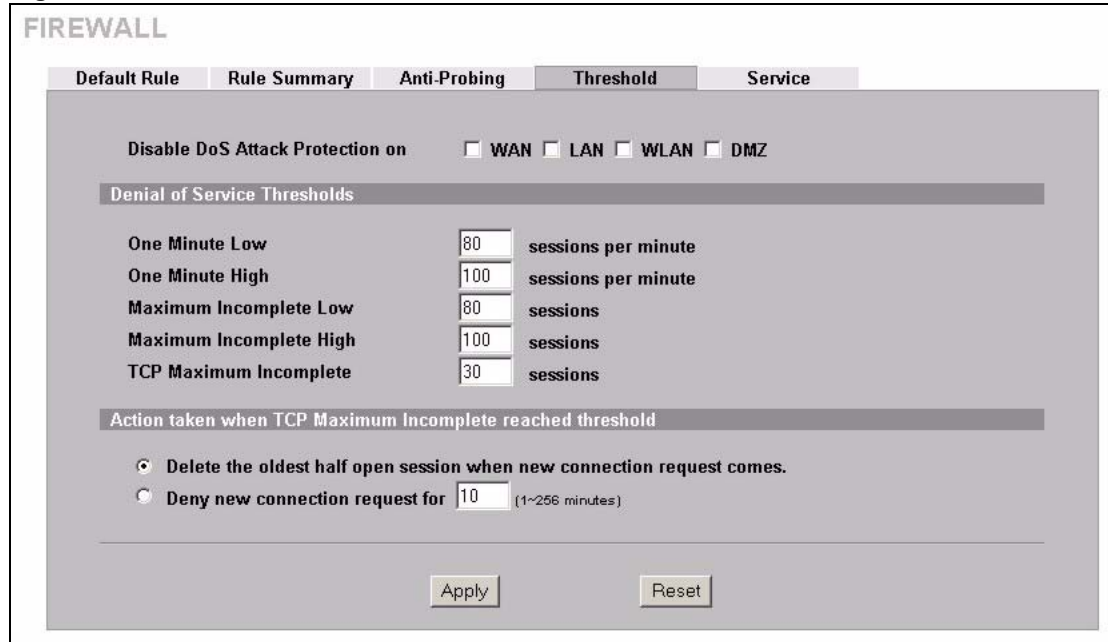
Whenever the number of half-open sessions with the same destination host address rises above a threshold (**TCP Maximum Incomplete**), the ZyWALL starts deleting half-open sessions according to one of the following methods:

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

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



**Figure 101** Firewall Threshold



The following table describes the labels in this screen.

**Table 72** Firewall Threshold

LABEL	DESCRIPTION
Disable DoS Attack Protection on	Select the check box of an interface to which the ZyWALL does not apply the thresholds. This disables DoS protection on the selected interface.
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.
One Minute High	This is the rate of new half-open sessions that causes the firewall to start deleting half-open sessions. When the rate of new connection attempts rises above this number, the ZyWALL deletes half-open sessions as required to accommodate new connection attempts.  The numbers, say 80 in the <b>One Minute Low</b> field and 100 in this field, cause the ZyWALL to start deleting half-open sessions when more than 100 session establishment attempts have been detected in the last minute, and to stop deleting half-open sessions when fewer than 80 session establishment attempts have been detected in the last minute.
Maximum Incomplete Low	This is the number of existing half-open sessions that causes the firewall to stop deleting half-open sessions. The ZyWALL continues to delete half-open requests as necessary, until the number of existing half-open sessions drops below this number.

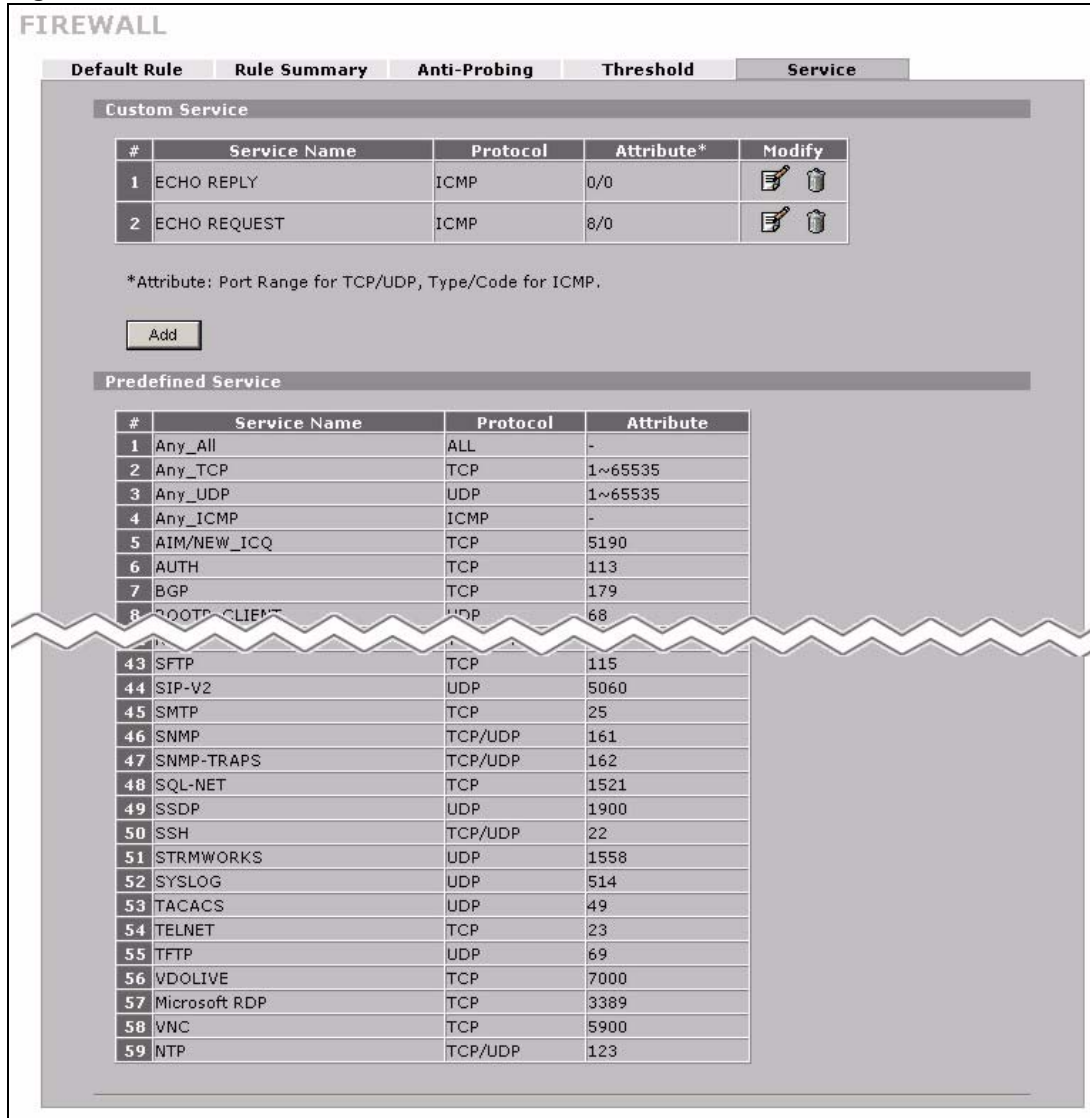
**Table 72** Firewall Threshold (continued)

LABEL	DESCRIPTION
Maximum Incomplete High	<p>This is the number of existing half-open sessions that causes the firewall to start deleting half-open sessions. When the number of existing half-open sessions rises above this number, the ZyWALL deletes half-open sessions as required to accommodate new connection requests. Do not set <b>Maximum Incomplete High</b> to lower than the current <b>Maximum Incomplete Low</b> number.</p> <p>The above values, say 80 in the <b>Maximum Incomplete Low</b> field and 100 in this field, cause the ZyWALL to start deleting half-open sessions when the number of existing half-open sessions rises above 100, and to stop deleting half-open sessions with the number of existing half-open sessions drops below 80.</p>
TCP Maximum Incomplete	<p>This is the number of existing half-open TCP sessions with the same destination host IP address that causes the firewall to start dropping half-open sessions to that same destination host IP address. Enter a number between 1 and 256. As a general rule, you should choose a smaller number for a smaller network, a slower system or limited bandwidth.</p>
Action taken when the TCP Maximum Incomplete threshold is reached.	
Delete the oldest half open session when new connection request comes	<p>Select this radio button to clear the oldest half open session when a new connection request comes.</p>
Deny new connection request for	<p>Select this radio button and specify for how long the ZyWALL should block new connection requests when <b>TCP Maximum Incomplete</b> is reached.</p> <p>Enter the length of blocking time in minutes (between 1 and 256).</p>
Apply	<p>Click <b>Apply</b> to save your changes back to the ZyWALL.</p>
Reset	<p>Click <b>Reset</b> to begin configuring this screen afresh.</p>

## 11.11 Service

Click **SECURITY, FIREWALL**, then the **Service** tab to open the screen as shown next. Use this screen to configure custom services for use in firewall rules or view the services that are predefined in the ZyWALL.

**Figure 102** Firewall Service



The following table describes the labels in this screen.

**Table 73** Firewall Service

LABEL	DESCRIPTION
Custom Service	This table shows all configured custom services.
#	This is the index number of the custom service.
Service Name	This is the name of the service.
Protocol	This is the IP protocol type. If you selected <b>Custom</b> , this is the IP protocol value you entered.
Attribute	This is the IP port number or ICMP type and code that defines the service.
Modify	Click the edit icon to go to the screen where you can edit the service. Click the delete icon to remove an existing service. A window displays asking you to confirm that you want to delete the service. Note that subsequent services move up by one when you take this action.

**Table 73** Firewall Service

LABEL	DESCRIPTION
Add	Click this button to bring up the screen that you use to configure a new custom service that is not in the predefined list of services.
Predefined Service	This table shows all the services that are already configured for use in firewall rules. See <a href="#">Section 11.11.2 on page 233</a> for more on the services.
#	This is the index number of the predefined service.
Service Name	This is the name of the service.
Protocol	This is the IP protocol type. There may be more than one IP protocol type.
Attribute	This is the IP port number or ICMP type and code that defines the service.

### 11.11.1 Firewall Edit Custom Service

Configure customized ports for services not predefined by the ZyWALL (see [Section 11.11.2 on page 233](#) for a list of predefined services). For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

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

**Figure 103** Firewall Edit Custom Service

The following table describes the labels in this screen.

**Table 74** Firewall Edit Custom Service

LABEL	DESCRIPTION
Service Name	Enter a unique name for your custom service.
IP Protocol	Choose the IP protocol ( <b>TCP</b> , <b>UDP</b> , <b>TCP/UDP</b> , <b>ICMP</b> or <b>Custom</b> ) that defines your customized service from the drop down list box.
Port Range	Enter the port number (from 1 to 255) that defines the customized service To specify one port only, enter the port number in the <b>From</b> field and enter it again in the <b>To</b> field. To specify a span of ports, enter the first port in the <b>From</b> field and enter the last port in the <b>To</b> field.

**Table 74** Firewall Edit Custom Service

LABEL	DESCRIPTION
Type/Code	This field is available only when you select <b>ICMP</b> in the <b>IP Protocol</b> field. The ICMP messages are identified by their types and in some cases codes. Enter the type number in the <b>Type</b> field and select the <b>Code</b> radio button and enter the code number if any.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

## 11.11.2 Predefined Services

The **Predefined Services** table in the **Service** screen 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, **DNS (UDP/TCP:53)** means UDP port 53 and TCP port 53.

**Table 75** Predefined Services

SERVICE	DESCRIPTION
Any_All(ALL:0)	This is for any IP protocol using any port or type.
Any_TCP(TCP:1~65535)	This is for any TCP protocol using any TCP port.
Any_UDP(UDP:1~65535)	This is for any UDP protocol using any UDP port.
Any_ICMP(ICMP:0)	This is for any ICMP protocol using any ICMP type and code.
AIM/New-ICQ(TCP:5190)	AOL's Internet Messenger service, used as a listening port by ICQ.
AUTH(TCP:113)	Authentication protocol used by some servers.
BGP(TCP:179)	Border Gateway Protocol.
BOOTP_CLIENT(UDP:68)	DHCP Client.
BOOTP_SERVER(UDP:67)	DHCP Server.
CU-SEEME (TCP/UDP:7648, 24032)	A popular videoconferencing solution from White Pines Software.
DNS(TCP/UDP:53)	Domain Name Server, a service that matches web names (e.g. www.zyxel.com) 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.
H.323(TCP:1720)	NetMeeting uses this protocol.
HTTP(TCP:80)	Hyper Text Transfer Protocol – a client/server protocol for the world wide web.
HTTPS(TCP:443)	HTTPS is a secured http session often used in e-commerce.
ICQ(UDP:4000)	This is a popular Internet chat program.
IKE(UDP:500)	The Internet Key Exchange algorithm is used for key distribution and management.

**Table 75** Predefined Services (continued)

SERVICE	DESCRIPTION
IMAP(TCP/UDP:143)	Internet Message Access Protocol (IMAP) is used to access mail stored on a remote mail server over a TCP/IP connection using port 143. IMAP has shorter response times than POP3.
IMAPS(TCP/UDP:993)	IMAP over TLS/SSL (IMAPS) is a secure protocol (that encrypts IMAP traffic) for receiving mail using a TLS/SSL connection.
AX.25(AX.25:0)	AX.25 (Amateur X.25, an "Amateur" version of X.25) is the communications protocol used for packet radio.
IPv6(IPv6:0)	IPv6 (Internet Protocol version 6) is a protocol designed by the IETF to replace and solve many problems of the version 4 (IPv4).
IPSEC_TRANSPORT / TUNNEL(AH:0)	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
IPSEC_TUNNEL(ESP:0)	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
IRC(TCP/UDP:6667)	This is another popular Internet chat program.
MSN(TCP:1863)	Microsoft Networks' messenger service uses this protocol.
MULTICAST(IGMP:0)	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
NetBIOS(TCP/UDP:137~139, 445)	NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to connect to and communicate with a LAN.
NEWS(TCP:144)	A protocol for news groups.
NFS(UDP:2049)	Network File System – NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP(TCP:119)	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
POP3(TCP:110)	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
POP3S(TCP/UDP:995)	POP3 over TLS/SSL allows users to download mail over a secure POP3 connection using TLS/SSL.
PPTP(TCP:1723)	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL(GRE:0)	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the data channel.
RCMD(TCP:512)	Remote Command Service.
REAL_AUDIO(TCP:7070)	A streaming audio service that enables real time sound over the web.
REXEC(TCP:514)	Remote Execution Daemon.
RLOGIN(TCP:513)	Remote Login.
ROADRUNNER(TCP/UDP:1026)	This is Time Warner's cable modem session management protocol. It handles authentication and dynamic addressing.
RTELNET(TCP:107)	Remote Telnet.
RTSP(TCP/UDP:554)	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP(TCP:115)	Simple File Transfer Protocol.

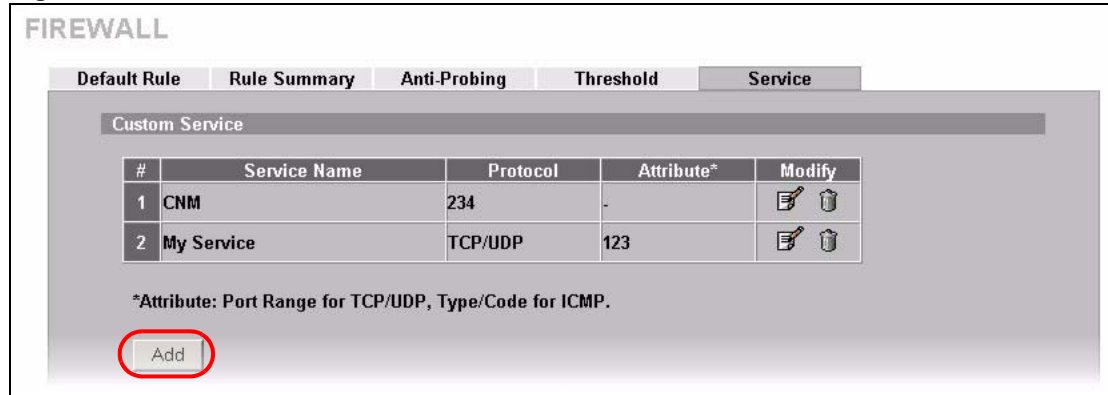
**Table 75** Predefined Services (continued)

SERVICE	DESCRIPTION
SIP-V2(UDP:5060)	The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet. SIP is used in VoIP (Voice over IP), the sending of voice signals over the Internet Protocol.
SMTP(TCP:25)	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP(TCP/UDP:161)	Simple Network Management Program.
SNMP-TRAPS(TCP/UDP:162)	Traps for use with the SNMP (RFC:1215).
SQL-NET(TCP:1521)	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSDP(UDP:1900)	Simple Service Discovery Protocol (SSDP) is a discovery service searching for Universal Plug and Play devices on your home network or upstream Internet gateways using UDP port 1900.
SSH(TCP/UDP:22)	Secure Shell Remote Login Program.
STRMWORKS(UDP:1558)	Stream Works Protocol.
SYSLOG(UDP:514)	Syslog allows you to send system logs to a UNIX server.
TACACS(UDP:49)	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET(TCP:23)	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP(UDP:69)	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE(TCP:7000)	Another videoconferencing solution.
Microsoft RDP(TCP:3389)	Microsoft offers terminal services through RDP (Remote Desktop Protocol) to allow RDP clients to connect to a Windows terminal server using UDP port 3389.
VNC(TCP:5900)	Virtual Network Computing (VNC) is used for remote connection (desktop sharing) between a VNC server and a VNC viewer on TCP port 5900.
NTP(TCP/UDP:123)	NTP (Network Time Protocol) is commonly used to synchronize the time with a remote time server.

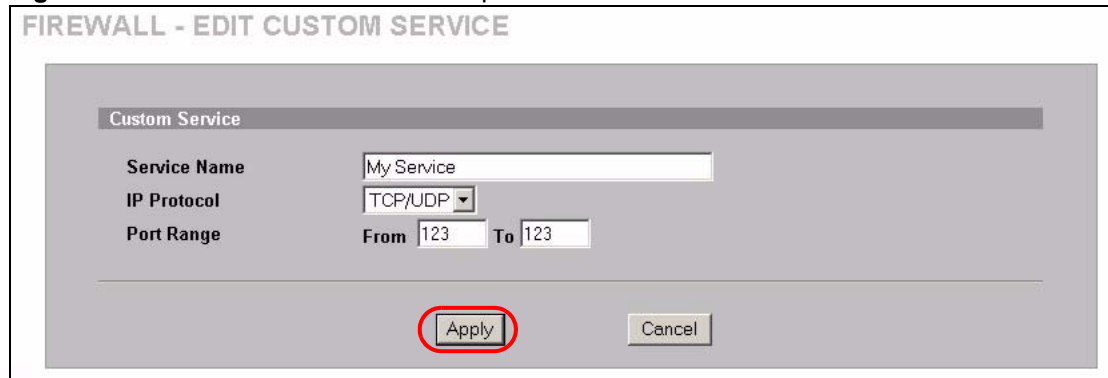
## 11.12 Example Firewall Rule

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

- 1 In the **Service** screen, click **Add** to open the **Edit Custom Service** screen.

**Figure 104** Service

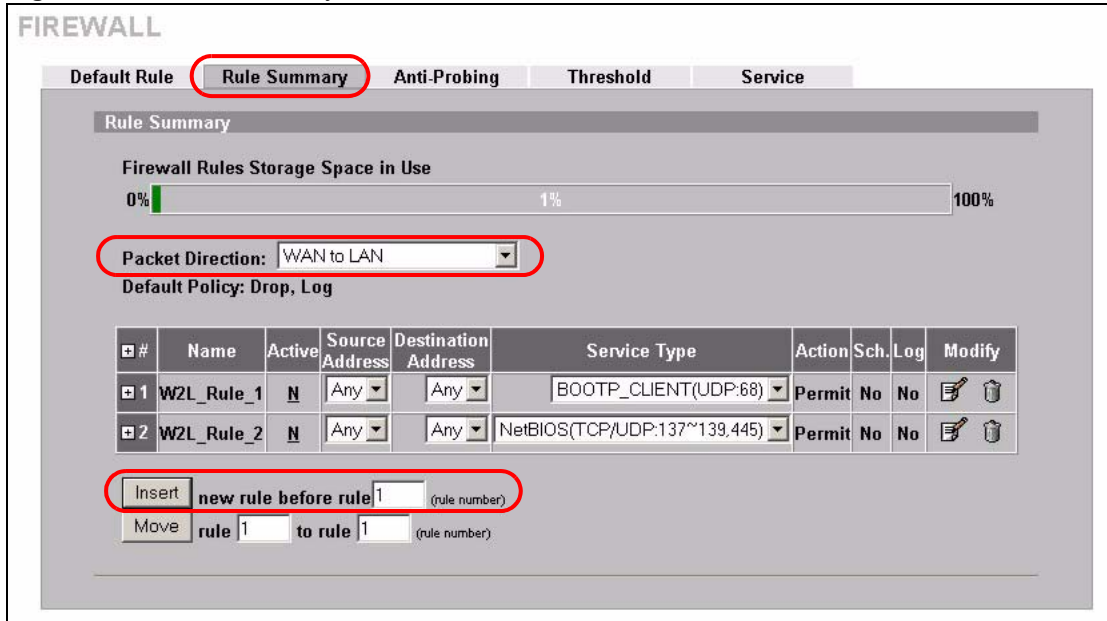
2 Configure it as follows and click **Apply**.

**Figure 105** Edit Custom Service Example

- 3 Click the **Rule Summary** tab. Select **WAN to LAN** from the **Packet Direction** drop-down list box.
- 4 In the **Rule Summary** screen, type the index number for where you want to put the rule. For example, if you type 6, your new rule becomes number 6 and the previous rule 6 (if there is one) becomes rule 7.
- 5 Click **Insert** to display the firewall rule configuration screen.

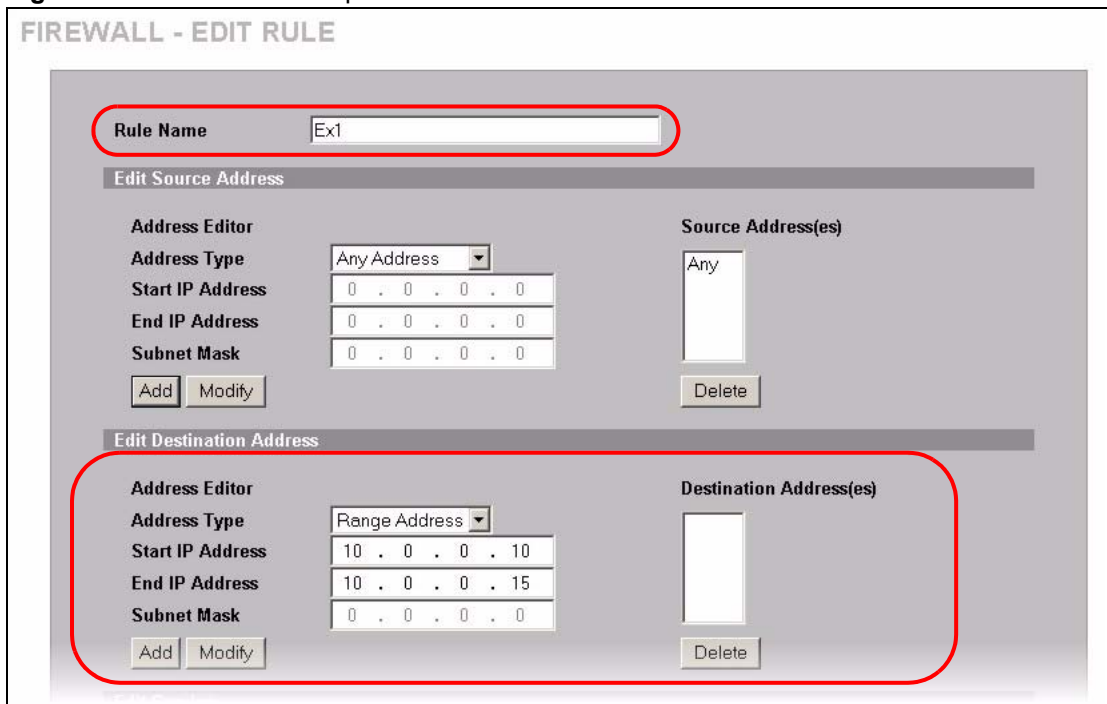


**Figure 106** Rule Summary



- 6 Enter the name of the firewall rule.
- 7 Select **Any** in the **Destination Address(es)** box and then click **Delete**.
- 8 Configure the destination address screen as follows and click **Add**.

**Figure 107** Rule Edit Example



- 9 In the **Edit Rule** screen, use the arrows between **Available Services** and **Selected Service(s)** to configure it as follows. Click **Apply** when you are done.

**Note:** Custom services show up with an \* before their names in the **Services** list box and the **Rule Summary** list box.

**Figure 108** My Service Rule Configuration

**FIREWALL - EDIT RULE**

Rule Name:

---

**Edit Source Address**

Address Editor: Address Type:  Start IP Address:  End IP Address:  Subnet Mask:

Source Address(es):

---

**Edit Destination Address**

Address Editor: Address Type:  Start IP Address:  End IP Address:  Subnet Mask:

Destination Address(es):

---

**Edit Service**

Available Services (See [Service](#)):

- \*CNM(IP:234)
- Any(All)
- Any(TCP)
- Any(UDP)
- Any(ICMP)
- AIM/NEW\_JCQ(TCP:5190)
- AUTH(TCP:113)
- BGP(TCP:179)
- BOOTP\_CLIENT(UDP:68)
- BOOTP\_SERVER(UDP:67)
- CU-SEEME(TCP/UDP:7648,24032)
- DNS(TCP/UDP:53)
- FINGER(TCP:79)
- FTP(TCP:20,21)
- H.323(TCP:1720)

Selected Service(s): \*My Service(TCP/UDP:123)

<<      >>

---

**Edit Schedule**

Day to Apply:  Sun  Mon  Tue  Wed  Thu  Fri  Sat

Time of Day to Apply: (24-Hour Format)

All day

Start:  (Hour)  (Minute)    End:  (Hour)  (Minute)

---

**Actions When Matched**

Log Packet Information When Matched

Send Alert Message to Administrator When Matched

Action for Matched Packets:

---

Apply

**Figure 109** My Service Example Rule Summary

**FIREWALL**

Default Rule   **Rule Summary**   Anti-Probing   Threshold   Service

**Rule Summary**

Firewall Rules Storage Space in Use  
 0%  100%

Packet Direction: WAN to LAN  
 Default Policy: Drop, Log

#	Name	Active	Source Address	Destination Address	Service Type	Action	Sch.	Log	Modify
1	Ex1	Y	Any	10.0.0.10 - 10.0.0.15	*My Service(TCP/UDP:123)	Permit	No	No	
2	W2L_Rule_1	N	Any	Any	BOOTP_CLIENT(UDP:68)	Permit	No	No	
3	W2L_Rule_2	N	Any	Any	NetBIOS(TCP/UDP:137~139,445)	Permit	No	No	

Insert new rule before rule  (rule number)  
 Move rule  to rule  (rule number)

Rule 1: Allows a My Service connection from the WAN to IP addresses 10.0.0.10 through 10.0.0.15 on the LAN.

# CHAPTER 12

## Intrusion Detection and Prevention (IDP)

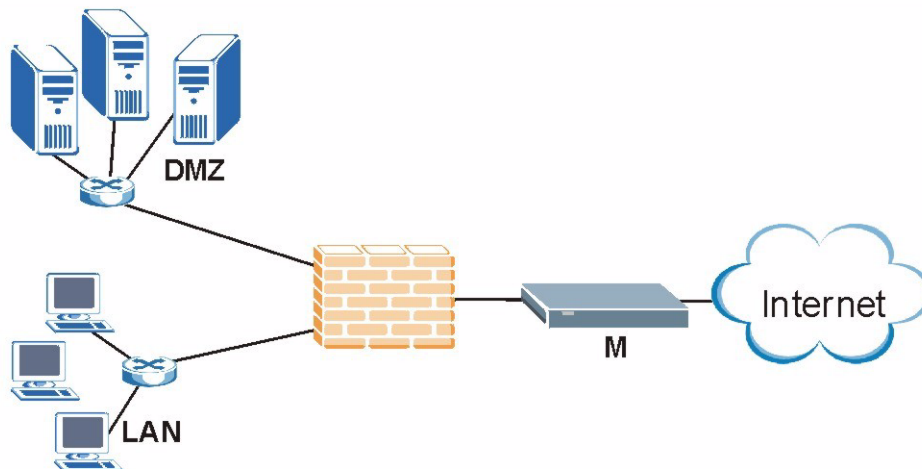
This chapter introduces some background information on IDP. Skip to the next chapter to see how to configure IDP on your ZyWALL.

### 12.1 Introduction to IDP

An IDP system can detect malicious or suspicious packets and respond instantaneously. It can detect anomalies based on violations of protocol standards (RFCs – Requests for Comments) or traffic flows and abnormal flows such as port scans.

[Figure 110 on page 240](#) represents a typical business network consisting of a LAN, a DMZ (DeMilitarized Zone) containing the company web, FTP, mail servers etc., a firewall and/or NAT router connected to a broadband modem (M) for Internet access.

**Figure 110** Network Intrusions



#### 12.1.1 Firewalls and Intrusions

Firewalls are designed to block clearly suspicious traffic and forward other traffic through. Many exploits take advantage of weaknesses in the protocols that are allowed through the firewall, so that once an inside server has been compromised it can be used as a backdoor to launch attacks on other servers.

Firewalls are usually deployed at the network edge. However, many attacks (inadvertently) are launched from within an organization. Virtual private networks (VPN), removable storage devices and wireless networks may all provide access to the internal network without going through the firewall.

### 12.1.2 IDS and IDP

An Intrusion Detection System (IDS) can detect suspicious activity, but does not take action against attacks. On the other hand an IDP is a proactive defense mechanisms designed to detect malicious packets within normal network traffic and take an action (block, drop, log, send an alert) against the offending traffic automatically before it does any damage. An IDS only raises an alert after the malicious payload has been delivered. Worms such as Slammer and Blaster have such fast proliferation speeds that by the time an alert is generated, the damage is already done and spreading fast.

There are two main categories of IDP; Host IDP and Network IDP.

### 12.1.3 Host IDP

The goal of host-based intrusions is to infiltrate files on an individual computer or server in with the goal of accessing confidential information or destroying information on a computer.

You must install Host IDP directly on the system being protected. It works closely with the operating system, monitoring and intercepting system calls to the kernel or APIs in order to prevent attacks as well as log them.

Disadvantages of host IDPs are that you have to install them on each device (that you want to protect) in your network and due to the necessarily tight integration with the host operating system, future operating system upgrades could cause problems.

### 12.1.4 Network IDP

Network-based intrusions have the goal of bringing down a network or networks by attacking computer(s), switch(es), router(s) or modem(s). If a LAN switch is compromised for example, then the whole LAN is compromised, resulting in the equivalent of a LAN Denial of Service (DoS) attack. Host-based intrusions may be used to cause network-based intrusions when the goal of the host virus is to propagate attacks on the network, or attack computer/server operating system vulnerabilities with the goal of bringing down the computer/server. Typical “network-based intrusions” are SQL slammer, Blaster, Nimda, MyDoom etc.

A Network IDP has at least two network interfaces, one internal and one external. As packets appear at an interface they are passed to the detection engine, which determines whether they are malicious or not. If a malicious packet is detected, an action is taken. The remaining packets that make up that particular TCP session are also discarded.

## 12.1.5 Example Intrusions

The following are some examples of intrusions.

### 12.1.5.1 SQL Slammer Worm

W32.SQLExp.Worm is a worm that targets the systems running Microsoft SQL Server 2000, as well as Microsoft Desktop Engine (MSDE) 2000. The worm sends 376 bytes to UDP port 1434, the SQL Server Resolution Service Port. The worm has the unintended payload of performing a Denial of Service attack due to the large number of packets it sends. Refer to Microsoft SQL Server 2000 or MSDE 2000 vulnerabilities in *Microsoft Security Bulletin MS02-039* and *Microsoft Security Bulletin MS02-061*.

### 12.1.5.2 Blaster W32.Worm

This is a worm that exploits the DCOM RPC vulnerability (see *Microsoft Security Bulletin MS03-026* and *Microsoft Security Bulletin MS03-039*) using TCP port 135. The worm targets only Windows 2000 and Windows XP machines. While Windows NT and Windows 2003 Server machines are vulnerable (if not properly patched), the worm is not coded to replicate on those systems. This worm attempts to download the msblast.exe file to the %WinDir%\system32 directory and then execute it. W32.Blaster.Worm does not mass mail to other devices.

### 12.1.5.3 Nimda

Its name (backwards for "admin") refers to an "admin.DLL" file that, when run, continues to propagate the virus. Nimda probes each IP address within a randomly selected range of IP addresses, attempting to exploit weaknesses that, unless already patched, are known to exist in computers with Microsoft's Internet Information Server. A system with an exposed IIS Web server will read a Web page containing an embedded JavaScript that automatically executes, causing the same JavaScript code to propagate to all Web pages on that server. As Microsoft Internet Explorer browsers version 5.01 or earlier visit sites at the infected Web server, they unwittingly download pages with the JavaScript code that automatically executes, causing the virus to be sent to other computers on the Internet in a somewhat random fashion. Nimda also can infect users within the Web server's own internal network that have been given a network share (a portion of file space). Finally, one of the things that Nimda has an infected system do is to send an e-mail with a "readme.exe" attachment to the addresses in the local Windows address book. A user who opens or previews this attachment (which is a Web page with the JavaScript) propagates the virus further.

Server administrators should get and apply the cumulative IIS patch that Microsoft has provided for previous viruses and ensure that no one at the server opens e-mail. You should update your Internet Explorer version to IE 5.5 SP2 or later. Scan and cleanse your system with anti-virus software.

#### 12.1.5.4 MyDoom

MyDoom W32.Mydoom.A@mm (also known as W32.Novarg.A) is a mass-mailing worm that arrives as an attachment with an bat, cmd, exe, pif, scr, or zip file extension. When a computer is infected, the worm sets up a backdoor into the system by opening TCP ports 3127 through 3198, which can potentially allow an attacker to connect to the computer and use it as a proxy to gain access to its network resources. In addition, the backdoor can download and execute arbitrary files. Systems affected are Windows 95, Windows 98, Windows Me, Windows NT, Windows 2000, Windows XP and Windows Server 2003.

W32/MyDoom-A is a worm that is spread by email. When the infected attachment is launched, the worm gathers e-mail addresses from address books and from files with the following extensions: WAB, TXT, HTM, SHT, PHP, ASP, DBX, TBB, ADB and PL. W32/MyDoom-A creates a file called Message in the temp folder and runs Notepad to display the contents, which displays random characters. W32/MyDoom-A creates randomly chosen email addresses in the "To:" and "From:" fields as well as a randomly chosen subject line. Attached files will have an extension of BAT, CMD, EXE, PIF, SCR or ZIP.

#### 12.1.6 ZyWALL IDP

The ZyWALL Internet Security Appliance is designed to protect against network-based intrusions. See [Section 13.2 on page 245](#) for more information on how to apply IDP to ZyWALL interfaces.

IDP is regularly updated by the ZyXEL Security Response Team (ZSRT). Regular updates are vital as new intrusions evolve.

# CHAPTER 13

## Configuring IDP

This chapter shows you how to configure IDP on the ZyWALL.

### 13.1 Overview

To use IDP on the ZyWALL, you need to insert the ZyWALL Turbo Card into the rear panel slot of the ZyWALL. See the ZyWALL Turbo Card guide for details.

**Note:** The ZyWALL has no wireless capability when ZyWALL Turbo Card is in place.

The ZyWALL Turbo Card does not have a MAC address.

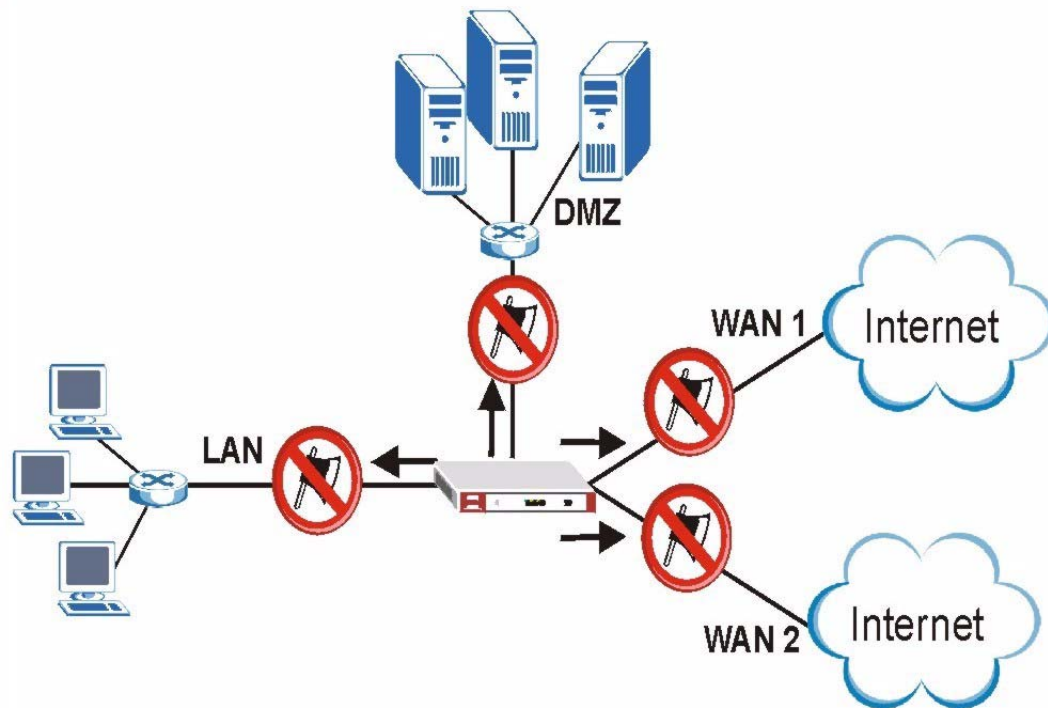
IDP cannot check encrypted traffic such as VPN tunnel traffic.

#### 13.1.1 Interfaces

The ZyWALL checks traffic going out from the ZyWALL to the interface(s) you specify for signature matches.

If a packet matches a signature, the action specified by the signature is taken. You can change the default signature actions in the **Signatures** screen.

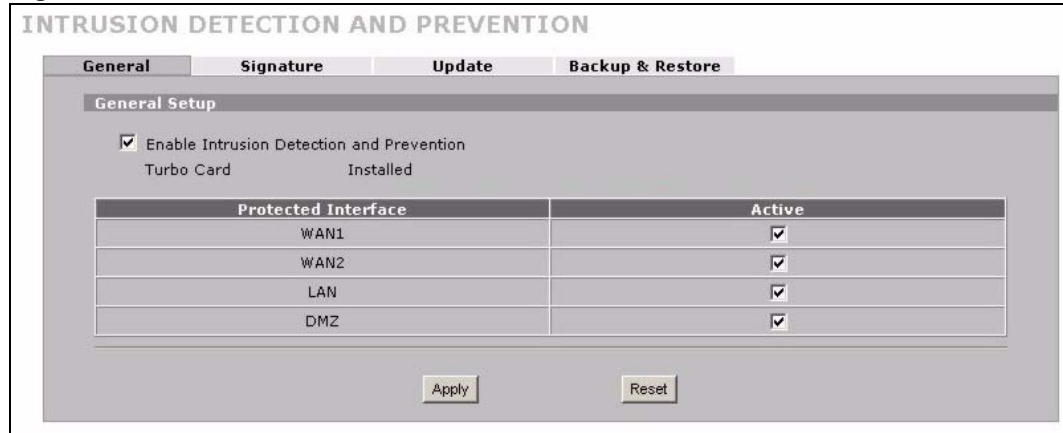


**Figure 111** Applying IDP to Interfaces

## 13.2 General Setup

Use this screen to enable IDP on the ZyWALL and choose what interface(s) you want to protect from intrusions.

Click **IDP** from the navigation panel. **General** is the first screen as shown in the following figure.

**Figure 112** IDP: General

The following table describes the labels in this screen.

**Table 76** IDP: General Setup

LABEL	DESCRIPTION
General Setup	
Enable Intrusion Detection and Protection	Select this check box to enable IDP on the ZyWALL. When this check box is cleared the ZyWALL is in IDP “bypass” mode and no IDP checking is done.
Turbo Card	This field displays whether or not a ZyWALL Turbo Card is installed.  <b>Note:</b> You cannot configure and save the IDP and Anti-Virus screens if the ZyWALL Turbo Card is not installed.
Protected Interface	Select the <b>Active</b> check box to apply IDP to the corresponding interface. Traffic going from the ZyWALL out through this interface is then checked against the signature database for possible intrusions. For example, if you want to protect the LAN computers from intrusions, select the <b>LAN</b> interface.
Apply	Click this button to save your changes back to the ZyWALL.
Reset	Click this button to begin configuring this screen afresh.

## 13.3 IDP Signatures

The rules that define how to identify and respond to intrusions are called “signatures”. Click **IDP** in the navigation panel and then click the **Signatures** tab to see the ZyWALL’s signatures.

### 13.3.1 Attack Types

Click **IDP** in the navigation panel and then select the **Signatures** tab. The **Attack Type** list box displays all intrusion types supported by the ZyWALL. **Other** covers all intrusion types not covered by other types listed.

To see signatures listed by intrusion type supported by the ZyWALL, select that type from the **Attack Type** list box.

**Figure 113** Attack Types



The following table describes each attack type.

**Table 77** Attack Types

TYPE	DESCRIPTION
DoS/DDoS	The goal of Denial of Service (DoS) attacks is not to steal information, but to disable a device or network on the Internet. A distributed denial-of-service (DDoS) attack is one in which multiple compromised systems attack a single target, thereby causing denial of service for users of the targeted system.
Buffer Overflow	A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. The excess information can overflow into adjacent buffers, corrupting or overwriting the valid data held in them.  Intruders could run codes in the overflow buffer region to obtain control of the system, install a backdoor or use the victim to launch attacks on other devices.
Access Control	Access control refers to procedures and controls that limit or detect access. Access control is used typically to control user access to network resources such as servers, directories, and files.
Scan	Scan refers to all port, IP or vulnerability scans. Hackers scan ports to find targets. They may use a TCP connect() call, SYN scanning (half-open scanning), Nmap etc. After a target has been found, a vulnerability scanner can be used to exploit exposures.
Trojan Horse	A Trojan horse is a harmful program that's hidden inside apparently harmless programs or data. It could be used to steal information or remotely control a device.
P2P	Peer-to-peer (P2P) is where computing devices link directly to each other and can directly initiate communication with each other; they do not need an intermediary. A device can be both the client and the server. In the ZyWALL, P2P refers to peer-to-peer applications such as eMule, eDonkey, BitTorrent, iMesh etc.
IM	IM (Instant Messaging) refers to chat applications. Chat is real-time communication between two or more users via networks-connected computers. After you enter a chat (or chat room), any member can type a message that will appear on the monitors of all the other participants.

**Table 77** Attack Types (continued)

TYPE	DESCRIPTION
Virus/Worm	A computer virus is a small program designed to corrupt and/or alter the operation of other legitimate programs. A worm is a program that is designed to copy itself from one computer to another on a network. A worm's uncontrolled replication consumes system resources thus slowing or stopping other tasks.  The IDP VirusWorm category refers to network-based viruses and worms. The Anti-Virus (AV) screen refers to file-based viruses and worms. Refer to the anti-virus chapter for additional information on file-based anti-virus scanning in the ZyWALL.
Porn	The ZyWALL can block web sites if their URLs contain certain pornographic words. It cannot block web pages containing those words if the associated URL does not.
Web Attack	Web attack signatures refer to attacks on web servers such as IIS (Internet Information Services).
SPAM	Spam is unsolicited "junk" e-mail sent to large numbers of people to promote products or services. Refer to the anti-spam chapter for more detailed information.
Other	This category refers to signatures for attacks that do not fall into the previously mentioned categories.

### 13.3.2 Intrusion Severity

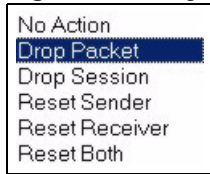
Intrusions are assigned a severity level based on the following table. The intrusion severity level then determines the default signature action.

**Table 78** Intrusion Severity

SEVERITY	DESCRIPTION
Severe	These are intrusions that try to run arbitrary code or gain system privileges.
High	These are known serious vulnerabilities or intrusions that are probably not false alarms.
Medium	These are medium threats, access control intrusions or intrusions that could be false alarms.
Low	These are mild threats or intrusions that could be false alarms.
Very Low	These are possible intrusions caused by traffic such as Ping, trace route, ICMP queries etc.

### 13.3.3 Signature Actions

You can enable/disable individual signatures. You can log and/or have an alert sent when traffic meets a signature criteria. You can also change the default action to be taken when a packet or stream matches a signature. The following figure and table describes these actions. Note that in addition to these actions, a log may be generated or an alert sent, if those check boxes are selected and the signature is enabled.

**Figure 114** Signature Actions

The following table describes signature actions.

**Table 79** Signature Actions

ACTION	DESCRIPTION
No Action	The intrusion is detected but no action is taken.
Drop Packet	The packet is silently discarded.
Drop Session	When the firewall is enabled, subsequent TCP/IP packets belonging to the same connection are dropped. Neither sender nor receiver are sent TCP RST packets. If the firewall is not enabled only the packet that matched the signature is dropped.
Reset Sender	When the firewall is enabled, the TCP/IP connection is silently torn down. Just the sender is sent TCP RST packets. If the firewall is not enabled only the packet that matched the signature is dropped.
Reset Receiver	When the firewall is enabled, the TCP/IP connection is silently torn down. Just the receiver is sent TCP RST packets. If the firewall is not enabled only the packet that matched the signature is dropped.
Reset Both	When the firewall is enabled, the TCP/IP connection is silently torn down. Both sender and receiver are sent TCP RST packets. If the firewall is not enabled only the packet that matched the signature is dropped.

### 13.3.4 Configuring IDP Signatures


Click **IDP** in the navigation panel and then click the **Signatures** tab to see the ZyWALL's "group view" signature screen where you can view signatures by attack type. To search for signatures based on other criteria such as signature name or ID, then click the **Switch to query view** link to go to the "query view" screen.

You can take actions on these signatures as described in [Section 13.3.3 on page 248](#). To revert to the default actions or to save sets of actions, go to the **Backup & Restore** screen.

**Figure 115** IDP: Signatures

The following table describes the labels in this screen.

**Table 80** IDP Signatures: Group View

LABEL	DESCRIPTION
Signature Groups	
Attack Type	Select the type of signatures you want to view from the list box. See <a href="#">Section 13.3.1 on page 246</a> for information on types of signatures.
Switch to query view	Click this hyperlink to go to a screen where you can search for signatures based on criteria other than attack type.
Name	The (read-only) signature name identifies a specific signature targeted at a specific intrusion. Click the hyperlink for more detailed information on the intrusion.
ID	Each intrusion has a unique identification number. This number may be searched at myZyXEL.com for more detailed information.
Severity	This field displays the level of threat that the intrusion may pose. See <a href="#">Table 78 on page 248</a> for more information on intrusion severity.
Platform	This field displays the computer or network device operating system that the intrusion targets or is vulnerable to the intrusion. These icons represent a Windows operating system, a UNIX-based operating system and a network device respectively. 
Active	Select the check box in the heading row to automatically select all check boxes and enable all signatures. Clear it to clear all entries and disable all signatures on the current page. For example, you could clear all check boxes for signatures that targets operating systems not in your network. This would speed up the IDP signature checking process. Alternatively, you may select or clear individual entries. The check box becomes gray when you select the check box. If you edited any of the check boxes in this column on the current page, use the check box in the heading row to switch between the settings (last partial edited, all selected and all cleared).

**Table 80** IDP Signatures: Group View (continued)

LABEL	DESCRIPTION
Log	<p>Select this check box to have a log generated when a match is found for a signature.</p> <p>Select the check box in the heading row to automatically select all check boxes or clear it to clear all entries on the current page.</p> <p>Alternatively, you may select or clear individual entries. The check box becomes gray when you select the check box.</p> <p>If you edited any of the check boxes in this column on the current page, use the check box in the heading row to switch between the settings (last partial edited, all selected and all cleared).</p>
Alert	<p>You can only edit the <b>Alert</b> check box when the corresponding <b>Log</b> check box is selected.</p> <p>Select this check box to have an e-mail sent when a match is found for a signature.</p> <p>Select the check box in the heading row to automatically select all check boxes or clear it to clear all entries on the current page.</p> <p>Alternatively, you may select or clear individual entries. The check box becomes gray when you select the check box.</p> <p>If you edited any of the check boxes in this column on the current page, use the check box in the heading row to switch between the settings (last partial edited, all selected and all cleared).</p>
Action	<p>You can change the default signature action here. See <a href="#">Table 79 on page 249</a> for more details on actions.</p>
Apply	<p>Click this button to save your changes back to the ZyWALL.</p>
Reset	<p>Click this button to begin configuring this screen afresh.</p>

### 13.3.5 Query View

Click **IDP** in the navigation panel and then click the **Signatures** tab to see the ZyWALL's "group view" signature screen, then click the **Switch to query view** link to go to this "query view" screen.

In this screen you can search for signatures based on:

- Signature name or ID or
- Severity, category (type), target operating system and by type of signature action such as active, log, alert and action as shown in the next two screen examples.

#### 13.3.5.1 Query Example 1

- 1 From the "group view" signature screen, click the **Switch to query view** link.
- 1 Select **Signature Search**.
- 2 Select **By Name** or **By ID** from the list box.
- 3 Enter a name (complete or partial) or complete ID to display all relevant signatures in the signature database.

**Note:** A partial name may be searched but a complete ID number must be entered before a match can be found. For example, a search by name for “w” (in the first example) finds all intrusions that contain this letter in the name field. However a search by ID for “1” would return no match. You must enter the complete ID as shown in the second example.

- 4 Click **Search**. If the search finds more signatures than can be displayed on one page, use the **Go to Page** list box to view other pages of signatures found in the search.
- 5 If you change the **Active**, **Log**, **Alert** and/or **Action** signature fields in the signatures found, then click **Apply** to save the changes to the ZyWALL.

**Figure 116** Signature Query by Partial Name

The screenshot displays the 'INTRUSION DETECTION AND PREVENTION' configuration page, specifically the 'Signature' tab. The interface is divided into two main sections: 'Query Signatures' and 'Configure Signatures'.

**Query Signatures:** This section allows for searching through various attributes. The 'Signature Search' option is selected, with 'By Name' chosen as the search criteria and 'xy' entered in the search box. Below this, there are several dropdown menus for filtering signatures based on Severity (Any, Severe, High, Medium, Low), Type (Any, DDOS, Buffer Overflow, Access Control, Scan), Platform (Any, Windows, Linux/Unix, Network device), Active (Any, Active, Inactive), Log (Any, Log, No Log), Alert (Any, Alert, No Alert), and Action (Any, No Action, Drop Packet, Drop Session, Reset Sender). A 'Search' button is located below these filters.

**Configure Signatures:** This section displays a table of search results. The table has columns for Name, ID, Severity, Type, Platform, Active, Log, Alert, and Action. Two signatures are listed:

Name	ID	Severity	Type	Platform	Active	Log	Alert	Action
<a href="#">SCAN SOCKS Proxy attempt</a>	1049159	Low	Scan	UNIX	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No Action
<a href="#">EXPLOIT delegate proxy overflow</a>	1048818	Severe	BufferOverflow	UNIX	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Drop Session

At the bottom of the 'Configure Signatures' section, there are 'Apply' and 'Reset' buttons.



**Figure 117** Signature Query by Complete ID

**INTRUSION DETECTION AND PREVENTION**

General **Signature** Update Backup & Restore

Query Signatures [Back to group view](#)

Signature Search By ID 
  
 Signature Search by Attributes.

Hold 'Ctrl' to make multiple selection on items in the lists:

Severity	Type	Platform	Active	Log	Alert	Action
Any	Any	Any	Any	Any	Any	Any
Severe	DDOS	Windows	Active	Log	Alert	No Action
High	Buffer Overflow	Linux/Unix	Inactive	No Log	No Alert	Drop Packet
Medium	Access Control	Network device				Drop Session
Low	Scan					Reset Sender

Search

Configure Signatures

Name	ID	Severity	Type	Platform	Active	Log	Alert	Action
<a href="#">TELNET root login</a>	1049263	Medium	AccessControl	UNIX	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No Action

Apply Reset

### 13.3.5.2 Query Example 2

- 1 From the “group view” signature screen, click the **Switch to query view** link.
- 1 Select **Signature Search By Attributes**.
- 2 Select the **Severity**, **Type**, **Platform**, **Active**, **Log**, **Alert** and/or **Action** items. In this example all severe **DDoS** type signatures that target the Windows operating system are displayed.
- 3 Click **Search**.

If you change the **Active**, **Log**, **Alert** and/or **Action** signature fields in the signatures found, then click **Apply** to save the changes to the ZyWALL.

**Figure 118** Signature Query by Attribute.

**INTRUSION DETECTION AND PREVENTION**

General Signature Update Backup & Restore

Query Signatures [Back to group view](#)

Signature Search By Name   
 Signature Search by Attributes.  
 Hold 'Ctrl' to make multiple selection on items in the lists:

Severity	Type	Platform	Active	Log	Alert	Action
Any	Any	Any	Any	Any	Any	Any
Severe	DDOS	Windows	Active	Log	Alert	No Action
High	Buffer Overflow	Linux/Unix	Inactive	No Log	No Alert	Drop Packet
Medium	Access Control	Network device				Drop Session
Low	Scan					Reset Sender

Search

Configure Signatures

Name	ID	Severity	Type	Platform	Active	Log	Alert	Action
<a href="#">DoS_MS-SQL_Slammer_Worm</a>	1050295	Severe	DDOS	Windows	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Drop Packet

Apply Reset

## 13.4 Update

The ZyWALL comes with built-in signatures created by the ZyXEL Security Response Team (ZSRT). These are regularly updated as new intrusions evolve. Use the **Update** screen to immediately download or schedule new signature downloads.

**Note:** You should have already registered the ZyWALL at myZyXEL.com (<http://www.myzyxel.com/myzyxel/>) and also have either activated the trial license or standard license (iCard). If your license has expired, you will have to renew it before updates are allowed.

### 13.4.1 mySecurity Zone

mySecurityZone is a web portal that provides all security-related information such as intrusion and anti-virus information for ZyXEL security products.

Click the intrusion **ID** hyperlink to go directly to information on that signature or enter <https://mysecurity.zyxel.com/mysecurity/> as the URL in your web browser.

You should have already registered your ZyWALL on myZyXEL.com at:

<http://www.myzyxel.com/myzyxel/>.

You can use your myZyXEL.com username and password to log into mySecurity Zone.

## 13.4.2 Configuring IDP Update

When scheduling signature updates, you should choose a day and time when your network is least busy so as to minimize disruption to your network. Your custom signature configurations are not over-written when you download new signatures.

File-based anti-virus signatures (see the anti-virus chapter) are included with IDP signatures. When you download new signatures using the anti-virus **Update** screen, IDP signatures are also downloaded. The version number changes both in the anti-virus **Update** screen and this screen. Both screens also share the same **Auto-Update** schedule. Changes made to the schedule in one screen are reflected in the other.

**Note:** The ZyWALL does not have to reboot when you upload new signatures.

Click **IDP** from the navigation panel and then click the **Update** tab.

**Figure 119** Signatures Update

The screenshot shows the 'INTRUSION DETECTION AND PREVENTION' configuration page, specifically the 'Update' tab. The page is divided into two main sections: 'Signature Information' and 'Signature Update'. The 'Signature Information' section displays the following details: Current Pattern Version: v1.004, Release Date: 2005-07-27 07:21:41, Last Update: 2005-07-28 15:27:55, and Current IDP Signatures: 1723. The 'Signature Update' section shows the Service Status as 'License Active' and the Expiration Date as '2007-01-22'. It includes a note to 'Synchronize the IDP and Anti-Virus Signature to the latest version with the online update server.' Below this, the 'Update Server' is set to 'myupdate.zywall.zyxel.com' with an 'Update Now' button. The 'Auto Update' section is checked, with radio buttons for 'Hourly', 'Daily', and 'Weekly'. The 'Daily' option is selected, with a dropdown menu set to '0' (O'clock). The 'Weekly' option is also visible, with a dropdown menu set to 'Sunday' and another dropdown set to '0' (O'clock). At the bottom of the page, there are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

**Table 81** Signatures Update

LABEL	DESCRIPTION
Signature Information	
Current Pattern Version	This field displays the signatures version number currently used by the ZyWALL. This number is defined by the ZyXEL Security Response Team (ZSRT) who maintain and update them.  This number increments as new signatures are added, so you should refer to this number regularly. Go to <a href="https://mysecurity.zyxel.com/mysecurity/">https://mysecurity.zyxel.com/mysecurity/</a> to see what the latest version number is. You can also subscribe to signature update e-mail notifications.
Release Date	This field displays the time (hour, minutes second) and date (month, date, year) that the above signature set was created.
Last Update	This field displays the last date and time you downloaded new signatures to the ZyWALL. It displays <b>N/A</b> if you have not downloaded any new signatures yet.
Current IDP Signatures	This field displays the number of IDP-related signatures.
Signature Update	
Service Status	This field displays <b>License Inactive</b> if you have not yet activated your trial or iCard license at myZyXEL.com.  It displays <b>License Inactive</b> and an expiration date if your trial or iCard license has expired (the expiration date is the date it expired).  It displays <b>Trial Active</b> and an expiration date when you have activated your trial license.  It displays <b>License Active</b> and an expiration date when you have activated your iCard license (the expiration date is the date it will expire).
Update Server	This is the URL of the signature server from which you download signatures. The default server at the time of writing is displayed as shown in the screen.
Update Now	Click this button to begin downloading signatures from the <b>Update Server</b> immediately.
Auto Update	Select the check box to configure a schedule for automatic signature updates. The <b>Hourly</b> , <b>Daily</b> and <b>Weekly</b> fields display when the check box is selected. The ZyWALL then automatically downloads signatures from the <b>Update Server</b> regularly at the time and/or day you specify.
Hourly	Select this option to have the ZyWALL check the update server for new signatures every hour. This may be advisable when new intrusions are currently spreading throughout the Internet.
Daily	Select this option to have the ZyWALL check the update server for new signatures every day at the hour you select from the list box. The ZyWALL uses a 24-hour clock. For example, choose 15 from the <b>O'clock</b> list box to have the ZyWALL check the update server for new signatures at 3 PM every day.
Weekly	Select this option to have the ZyWALL check the update server for new signatures once a week on the day and hour you select from the list boxes. The ZyWALL uses a 24-hour clock, so for example, choose <b>Wednesday</b> and 15 from the respective list boxes to have the ZyWALL check the update server for new signatures at 3PM every Wednesday.
Apply	Click this button to save your changes back to the ZyWALL.
Reset	Click this button to close this screen without saving any changes.

## 13.5 Backup and Restore

You can change the pre-defined **Active**, **Log**, **Alert** and/or **Action** settings of individual signatures.

**Figure 120** IDP: Backup & Restore

The screenshot shows the 'INTRUSION DETECTION AND PREVENTION' configuration interface. At the top, there are four tabs: 'General', 'Signature', 'Update', and 'Backup & Restore'. The 'Backup & Restore' tab is selected. The screen is divided into three sections:

- Backup Configuration:** Contains the instruction 'Click Backup to save the current configuration of IDP to your computer.' and a 'Backup' button.
- Restore Configuration:** Contains the instruction 'To restore a previously saved IDP configuration file to your system, browse to the configuration file and click Upload.' Below this is a 'File Path' input field with a 'Browse...' button, and an 'Upload' button.
- Back to Factory Defaults:** Contains the instruction 'Click Reset to clear all user-entered IDP configuration information and return to factory defaults.' and a 'Reset' button.

Use the **Backup & Restore** screen to:

- Back up IDP signatures with your custom configured settings. Click **Backup** and then choose a location and filename for the IDP configuration set.
- Restore previously saved IDP signatures (with your custom configured settings). Click **Restore** and choose the path and location where the previously saved file resides on your computer.
- Revert to the original ZSRT-defined signature **Active**, **Log**, **Alert** and/or **Action** settings. Click **Reset**.

# CHAPTER 14

## Anti-Virus

This chapter introduces and shows you how to configure the anti-virus scanner.

### 14.1 Anti-Virus Overview

A computer virus is a small program designed to corrupt and/or alter the operation of other legitimate programs. A worm is a self-replicating virus that resides in active memory and duplicates itself. The effect of a virus attack varies from doing so little damage that you are unaware your computer is infected to wiping out the entire contents of a hard drive to rendering your computer inoperable.

#### 14.1.1 Types of Computer Viruses

The following table describes some of the common computer viruses.

**Table 82** Common Computer Virus Types

TYPE	DESCRIPTION
File Infector	This is a small program that embeds itself in a legitimate program. A file infector is able to copy and attach itself to other programs that are executed on an infected computer.
Boot Sector Virus	This type of virus infects the area of a hard drive that a computer reads and executes during startup. The virus causes computer crashes and to some extent renders the infected computer inoperable.
Macro Virus	Macro viruses or Macros are small programs that are created to perform repetitive actions. Macros run automatically when a file to which they are attached is opened. Macros spread more rapidly than other types of viruses as data files are often shared on a network.
E-mail Virus	E-mail viruses are malicious programs that spread through e-mail.
Polyphormic Virus	A polymorphic virus (also known as a mutation virus) tries to evade detection by changing a portion of its code structure after each execution or self replication. This makes it harder for an anti-virus scanner to detect or intercept it. A polymorphic virus can also belong to any of the virus types discussed above.

#### 14.1.2 Computer Virus Infection and Prevention

The following describes a simple life cycle of a computer virus.

- 1 A computer gets a copy of a virus from a source such as the Internet, e-mail, file sharing or any removable storage media. The virus is harmless until the execution of an infected program.

- 2 The virus spreads to other files and programs on the computer.
- 3 The infected files are unintentionally sent to another computer thus starting the spread of the virus.
- 4 Once the virus is spread through the network, the number of infected networked computers can grow exponentially.

### 14.1.3 Types of Anti-Virus Scanner

The section describes two types of anti-virus scanner: host-based and network-based.

A host-based anti-virus (HAV) scanner is often software installed on computers and/or servers in the network. It inspects files for virus patterns as they are moved in and out of the hard drive. However, host-based anti-virus scanners cannot eliminate all viruses for a number of reasons:

- HAV scanners are slow in stopping virus threats through real-time traffic (such as from the Internet).
- HAV scanners may reduce computing performance as they also share the resources (such as CPU time) on the computer for file inspection.
- You have to update the virus signatures and/or perform virus scans on all computers in the network regularly.

A network-based anti-virus (NAV) scanner is often deployed as a dedicated security device (such as your ZyWALL) on the network edge. NAV scanners inspect real-time data traffic (such as E-mail messages or web) that tends to bypass HAV scanners. The following lists some of the benefits of NAV scanners.

- NAV scanners stops virus threats at the network edge before they enter or exit a network.
- NAV scanners reduce computing loading on computers as the read-time data traffic inspection is done on a dedicated security device.

## 14.2 Introduction to the ZyWALL Anti-Virus Scanner

The ZyWALL has a built-in signature database. Setting up the ZyWALL between your local network and the Internet allows the ZyWALL to scan files transmitting through the enabled interfaces into your network. As a network-based anti-virus scanner, the ZyWALL helps stop threats at the network edge before they reach the local host computers.

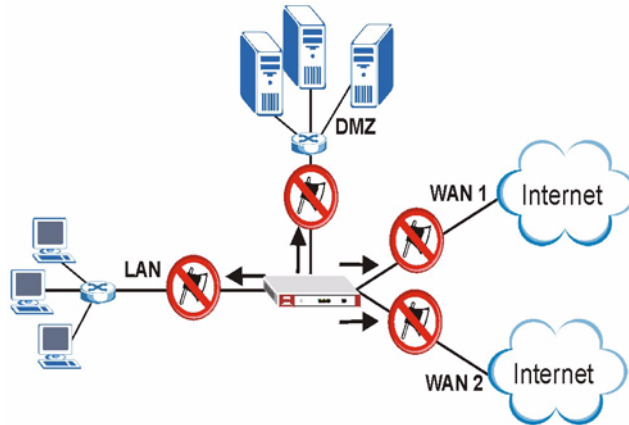
You can set the ZyWALL to examine files received through the following protocols:

- FTP (File Transfer Protocol)
- HTTP (Hyper Text Transfer Protocol)
- SMTP (Simple Mail Transfer Protocol)
- POP3 (Post Office Protocol version 3)

## 14.2.1 How the ZyWALL Anti-Virus Scanner Works

The ZyWALL checks traffic going to the interface(s) you specify for signature matches.

**Figure 121** ZyWALL Anti-virus Example



The following describes the virus scanning process on the ZyWALL.

- 1 The ZyWALL first identifies SMTP, POP3, HTTP and FTP packets through standard ports.
- 2 If the packets are not session connection setup packets (such as SYN, ACK and FIN), the ZyWALL records the sequence of the packets.
- 3 The scanning engine checks the contents of the packets for virus.
- 4 If a virus pattern is matched, the ZyWALL “destroys” the file by removing the infected portion of the file.
- 5 If the send alert message function is enabled, the ZyWALL sends an alert to the file’s intended destination computer(s).

**Note:** Since the ZyWALL erases the infected portion of the file before sending it, you may not be able to open the file.

## 14.2.2 Notes About the ZyWALL Anti-Virus

To use the anti-virus scanner on the ZyWALL, you need to insert the ZyWALL Turbo Card into the rear panel slot of the ZyWALL. See the ZyWALL Turbo Card guide for details.

**Note:** The ZyWALL has no wireless capability when the ZyWALL Turbo Card is in place.

The ZyWALL Turbo Card does not have a MAC address.

The following lists important notes about the anti-virus scanner:

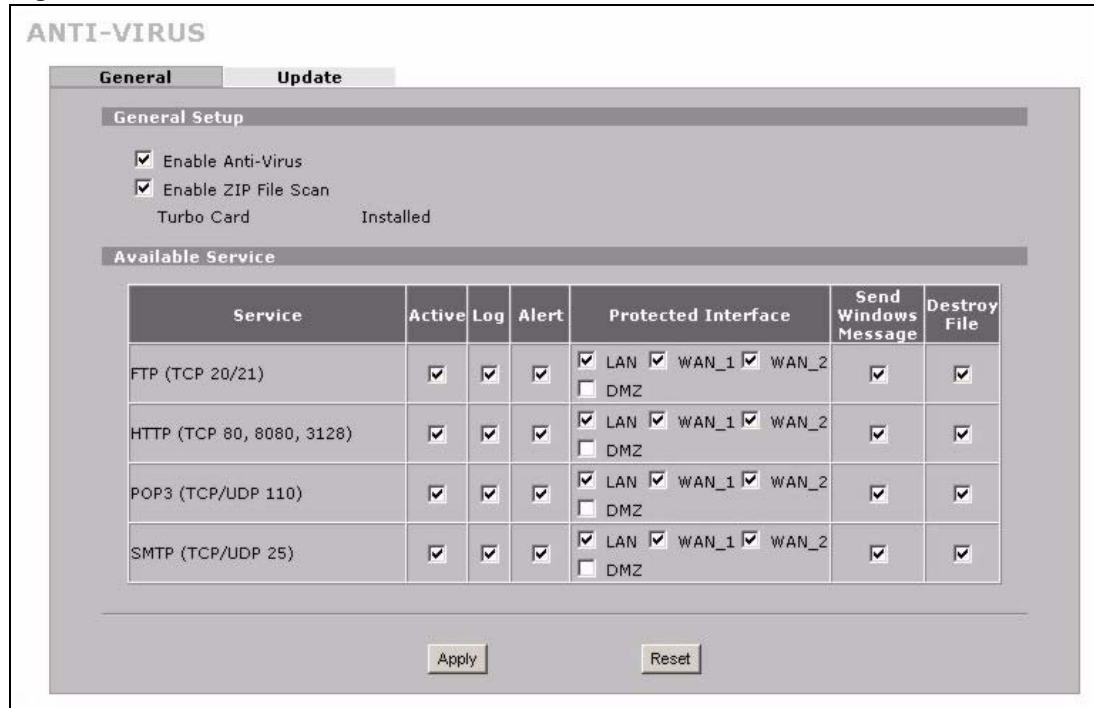


- 1 The ZyWALL anti-virus scanner cannot detect polymorphic viruses.
- 2 The ZyWALL does not scan the following file/traffic types:
  - Simultaneous downloads of a file using multiple connections. For example, when you use FlashGet to download sections of a file simultaneously.
  - Encrypted traffic (such as on a VPN) or password-protected files.
  - Traffic through custom (none-standard) ports.
  - ZIP file(s) within a ZIP file.
- 3 When a virus is detected, an alert message is displayed in Microsoft Windows computers.<sup>2</sup>

### 14.3 General Anti-Virus Setup

Click **SECURITY, ANTI-VIRUS** to display the configuration screen as shown next.

**Figure 122** Anti-Virus: General



2. For Windows 98/Me, refer to the [Appendix J on page 726](#) for requirements.

The following table describes the labels in this screen.

**Table 83** Anti-Virus: General

LABEL	DESCRIPTION
General Setup	
Enable Anti-Virus	<p>Select <b>Enable Anti-Virus</b> to activate the anti-virus feature on the ZyWALL. Clear this check box to disable it.</p> <p><b>Note:</b> Before you use the anti-virus feature, you must register for the service (refer to the chapter on registration for more information).</p>
Enable ZIP File Scan	<p>Select this check box to have the ZyWALL scan a ZIP file (with the “zip” or “gzip” file extension). The ZyWALL first decompresses the ZIP file and then scans the contents for viruses.</p> <p><b>Note:</b> The ZyWALL decompresses a ZIP file once. The ZyWALL does NOT decompress any ZIP file(s) within the ZIP file.</p>
Turbo Card	<p>This field displays whether or not a ZyWALL Turbo Card is installed.</p> <p><b>Note:</b> You cannot configure and save the IDP and Anti-Virus screens if the ZyWALL Turbo Card is not installed.</p>
Available Service	
Service	This field displays the service names and standard port numbers that identify them.
Active	Select <b>Active</b> to enable anti-virus scanner for the corresponding service.
Log	Select <b>Log</b> to create a log when a virus is detected.
Alert	<p>This field is applicable only when you select <b>Log</b>.</p> <p>Select <b>Alert</b> to create an alert when a virus is detected.</p>
Protected Interface	<p>Select the interface(s) where you want the ZyWALL to scan files for viruses. Choices are <b>LAN</b>, <b>WAN</b> (or <b>WAN1</b>, <b>WAN2</b>) and <b>DMZ</b>.</p>
Send Windows Message	Select this check box to set the ZyWALL to send a message alert to files' intended user(s) using Microsoft Windows computer connected to the protected interface.
Destroy File	Select this check box to set the ZyWALL to erase the infected portion of the file before sending it. Once destroyed, you may not be able to open the file.
Apply	Click <b>Apply</b> to save your changes.
Reset	Click <b>Reset</b> to start configuring this screen again.

## 14.4 Signature Update

The ZyWALL comes with built-in signatures created by the ZyXEL Security Response Team (ZSRT). These are regularly updated as new intrusions evolve. Use the **Update** screen to immediately download or schedule new signature downloads.

**Note:** You should have already registered the ZyWALL at myZyXEL.com (<http://www.myzyxel.com/myzyxel/>) and also have either activated the trial license or standard license (iCard). If your license has expired, you will have to renew it before updates are allowed.

### 14.4.1 mySecurity Zone

mySecurity Zone is a web portal that provides all security-related information such as intrusion and anti-virus information for ZyXEL security products.

You should have already registered your ZyWALL on myZyXEL.com at:

<http://www.myzyxel.com/myzyxel/>.

You can use your myZyXEL.com username and password to log into mySecurity Zone.

### 14.4.2 Configuring Anti-virus Update

When scheduling signature updates, you should choose a day and time when your network is least busy so as to minimize disruption to your network. Your custom signature configurations are not over-written when you download new signatures.

IDP signatures (see the chapters on IDP) are included with file-based anti-virus signatures. When you download new signatures using the IDP **Update** screen, anti-virus signatures are also downloaded. The version number changes both in the IDP **Update** screen and this screen. Both screens also share the same **Auto-Update** schedule. Changes made to the schedule in one screen are reflected in the other.

**Note:** The ZyWALL does not have to reboot when you upload new signatures.

Click **SECURITY, ANTI-VIRUS** from the navigation panel and then click the **Update** tab.

**Figure 123** Anti-Virus: Update

The following table describes the labels in this screen.

**Table 84** Anti-Virus: Update

LABEL	DESCRIPTION
Signature Information	
Current Pattern Version	This field displays the signatures version number currently used by the ZyWALL. This number is defined by the ZyXEL Security Response Team (ZSRT) who maintain and update them.  This number increments as new signatures are added, so you should refer to this number regularly. Go to <a href="https://mysecurity.zyxel.com/mysecurity/">https://mysecurity.zyxel.com/mysecurity/</a> to see what the latest version number is. You can also subscribe to signature update e-mail notifications.
Release Date	This field displays the time (hour, minutes second) and date (month, date, year) that the above signature set was created.
Last Update	This field displays the last date and time you downloaded new signatures to the ZyWALL. It displays <b>N/A</b> if you have not downloaded any new signatures yet.
Current Anti-Virus Signatures	This field displays the number of Anti-Virus-related signatures.
Signature Update	
Service Status	This field displays <b>License Inactive</b> if you have not yet activated your trial or iCard license at myZyXEL.com.  It displays <b>License Inactive</b> and an expiration date if your trial or iCard license has expired (the expiration date is the date it expired).  It displays <b>Trial Active</b> and an expiration date when you have activated your trial license.  It displays <b>License Active</b> and an expiration date when you have activated your iCard license (the expiration date is the date it will expire).
Update Server	This is the URL of the signature server from which you download signatures. The default server at the time of writing is displayed as shown in the screen.

**Table 84** Anti-Virus: Update (continued)

LABEL	DESCRIPTION
Update Now	Click this button to begin downloading signatures from the <b>Update Server</b> immediately.
Auto Update	Select the check box to configure a schedule for automatic signature updates. The <b>Hourly</b> , <b>Daily</b> and <b>Weekly</b> fields display when the check box is selected. The ZyWALL then automatically downloads signatures from the <b>Update Server</b> regularly at the time and/or day you specify.
Hourly	Select this option to have the ZyWALL check the update server for new signatures every hour. This may be advisable when new viruses are currently spreading throughout the Internet.
Daily	Select this option to have the ZyWALL check the update server for new signatures every day at the hour you select from the list box. The ZyWALL uses a 24-hour clock. For example, choose 15 from the <b>O'clock</b> list box to have the ZyWALL check the update server for new signatures at 3 PM every day.
Weekly	Select this option to have the ZyWALL check the update server for new signatures once a week on the day and hour you select from the list boxes. The ZyWALL uses a 24-hour clock, so for example, choose <b>Wednesday</b> and <b>15</b> from the respective list boxes to have the ZyWALL check the update server for new signatures at 3PM every Wednesday.
Apply	Click this button to save your changes back to the ZyWALL.
Reset	Click this button to close this screen without saving any changes.

# CHAPTER 15

## Anti-Spam

This chapter covers how to use the ZyWALL's anti-spam feature to deal with junk e-mail (spam).

### 15.1 Anti-Spam Overview

The ZyWALL's anti-spam feature identifies unsolicited commercial or junk e-mail (spam). You can set the ZyWALL to mark or discard spam. The ZyWALL can use an anti-spam external database to help identify spam. Use the whitelist to identify legitimate e-mail. Use the blacklist to identify spam e-mail.

#### 15.1.1 Anti-Spam External Database

If an e-mail does not match any of the whitelist or blacklist entries, the ZyWALL calculates a digest (fingerprint ID) of the e-mail and sends it to the anti-spam external database. The anti-spam external database checks the digest against (more than a million) known spam patterns. The anti-spam external database uses the following spam detection engines in checking each e-mail.

- SpamBulk: This engine identifies e-mail that has been sent in bulk or is similar to e-mail that is sent in bulk.
- SpamRepute: This engine checks to see if most people want the e-mail.
- SpamContent: This engine checks to see if the message would generally be considered offensive.
- SpamTricks: This engine checks to see if the e-mail is formatted to be economical for spammers or to circumvent anti-spam rules.

The anti-spam external database then uses a proprietary Bayesian<sup>1</sup> statistical formula to combine the results into one score of how likely the e-mail is to be spam and sends it to the ZyWALL. The possible range for the spam score is 0~100. The closer the score is to 100, the more likely the e-mail is to be spam. You must subscribe to and activate the anti-spam external database service in order to use it (see [Section 15.1.7 on page 270](#) for details).

---

1. Bayesian analysis interprets probabilities as degrees of belief rather than as proportions, frequencies and such. Bayesian analysis frequently uses Bayes' theorem, hence the name.

### 15.1.1.1 SpamBulk Engine

The e-mail fingerprint ID that the ZyWALL generates and sends to the anti-spam external database only includes the parts of the e-mail that are the most difficult for spammers (senders of spam) to change or fake. The anti-spam external database maintains a database of e-mail fingerprint IDs. The anti-spam external database SpamBulk engine then queries the database in analyzing later e-mails.

The SpamBulk Engine also uses Bayesian statistical analysis to detect whether an e-mail is fundamentally the same as a known spam message in spite of a spammer's attempt to disguise it.

### 15.1.1.2 SpamRepute Engine

The SpamRepute engine calculates the reputation of the sender (whether or not most people want to receive the e-mail from this sender).

The SpamRepute engine checks proprietary and third-party databases of known spammer email addresses, domains and IP addresses. The SpamRepute engine also uses Bayesian statistical analysis to detect whether an e-mail is sent from a known in spite of a spammer's attempt to disguise the sender's identity. The anti-spam external database combines all of this data into a SpamRepute Index for calculating the reputation of the sender in order to guard against foreign language spam, fraud and phishing.

### 15.1.1.3 SpamContent Engine

The SpamContent engine examines the e-mail's content to decide if it would generally be considered offensive. The vocabulary design, format and layout are considered as part of thousands of checks on message attributes that include the following.

- To Field
- Subject Field
- Header Fields
- Email Format, Design, and Layout
- Vocabulary, Word Formatting and Word Patterns
- Foreign Language Detection
- SMTP Envelope Content and Analysis
- Country Trace
- Image Layout Classification
- Hyperlink Analysis and Comparison
- Contact Verification

The SpamContent engine parses words into pieces to detect similar vocabulary even if the words do not match exactly. The anti-spam external database also performs Bayesian statistical analysis on the e-mail's content. The engine uses artificial intelligence technology to 'learn' over time, as spam changes.

### 15.1.1.4 SpamTricks Engine

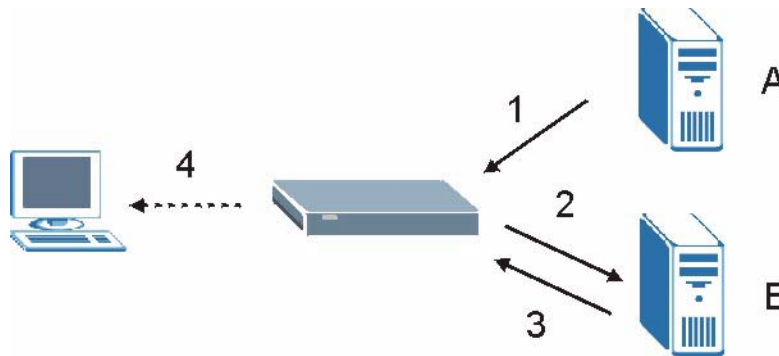
The SpamTricks engine checks for the tactics that spammers use to minimize the expense of sending lots of e-mail and tactics that they use to bypass spam filters.

Use of relays, image-only e-mails, manipulation of mail formats and HTML obfuscation are common tricks for which the SpamTricks engine checks. The SpamTricks engine also checks for “phishing” (see [Section 15.1.3 on page 268](#) for more on phishing).

### 15.1.2 Spam Threshold

You can configure the threshold for what spam score is classified as spam. The ZyWALL considers any e-mail with a spam score higher than the spam threshold to be spam. Any e-mail with a score less than or equal to the spam threshold is treated as legitimate. The following is an example of the ZyWALL checking e-mail with the external database.

**Figure 124** Anti-spam External Database Example



- 1 E-mail comes into the ZyWALL from an e-mail server (A in the figure).
- 2 The ZyWALL calculates a digest of the e-mail and sends it to the anti-spam external database.
- 3 The anti-spam external database calculates a spam score for the e-mail and sends the score back to the ZyWALL.
- 4 The ZyWALL forwards the e-mail if the spam score is at or below the ZyWALL's spam threshold. If the spam score is higher than the spam threshold, the ZyWALL takes the action that you configured for dealing with spam.

### 15.1.3 Phishing

Phishing is a scam where fraudsters send e-mail claiming to be from a well-known enterprise in an attempt to steal private information. For example, the e-mail might appear to be from a bank, online payment service, or even a government agency. It generally tells you to click a link and update your identity information in order for the business or organization to verify your account. The link directs you to a phony website that mimics the business or organization's website. The fraudsters then use your personal information to pretend to be you and commit crimes like running up bills in your name (identity theft).



The anti-spam external database checks for spoofing of e-mail attributes (like the IP address) and uses statistical analysis to detect phishing.

### 15.1.4 Whitelist

Configure whitelist entries to identify legitimate e-mail. The whitelist entries have the ZyWALL classify any e-mail that is from a specified sender or uses a specified MIME (Multipurpose Internet Mail Extensions) header or MIME header value as being legitimate (see [Section 15.1.7 on page 270](#) for more on MIME headers). The anti-spam feature checks an e-mail against the whitelist entries before doing any other anti-spam checking. If the e-mail matches a whitelist entry, the ZyWALL classifies the e-mail as legitimate and does not perform any more anti-spam checking on that individual e-mail. A properly configured whitelist helps keep important e-mail from being incorrectly classified as spam. The whitelist can also increase the ZyWALL's anti-spam speed and efficiency by not having the ZyWALL perform the full anti-spam checking process on legitimate e-mail.

### 15.1.5 Blacklist

Configure blacklist entries to identify spam. The blacklist entries have the ZyWALL classify any e-mail that is from a specified sender or uses a specified MIME (Multipurpose Internet Mail Extensions) header or MIME header value as being spam. If an e-mail does not match any of the whitelist entries, the ZyWALL checks it against the blacklist entries. The ZyWALL classifies an e-mail that matches a blacklist entry as spam and immediately takes the action that you configured for dealing with spam. The ZyWALL does not perform any more anti-spam checking on that individual e-mail. A properly configured blacklist helps catch spam e-mail and increases the ZyWALL's anti-spam speed and efficiency.

### 15.1.6 SMTP and POP3

Simple Mail Transfer Protocol (SMTP) is the Internet's message transport standard. It controls the sending of e-mail messages between servers. E-mail clients (also called e-mail applications) then use mail server protocols such as POP (Post Office Protocol) or IMAP (Internet Message Access Protocol) to retrieve e-mail. E-mail clients also generally use SMTP to send messages to a mail server. The older POP2 requires SMTP for sending messages while the newer POP3 can be used with or without it. This is why many e-mail applications require you to specify both the SMTP server and the POP or IMAP server (even though they may actually be the same server).

The ZyWALL's anti-spam feature checks SMTP (TCP port 25) and POP3 (TCP port 110) e-mails. The anti-spam feature does not check (or act upon) e-mails that use other protocols (such as IMAP) or other port numbers.

## 15.1.7 MIME Headers

MIME (Multipurpose Internet Mail Extensions) allows varied media types to be used in e-mail. MIME headers describe an e-mail's content encoding and type. For example, it may show which program generated the e-mail and what type of text is used in the e-mail body. Here are some examples of MIME headers:

- X-Priority: 3 (Normal)
- X-MSMail-Priority: Normal
- Content-Type: text/plain; charset="iso-8859-1"
- Content-Transfer-Encoding: base64

In an MIME header, the part that comes before the colon (:) is the header. The part that comes after the colon is the value. Spam often has blank header values or comments in them that are part of an attempt to bypass spam filters.

## 15.2 Anti-Spam General Screen

Click **SECURITY, ANTI-SPAM** to open the **Anti-Spam General** screen. Use this screen to turn the anti-spam feature on or off and set how the ZyWALL treats spam.

**Figure 125** Anti-Spam: General

**ANTI-SPAM**

**General** External DB Lists

**General Setup**

Enable Anti-Spam

**Action for Spam Mails**

Phishing Tag [70\_J\_FISH]

Spam Tag [70\_J\_SPAM]

Forward SMTP & POP3 mail with tag in mail subject.

Discard SMTP mail. Forward POP3 mail with tag in mail subject.

**Action taken when mail sessions threshold is reached**

Forward

Block

Apply Reset

The following table describes the labels in this screen.

**Table 85** Anti-Spam: General

LABEL	DESCRIPTION
General Setup	
Enable Anti-spam	<p>Select this check box to enable the anti-spam feature.</p> <p><b>Note:</b> The anti-spam feature checks all SMTP and POP3 e-mail going through the ZyWALL, regardless of through which port the e-mail came in or to which port it is going.</p>
Action for Spam Mails	Use this section to set how the ZyWALL is to handle spam mail.
Phishing Tag	<p>Enter a message or label (up to 16 ASCII characters) to add to the mail subject of e-mails that the anti-spam external database classifies as phishing.</p> <p><b>Note:</b> You must register for and enable the anti-spam external database feature in order for the ZyWALL to use this tag (see Chapter 10 on page 185 for details).</p>
Spam Tag	Enter a message or label (up to 16 ASCII characters) to add to the mail subject of e-mails that the ZyWALL classifies as spam.
Forward SMTP & POP3 mail with tag in mail subject	<p>Select this radio button to have the ZyWALL forward spam e-mail with the tag that you define.</p> <p>Even if you plan to use the discard option, you may want to use this initially as a test to check how accurate your anti-spam settings are. Check the e-mail the ZyWALL forwards to you to make sure that unwanted e-mail is marked as spam and legitimate e-mail is not marked as spam.</p>
Discard SMTP mail. Forward POP3 mail with tag in mail subject	Select this radio button to have the ZyWALL discard spam SMTP e-mail. The ZyWALL will still forward spam POP3 e-mail with the tag that you define.
Action taken when mail sessions threshold is reached	<p>The anti-spam feature limits the number of concurrent e-mail sessions. An e-mail session is when an e-mail client and e-mail server (or two e-mail servers) connect through the ZyWALL. Use this section to configure what the ZyWALL does when the number of concurrent e-mail sessions goes over the threshold (see the appendix of product specifications for the threshold).</p> <p>Select <b>Forward</b> to have the ZyWALL allow the excess e-mail sessions without any spam filtering.</p> <p>Select <b>Block</b> to have the ZyWALL drop mail connections to stop the excess e-mail sessions. The e-mail client or server will have to attempt to send or receive e-mail later when the number of e-mail sessions is under the threshold.</p>
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 15.3 Anti-Spam External DB Screen

Click **SECURITY, ANTI-SPAM, External DB** to display the **Anti-Spam External DB** screen. Use this screen to enable or disable the use of the anti-spam external database. You can also configure the spam threshold and what to do when no valid spam score is received. You must register for this service before you can use it (see [Chapter 4 on page 104](#) for details).

**Figure 126** Anti-Spam: External DB

The following table describes the labels in this screen.

**Table 86** Anti-Spam: External DB

LABEL	DESCRIPTION
External Database	
Enable External Database	Enable the anti-spam external database feature to have the ZyWALL calculate a digest of an e-mail and send it to an anti-spam external database. The anti-spam external database sends a spam score for the e-mail back to the ZyWALL.
Spam Threshold	<p>The anti-spam external database checks an e-mail's digest and sends back a score that rates how likely the e-mail is to be spam. The possible range for the spam score is 0~100. The closer the score is to 100, the more likely the e-mail is to be spam.</p> <p>Set the spam score threshold (from 0 to 100) for considering an e-mail to be spam. The ZyWALL classifies any e-mail with a spam score at or below the spam threshold as not being spam and any e-mail with a spam score higher than the spam threshold as being spam.</p> <p>A lower spam threshold catches more spam e-mails, but may also classify more legitimate e-mail as spam.</p> <p>A higher spam threshold lessens the chance of classifying legitimate e-mail as spam, but may allow more spam to get through.</p>

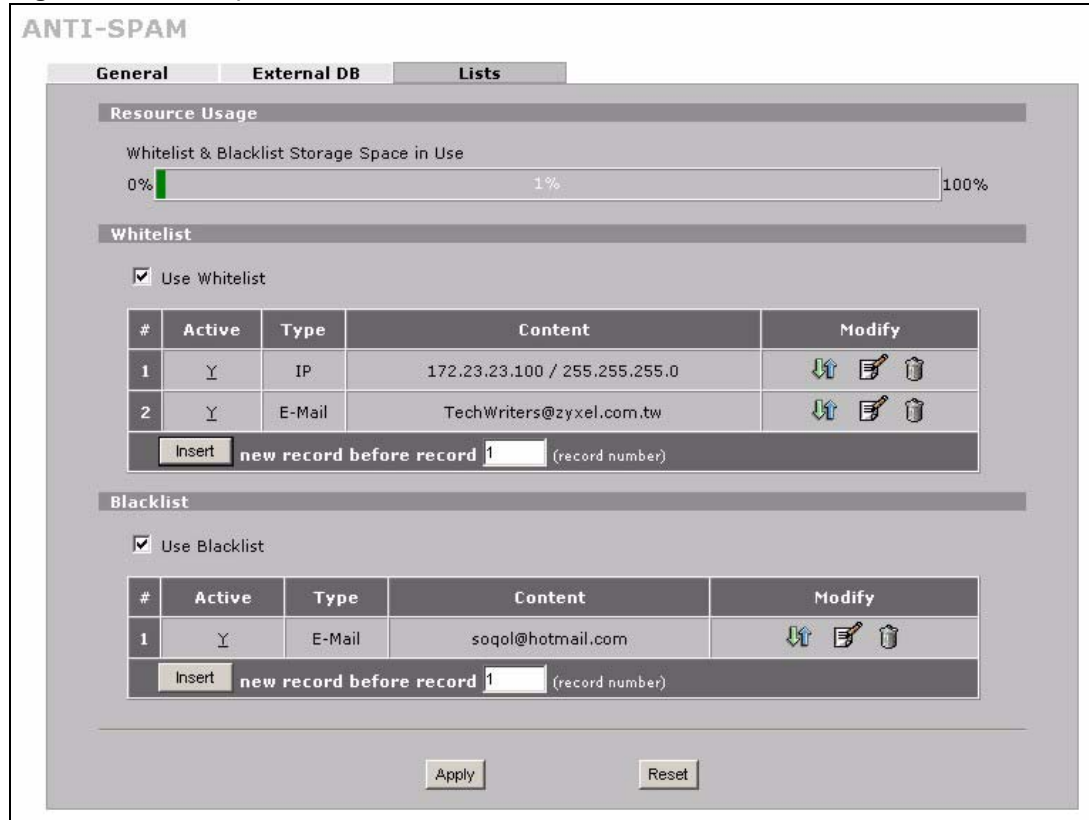
**Table 86** Anti-Spam: External DB (continued)

LABEL	DESCRIPTION
Action for No Spam Score	<p>Use this field to configure what the ZyWALL does if it does not receive a valid response from the anti-spam external database.</p> <p>If the ZyWALL does not receive a response within seven seconds, it sends the e-mail digest a second time. If the ZyWALL still does not receive a response after another seven seconds, it takes the action that you configure here. The ZyWALL also takes this action if it receives an invalid response.</p> <p>Here are possible reasons that would cause the ZyWALL to take this action:</p> <ol style="list-style-type: none"> <li>1. The ZyWALL was not able to connect to the anti-spam external database.</li> <li>2. The ZyWALL connected to the anti-spam external database, but there was no HTTP response within seven seconds.</li> <li>3. The ZyWALL received an error code from the anti-spam external database.</li> <li>4. The ZyWALL received an invalid spam score (for example a number higher than 100).</li> <li>5. The ZyWALL received an unknown response to the anti-spam query.</li> </ol>
Tag for No Spam Score	Enter a message or label (up to 16 ASCII characters) to add to the mail subject of e-mails that it forwards if a valid spam score was not received within ten seconds.
Forward SMTP & POP3 mail with tag in mail subject	Select this radio button to have the ZyWALL forward mail with the tag that you define.
Discard SMTP mail. Forward POP3 mail with tag in mail subject	Select this radio button to have the ZyWALL discard SMTP mail. The ZyWALL will still forward POP3 mail with the tag that you define.
External Database Service Status	<p>This read-only field displays the status of your anti-spam external database service registration and activation.</p> <p><b>License Inactive</b> displays if you have not successfully registered and activated the anti-spam external database service.</p> <p><b>License Inactive</b> and the date your subscription expired display if your subscription to the anti-spam external database service has expired.</p> <p><b>License Active</b> and the subscription expiration date display if you have successfully registered the ZyWALL and activated the anti-spam external database service.</p> <p><b>Trial Active</b> and the trial subscription expiration date display if you have successfully registered the ZyWALL and activated the anti-spam external database service trial subscription.</p>
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 15.4 Anti-Spam Lists Screen

Click **SECURITY, ANTI-SPAM, Lists** to display the **Anti-Spam Lists** screen.

Configure the whitelist to identify legitimate e-mail. Configure the blacklist to identify spam e-mail. You can create whitelist or blacklist entries based on the sender's IP address or e-mail address. You can also create entries that check for particular MIME headers or MIME header values.

**Figure 127** Anti-Spam: Lists

The following table describes the labels in this screen.

**Table 87** Anti-Spam: Lists

LABEL	DESCRIPTION
Resource Usage	
Whitelist & Blacklist Storage Space in Use	This bar displays the percentage of the ZyWALL's anti-spam whitelist and blacklist storage space that is currently in use. The bar turns from green to red when the maximum is being approached. When the bar is red, you should consider deleting unnecessary entries before adding more.
Whitelist	
Use Whitelist	Select this check box to have the ZyWALL forward e-mail that matches a whitelist entry without doing any more anti-spam checking on that individual e-mail.
Active	This field shows whether or not an entry is turned on.
Type	This field displays whether the entry is based on the e-mail's source IP address, source e-mail address or an MIME header.
Content	This field displays the source IP address, source e-mail address or MIME header for which the entry checks.
Modify	Click the <b>Edit</b> icon to change the entry. Click the <b>Remove</b> icon to delete the entry. Click the <b>Move</b> icon to change the entry's position in the list.

**Table 87** Anti-Spam: Lists (continued)

LABEL	DESCRIPTION
Insert	Type the index number where you want to put an entry. For example, if you type 6, your new entry becomes number 6 and the previous entry 6 (if there is one) becomes entry 7. Click <b>Insert</b> to display the screen where you edit an entry.
Blacklist	
Use Blacklist	Select this check box to have the ZyWALL treat e-mail that matches a blacklist entry as spam.
Active	This field shows whether or not an entry is turned on.
Type	This field displays whether the entry is based on the e-mail's source IP address, source e-mail address or an MIME header.
Content	This field displays the source IP address, source e-mail address or MIME header for which the entry checks.
Modify	Click the <b>Edit</b> icon to change the entry. Click the <b>Remove</b> icon to delete the entry. Click the <b>Move</b> icon to change the entry's position in the list.
Insert	Type the index number where you want to put an entry. For example, if you type 6, your new entry becomes number 6 and the previous entry 6 (if there is one) becomes entry 7. Click <b>Insert</b> to display the screen where you edit an entry.
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 15.5 Anti-Spam Rule Edit Screen

Click **SECURITY, ANTI-SPAM, Lists** to display the **Anti-Spam Lists** screen. To create a new anti-spam whitelist or blacklist entry, type the index number where you want to put the entry. and click **Insert** to display the **ANTI-SPAM Rule Edit** screen.

If you have already configured an anti-spam whitelist or blacklist entry, you can click the edit icon to display the **ANTI-SPAM Rule Edit** screen.

**Figure 128** Anti-Spam Rule Edit

The screenshot shows a web-based configuration window titled "ANTI-SPAM - EDIT WHITELIST". The main content area is labeled "Rule Edit" and contains the following elements:

- An "Active" checkbox, which is currently unchecked.
- A "Type" dropdown menu with "IP" selected.
- An "IP Address" input field containing the text "0 . 0 . 0 . 0".
- An "IP Subnet Mask" input field containing the text "0 . 0 . 0 . 0".
- At the bottom of the window, there are two buttons: "Apply" and "Cancel".

The following table describes the labels in this screen.

**Table 88** Anti-Spam Rule Edit

LABEL	DESCRIPTION
Rule Edit	
Active	Turn this entry on to have the ZyWALL use it as part of the whitelist or blacklist. You must also turn on the use of the corresponding list (in the <b>Anti-Spam Customization</b> screen) and the anti-spam feature (in the <b>Anti-Spam General</b> screen).
Type	<p>Use this field to base the entry on the e-mail's source IP address, source e-mail address or an MIME header.</p> <p>Select <b>IP</b> to have the ZyWALL check e-mail for a specific source IP address. You can create whitelist IP address entries for e-mail servers on your LAN or DMZ to speed up the ZyWALL's processing of your outgoing e-mail.</p> <p>Select <b>E-Mail</b> to have the ZyWALL check e-mail for a specific source e-mail address or domain name.</p> <p>You can create a whitelist entry for your company's domain name (or e-mail accounts) to speed up the ZyWALL's processing of e-mail sent by your company's employees.</p> <p>Select <b>MIME Header</b> to have the ZyWALL check e-mail for specific MIME headers or values.</p> <p>Configure blacklist MIME header entries to check for e-mail from bulk mail programs or that have content that are commonly used in spam. You can also configure whitelist MIME header entries to allow certain MIME headers or values that identify the e-mail as being from a trusted source.</p>
IP Address	This field displays when you select the <b>IP</b> type. Enter an IP address in dotted decimal notation.
IP Subnet Mask	This field displays when you select the <b>IP</b> type. Enter the subnet mask here, if applicable.
E-Mail Address	<p>This field displays when you select the <b>E-Mail</b> type. Enter an e-mail address or domain name (up to 63 ASCII characters).</p> <p>You can enter an individual e-mail address like abc@def.com.</p> <p>If you enter a domain name, the ZyWALL searches the source e-mail address string after the "@" symbol to see if it matches the domain name.</p> <p>For example, you configure a entry with "def.com" as the domain name: E-mails sent from def.com e-mail addresses such as abc@def.com match the entry. E-mails sent from mail.def.com, such as abc@mail.def.com do not match the entry since "mail.def.com" does not match "def.com".</p>
Header	<p>This field displays when you select the <b>MIME Header</b> type.</p> <p>Type the header part of an MIME header (up to 63 ASCII characters).</p> <p>In an MIME header, the header is the part that comes before the colon (:).</p> <p>For example, if you want the whitelist or blacklist entry to check for the MIME header "X-MSMail-Priority: Normal", enter "X-MSMail-Priority" here as the MIME header.</p>
Value	<p>This field displays when you select the <b>MIME Header</b> type.</p> <p>Type the value part of an MIME header (up to 63 ASCII characters).</p> <p>In an MIME header, the part that comes after the colon is the value.</p> <p>For example, if you want the whitelist or blacklist entry to check for the MIME header "X-MSMail-Priority: Normal", enter "Normal" here as the MIME value.</p>



**Table 88** Anti-Spam Rule Edit

LABEL	DESCRIPTION
Apply	Click <b>Apply</b> to save your settings and exit this screen.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

# CHAPTER 16

## Content Filtering Screens

This chapter provides an overview of content filtering.

### 16.1 Content Filtering Overview

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

#### 16.1.1 Restrict Web Features

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

#### 16.1.2 Create a Filter List

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

#### 16.1.3 Customize Web Site Access

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

### 16.2 Content Filter General

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

**Figure 129** Content Filter : General

The following table describes the labels in this screen.

**Table 89** Content Filter : General

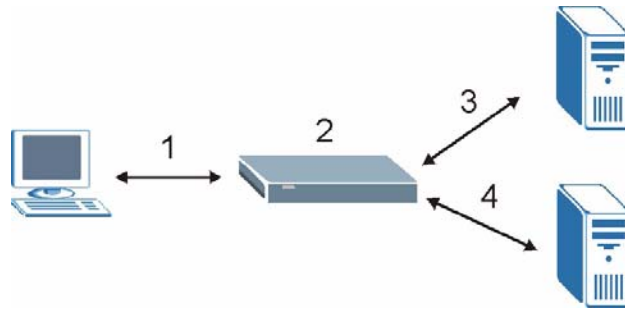
LABEL	DESCRIPTION
General Setup	
Enable Content Filter	Select this check box to enable the content filter.
Restrict Web Features	Select the check box(es) to restrict a feature. When you download a page containing a restricted feature, that part of the web page will appear blank or grayed out.
Block ActiveX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

**Table 89** Content Filter : General

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

## 16.3 Content Filtering with an External Database

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

**Figure 130** Content Filtering Lookup Procedure

- 1 A computer behind the ZyWALL tries to access a web site.
- 2 The ZyWALL looks up the web site in its cache. If an attempt to access the web site was made in the past, a record of that web site's category will be in the ZyWALL's cache. The ZyWALL blocks, blocks and logs or just logs the request based on your configuration.
- 3 Use the **CONTENT FILTER Cache** screen to configure how long a web site address remains in the cache as well as view those web site addresses (see [Section 16.7 on page 291](#)). All of the web site address records are also cleared from the local cache when the ZyWALL restarts.
- 4 If the ZyWALL has no record of the web site, it will query the external content filtering database and simultaneously send the request to the web server.
 

The external content filtering database may change a web site's category or categorize a previously uncategorized web site.
- 5 The external content filtering server sends the category information back to the ZyWALL, which then blocks and/or logs access to the web site. The web site's address and category are then stored in the ZyWALL's content filtering cache.

## 16.4 Content Filter Categories

Click **SECURITY, CONTENT FILTER**, and then the **Categories** tab to display the **CONTENT FILTER Categories** screen. Use this screen to configure category-based content filtering. You can set the ZyWALL to use external database content filtering and select which web site categories to block and/or log. You must register for external content filtering before you can use it. Use the **REGISTRATION** screens (see [Chapter 4 on page 104](#)) to create a myZyXEL.com account, register your device and activate the external content filtering service.

Do the following to view content filtering reports (see [Chapter 17 on page 294](#) for details).

- 1 Log into myZyXEL.com and click your device's link to open its **Service Management** screen.
- 2 Click **Content Filter** in the **Service Name** field to open the Blue Coat login screen.
- 3 Enter your ZyXEL device's MAC address (in lower case) in the **Name** field. You can find this MAC address in the **Service Management** screen ([Figure 136 on page 296](#)). Type your myZyXEL.com account password in the **Password** field. Click **Submit**.

**Figure 131** Content Filter : Categories

The following table describes the labels in this screen.

**Table 90** Content Filter: Categories

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

**Table 90** Content Filter: Categories (continued)

LABEL	DESCRIPTION
Unrated Web Pages	<p>Select <b>Block</b> to prevent users from accessing web pages that the external database content filtering has not categorized.</p> <p>When the external database content filtering blocks access to a web page, it displays the denied access message that you configured in the <b>CONTENT FILTER General</b> screen along with the category of the blocked web page.</p> <p>Select <b>Log</b> to record attempts to access web pages that are not categorized.</p>
When Content Filter Server Is Unavailable	<p>Select <b>Block</b> to block access to any requested web page if the external content filtering database is unavailable. The following are possible causes:</p> <ul style="list-style-type: none"> <li>There is no response from the external content filtering server within the time period specified in the <b>Content Filter Server Unavailable Timeout</b> field.</li> <li>The ZyWALL is not able to resolve the domain name of the external content filtering database.</li> <li>There is an error response from the external content filtering database. This can be caused by an expired content filtering registration (External content filtering's license key is invalid").</li> </ul> <p>Select <b>Log</b> to record attempts to access web pages that occur when the external content filtering database is unavailable.</p>
Content Filter Server Unavailable Timeout	<p>Specify a number of seconds (1 to 30) for the ZyWALL to wait for a response from the external content filtering server. If there is still no response by the time this period expires, the ZyWALL blocks or allows access to the requested web page based on the setting in the <b>Block When Content Filter Server Is Unavailable</b> field.</p>
Select Categories	
Select All Categories	<p>Select this check box to restrict access to all site categories listed below.</p>
Clear All Categories	<p>Select this check box to clear the selected categories below.</p>
Adult/Mature Content	<p>Selecting this category excludes pages that contain material of adult nature that does not necessarily contain excessive violence, sexual content, or nudity. These pages include very profane or vulgar content and pages that are not appropriate for children.</p>
Pornography	<p>Selecting this category excludes pages that contain sexually explicit material for the purpose of arousing a sexual or prurient interest.</p>
Sex Education	<p>Selecting this category excludes pages that provide graphic information (sometimes graphic) on reproduction, sexual development, safe sex practices, sexuality, birth control, and sexual development. It also includes pages that offer tips for better sex as well as products used for sexual enhancement.</p>
Intimate Apparel/Swimsuit	<p>Selecting this category excludes pages that contain images or offer the sale of swimsuits or intimate apparel or other types of suggestive clothing. It does not include pages selling undergarments as a subsection of other products offered.</p>
Nudity	<p>Selecting this category excludes pages containing nude or seminude depictions of the human body. These depictions are not necessarily sexual in intent or effect, but may include pages containing nude paintings or photo galleries of artistic nature. This category also includes nudist or naturist pages that contain pictures of nude individuals.</p>

**Table 90** Content Filter: Categories (continued)

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



**Table 90** Content Filter: Categories (continued)

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

**Table 90** Content Filter: Categories (continued)

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

**Table 90** Content Filter: Categories (continued)

LABEL	DESCRIPTION
Humor/Jokes	Selecting this category excludes pages that primarily focus on comedy, jokes, fun, etc. This may include pages containing jokes of adult or mature nature. Pages containing humorous Adult/Mature content also have an Adult/Mature category rating.
Streaming Media/MP3	Selecting this category excludes pages that sell, deliver, or stream music or video content in any format, including pages that provide downloads for such viewers.
Software Downloads	Selecting this category excludes pages that are dedicated to the electronic download of software packages, whether for payment or at no charge.
Pay to Surf	Selecting this category excludes pages that pay users in the form of cash or prizes, for clicking on or reading specific links, email, or web pages.
For Kids	Selecting this category excludes pages designed specifically for children.
Web Advertisements	Selecting this category excludes pages that provide online advertisements or banners. This does not include advertising servers that serve adult-oriented advertisements.
Web Hosting	Selecting this category excludes pages of organizations that provide top-level domain pages, as well as web communities or hosting services.
Advanced/Basic	Click <b>Advanced</b> to see an expanded list of categories, or click <b>Basic</b> to see a smaller list.
Test Web Site Attribute	
Test if Web site is blocked	You can check whether or not the content filter currently blocks any given web page. Enter a web site URL in the text box.
Test Against Local Cache	Click this button to test whether or not the web site above is saved in the ZyWALL's database of restricted web pages.
Test Against Internet Server	Click this button to test whether or not the web site above is saved in the external content filter server's database of restricted web pages.
Content Filter Service Status	<p>This read-only field displays the status of your category-based content filtering (using an external database) service subscription.</p> <p><b>License Inactive</b> displays if you have not registered and activated the category-based content filtering service.</p> <p><b>License Active</b> and the subscription expiration date display if you have registered the ZyWALL and activated the category-based content filtering service.</p> <p><b>Trial Active</b> and the trial subscription expiration date display if you have registered the ZyWALL and activated the category-based content filtering service.</p> <p><b>License Inactive</b> and the date your subscription expired display if your subscription to the category-based content filtering service has expired.</p> <p><b>Note:</b> After you register for content filtering, you need to wait up to five minutes for content filtering to be activated. See <a href="#">Section 17.1 on page 294</a> for how to check the content filtering activation.</p>
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 16.5 Content Filter Customization

Click **SECURITY, CONTENT FILTER**, then the **Customization** tab to display the **CONTENT FILTER Customization** screen.

You can create a list of good (allowed) web site addresses and a list of bad (blocked) web site addresses. You can also block web sites based on whether the web site's address contains a keyword. Use this screen to add or remove specific sites or keywords from the filter list.

**Figure 132** Content Filter: Customization

The screenshot displays the 'CONTENT FILTER' configuration page, specifically the 'Customization' tab. The page is divided into several sections:

- Web Site List Customization:** Includes a checked checkbox for 'Enable Web site customization.' Below it are two unchecked checkboxes: 'Disable all Web traffic except for trusted Web sites.' and 'Don't block Java/ActiveX/Cookies/Web proxy to trusted Web sites.'
- Trusted Web Sites:** Features an 'Add Trusted Web Site' input field with an 'Add' button. To the right, a 'Trusted Web Sites' list contains 'www.zyxel.com.tw' with a 'Delete' button.
- Forbidden Web Site List:** Features an 'Add Forbidden Web Site' input field with an 'Add' button. To the right, a 'Forbidden Web Sites' list contains 'www.playboy.com' with a 'Delete' button.
- Keyword Blocking:** Includes a checked checkbox for 'Block Web sites which contain these keywords.' Below it is an 'Add Keyword' input field with an 'Add' button. To the right, a 'Keyword List' contains 'bad' and 'sex' with a 'Delete' button.

At the bottom of the page, there are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

**Table 91** Content Filter: Customization

LABEL	DESCRIPTION
Web Site List Customization	
Enable Web site customization	Select this check box to allow trusted web sites and block forbidden web sites. Content filter list customization may be enabled and disabled without re-entering these site names.
Disable all Web traffic except for trusted Web sites	When this box is selected, the ZyWALL only allows Web access to sites on the <b>Trusted Web Site</b> list. If they are chosen carefully, this is the most effective way to block objectionable material.
Don't block Java/ActiveX/ Cookies/Web proxy to trusted Web sites	When this box is selected, the ZyWALL will permit Java, ActiveX and Cookies from sites on the <b>Trusted Web Site</b> list to the LAN. In certain cases, it may be desirable to allow Java, ActiveX or Cookies from sites that are known and trusted.
Trusted Web Sites	These are sites that you want to allow access to, regardless of their content rating, can be allowed by adding them to this list. You can enter up to 32 entries.
Add Trusted Web Site	Enter host names such as www.good-site.com into this text field. Do not enter the complete URL of the site – that is, do not include “http://”. All subdomains are allowed. For example, entering “zyxel.com” also allows “www.zyxel.com”, “partner.zyxel.com”, “press.zyxel.com”, etc.
Trusted Web Sites	This list displays the trusted web sites already added.
Add	Click this button when you have finished adding the host name in the text field above.
Delete	Select a web site name from the <b>Trusted Web Site List</b> , and then click this button to delete it from that list.
Forbidden Web Site List	Sites that you want to block access to, regardless of their content rating, can be allowed by adding them to this list. You can enter up to 32 entries.
Add Forbidden Web Site	Enter host names such as www.bad-site.com into this text field. Do not enter the complete URL of the site – that is, do not include “http://”. All subdomains are blocked. For example, entering “bad-site.com” also blocks “www.bad-site.com”, “partner.bad-site.com”, “press.bad-site.com”, etc.
Forbidden Web Sites	This list displays the forbidden web sites already added.
Add	Click this button when you have finished adding the host name in the text field above.
Delete	Select a web site name from the <b>Forbidden Web Site List</b> , and then click this button to delete it from that list.
Keyword Blocking	<p><b>Keyword Blocking</b> allows you to block websites with URLs that contain certain keywords in the domain name or IP address.</p> <p><b>Note:</b> See <a href="#">Section 16.6 on page 290</a> for how to set how much of the URL the ZyWALL checks.</p>
Block Web sites which contain these keywords.	Select this checkbox to enable keyword blocking.
Add Keyword	Enter a keyword (up to 31 printable ASCII characters) to block. You can also enter a numerical IP address.
Keyword List	This list displays the keywords already added.

**Table 91** Content Filter: Customization (continued)

LABEL	DESCRIPTION
Add	Click this button when you have finished adding the key words field above.
Delete	Select a keyword from the <b>Keyword List</b> , and then click this button to delete it from that list.
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 16.6 Customizing Keyword Blocking URL Checking

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

### 16.6.1 Domain Name or IP Address URL Checking

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

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

For example, with the URL [www.zyxel.com.tw/news/pressroom.php](http://www.zyxel.com.tw/news/pressroom.php), content filtering only searches for keywords within [www.zyxel.com.tw](http://www.zyxel.com.tw).

### 16.6.2 Full Path URL Checking

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

For example, with the URL [www.zyxel.com.tw/news/pressroom.php](http://www.zyxel.com.tw/news/pressroom.php), full path URL checking searches for keywords within [www.zyxel.com.tw/news/](http://www.zyxel.com.tw/news/).

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

### 16.6.3 File Name URL Checking

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

For example, filename URL checking searches for keywords within the URL [www.zyxel.com.tw/news/pressroom.php](http://www.zyxel.com.tw/news/pressroom.php).

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

## 16.7 Content Filtering Cache

Click **SECURITY, CONTENT FILTER**, then the **Cache** tab to display the **CONTENT FILTER Cache** screen. Use this screen to view and configure your ZyWALL's URL caching. You can also configure how long a categorized web site address remains in the cache as well as view those web site addresses to which access has been allowed or blocked based on the responses from the external content filtering server. The ZyWALL only queries the external content filtering database for sites not found in the cache.

You can remove individual entries from the cache. When you do this, the ZyWALL queries the external content filtering database the next time someone tries to access that web site. This allows you to check whether a web site's category has been changed.

Please see [Section 17.3 on page 299](#) for how to submit a web site that has been incorrectly categorized.

**Figure 133** Content Filter: Cache

**CONTENT FILTER**

**General** | **Categories** | **Customization** | **Cache**

**URL Cache Setup**

Maximum TTL  (1~720 hours)

**URL Cache Entry**

Total: 8

#	Action	URL	Remaining Time (hour)	Modify
1	Blocked	www.playboy.com/	72	
2	Allowed	ofs.zyxel.com.tw/officescan/cgi/cgiOnUpdate.exe	72	
3	Allowed	www.zyxel.com/	72	
4	Allowed	www.google.com/	72	
5	Allowed	www.bbc.co.uk/	72	
6	Allowed	adstat3.kkman.com.tw/?ver=03000000&ad54=1	72	
7	Allowed	www.yahoo.com.tw/	72	
8	Allowed	www.zyxel.com.tw/	72	

The following table describes the labels in this screen.

**Table 92** Content Filter: Cache

LABEL	DESCRIPTION
URL Cache Setup	
Maximum TTL	Type the maximum time to live (TTL) (1 to 720 hours). This sets how long the ZyWALL is to allow an entry to remain in the URL cache before discarding it.
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.
URL Cache Entry	
Flush	Click this button to clear all web site addresses from the cache manually.
Refresh	Click this button to reload the cache.
#	This is the index number of a categorized web site address record.
Action	This field shows whether access to the web site's URL was blocked-or allowed. Click the column heading to sort the entries. Point the triangle up to display the blocked URLs before the URLs to which access was allowed. Point the triangle down to display the URLs to which access was allowed before the blocked URLs.
URL	This is a web site's address that the ZyWALL previously checked with the external content filtering database.
Port	This is the service port number for which access was requested.
Remaining Time (hour)	This is the number of hours left before the URL entry is discarded from the cache.
Modify	Click the delete icon to remove the URL entry from the cache.





# CHAPTER 17

## Content Filtering Reports

This chapter describes how to view content filtering reports after you have activated the category-based content filtering subscription service.

See [Chapter 4 on page 104](#) on how to create a myZyXEL.com account, register your device and activate the subscription services using the **REGISTRATION** screens.

### 17.1 Checking Content Filtering Activation

After you activate content filtering, you need to wait up to five minutes for content filtering to be turned on.

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

- 1 Go to your device's web configurator's **CONTENT FILTER Categories** screen.
- 2 Select at least one category and click **Apply**.
- 3 Enter a valid URL or IP address of a web site in the **Test if Web site is blocked** field and click the **Test Against Internet Server** button.  
When content filtering is active, you should see an access blocked or access forwarded message. An error message displays if content filtering is not active.

### 17.2 Viewing Content Filtering Reports

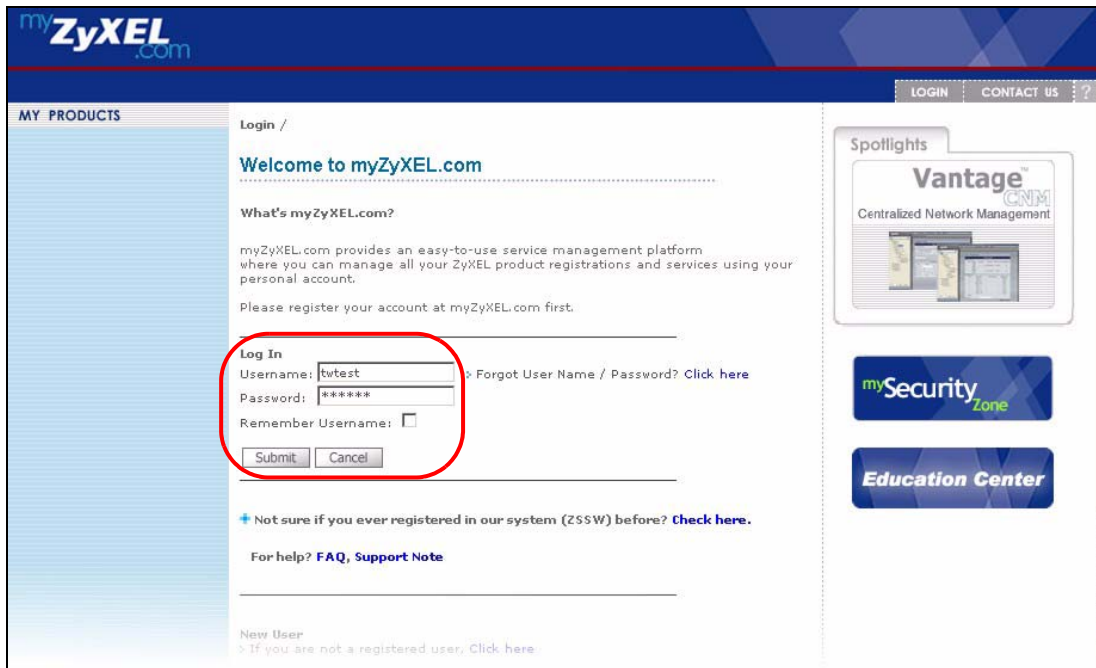
Content filtering reports are generated statistics and charts of access attempts to web sites belonging to the categories you selected in your device content filter screen.

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

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

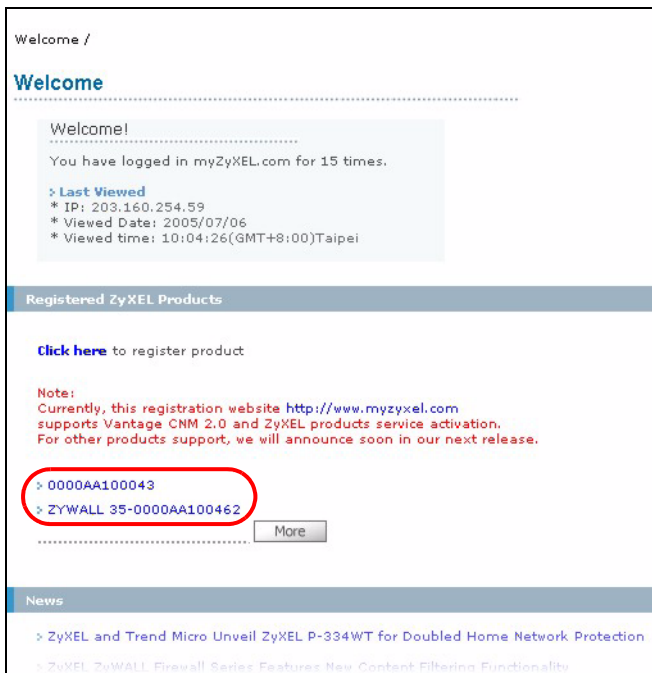
- 1 Go to <http://www.myZyXEL.com>.
- 2 Fill in your myZyXEL.com account information and click **Submit**.

**Figure 134** myZyXEL.com: Login



- 3 A welcome screen displays. Click your ZyWALL's model name and/or MAC address under **Registered ZyXEL Products**. You can change the descriptive name for your ZyWALL using the **Rename** button in the **Service Management** screen (see [Figure 136](#) on page 296).

**Figure 135** myZyXEL.com: Welcome



- 4 In the **Service Management** screen click **Content Filter** in the **Service Name** field to open the Blue Coat login screen.

**Figure 136** myZyXEL.com: Service Management

My Products / Service Activation

### Service Management

---

**Product Information**

0000AA100043

Serial Number: AAAA100043  
 Products: ZYWALL\_35  
 Authentication Code / MAC Address: 0000AA100043  
 Activation Key: N/A

**Manage Product**

Manage this product's registration by clicking on the appropriate buttons below:

0000AA100043

**Applicable Service List**

To enable your service(s), please click "Activate" shown below to enter your license key(s).  
 To login the Content Filter admin site, please click and input the mac address(lower case) & password.

	Service Name	Service Activation	Status	Expiry Date	Remark
1	Anti Spam	Upgrade	Trial	2005-10-06	-
2	Content Filter	Upgrade	Installed	2006-07-13	-
3	IDP AV	Upgrade	Trial	2005-11-09	-

**5** Enter your ZyXEL device's MAC address (in lower case) in the **Name** field. You can find this MAC address in the **Service Management** screen (Figure 136 on page 296). Type your myZyXEL.com account password in the **Password** field.

**6** Click **Submit**.

**Figure 137** Blue Coat: Login

**ZyXEL** Powered By **Blue Coat**

**System Login**

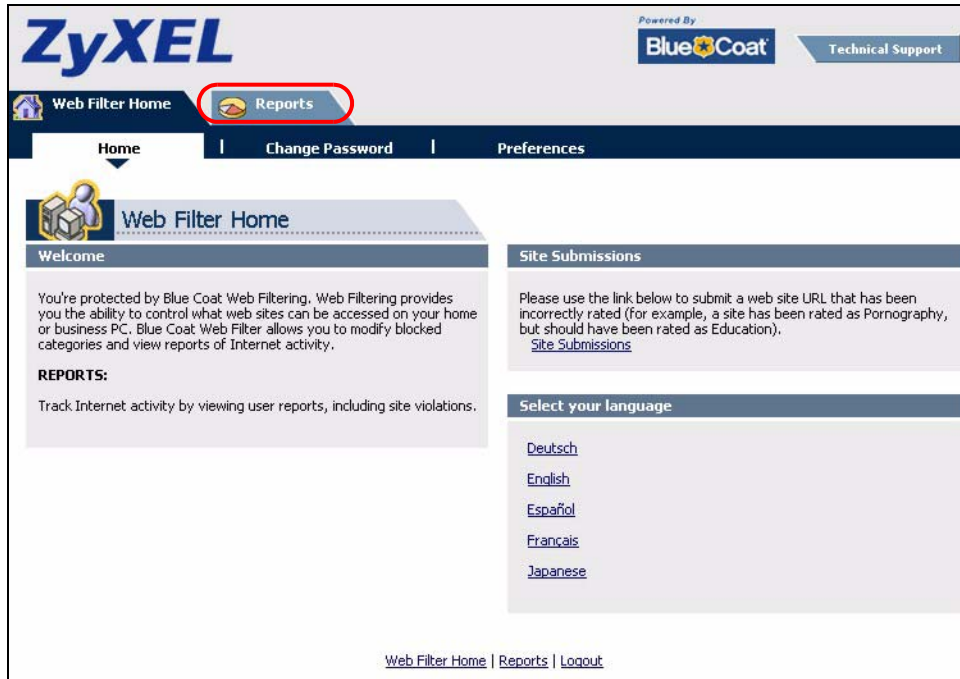
Welcome to your Blue Coat Web Filter Administration site. Please login using your Username and Password.

**Name**

**Password**

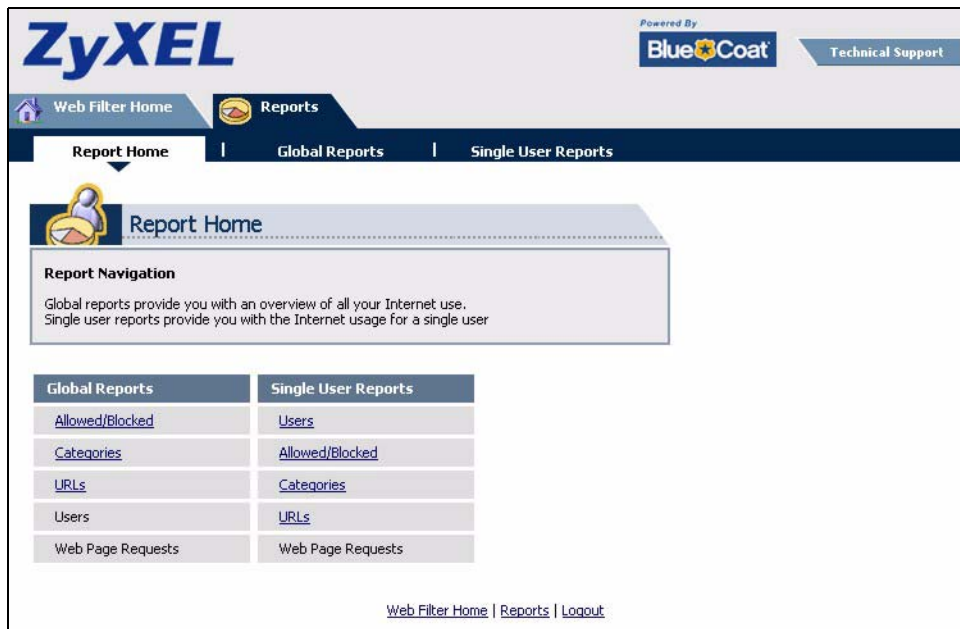
**7** In the **Web Filter Home** screen, click the **Reports** tab.

**Figure 138** Content Filtering Reports Main Screen



**8** Select items under **Global Reports** or **Single User Reports** to view the corresponding reports.

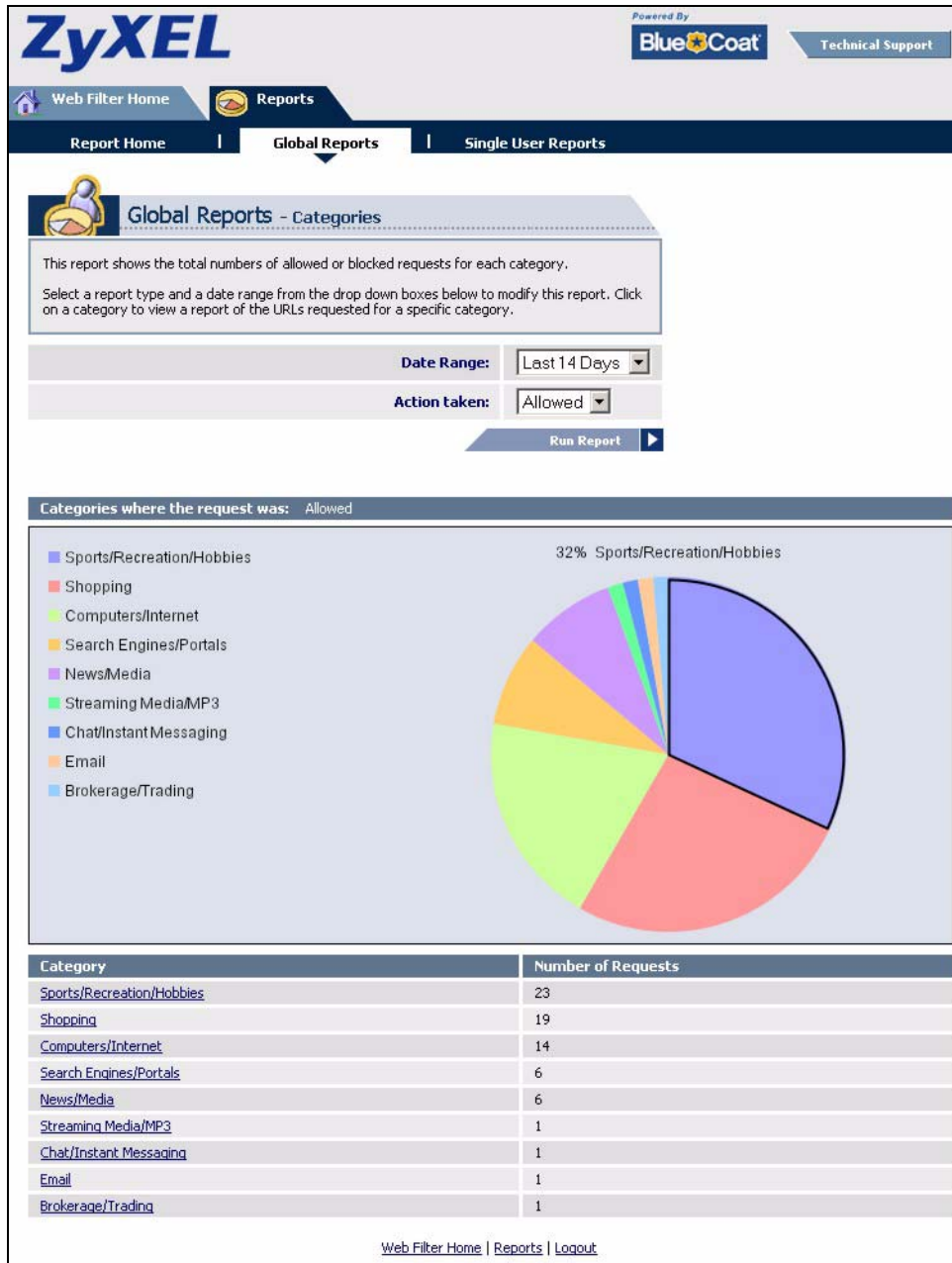
**Figure 139** Blue Coat: Report Home



**9** Select a time period in the **Date Range** field, either **Allowed** or **Blocked** in the **Action Taken** field and a category (or enter the user name if you want to view single user reports) and click **Run Report**. The screens vary according to the report type you selected in the **Report Home** screen.

**10** A chart and/or list of requested web site categories display in the lower half of the screen.

Figure 140 Global Report Screen Example



**11** You can click a category in the **Categories** report or click **URLs** in the **Report Home** screen to see the URLs that were requested.

Figure 141 Requested URLs Example

**ZyXEL** Powered By **BlueCoat** Technical Support

Web Filter Home | Reports | Global Reports | Single User Reports

**Global Reports - URLs**

This report displays allowed or blocked URLs requested within a specific category.  
Click on a URL to view the users that requested that URL.

Date Range: Last 14 Days  
Action taken: Allowed  
Category: Sports/Recreation/Hobbies

Run Report

URLs Requested for category: Sports/Recreation/Hobbies

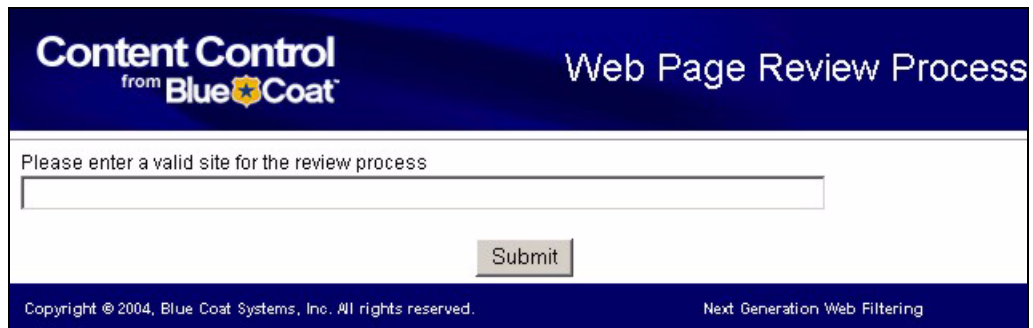
Item #	URL	Number of Requests	Open Web Page
1	adsatt.espn.go.com/insertfiles/javascript/flash.js	1	
2	sports.espn.go.com/crossdomain.xml	1	
3	sports.espn.go.com/sports/tvlistings/fp/headerData	1	
4	espn.go.com/Adserver?CallDown&AdTypes=MotionLogo;	1	
5	espn.go.com/myespn/login3.html	1	
6	broadband.espn.go.com/EBB2/popup	1	
7	sports-alt.espn.go.com/espn/format/sponsoredLinkSpot_redesign3	1	
8	sports.espn.go.com/espn/fp/pollData	1	
9	sports.espn.go.com/espn/util/encodeLess?id=1878300	1	
10	sports.espn.go.com/espn/util/encodeLess?id=1872951	1	
11	sports.espn.go.com/espn/fp/pollDataJS	1	
12	static.espn.go.com/swf/fp/superheadline.swf?h=Spur-fect+Ending&tex	1	
13	espn.go.com	1	
14	wimbledon.org/includes/js/external_sb.js	1	
15	espn.go.com/swf/header2005/headers/mlb_hdr.swf	1	
16	espn.go.com/swf/header2005/search/searchBar.swf	1	
17	sports.espn.go.com/mlb/xml/upcomingTV?sport=mlb	1	
18	espn.go.com/insertfiles/javascript/horizNav.js	1	
19	sports.espn.go.com/mlb/index	1	
20	espn.go.com/swf/header2005/tvschedule/tvschedule.swf	1	
21	espn-i.starwave.com/media/apphoto/WATW11606230650_thumbnail.jpeg	1	
22	espn.starwave.com/insertfiles/javascript/motion/motion_index_02.js	1	
23	sports.espn.go.com/espn/fp/pollDataGen?id=30688	1	

Web Filter Home | Reports | Logout

## 17.3 Web Site Submission

You may find that a web site has not been accurately categorized or that a web site's contents have changed and the content filtering category needs to be updated. Use the following procedure to submit the web site for review.

- 1 Log into the content filtering reports web site (see [Section 17.2 on page 294](#)).
- 2 In the **Web Filter Home** screen (see [Figure 138 on page 297](#)), click **Site Submissions** to open the **Web Page Review Process** screen shown next.

**Figure 142** Web Page Review Process Screen

The screenshot shows a web interface for 'Content Control from Blue Coat'. The title is 'Web Page Review Process'. Below the title is a text input field with the placeholder text 'Please enter a valid site for the review process'. A 'Submit' button is located below the input field. At the bottom of the page, there is a copyright notice: 'Copyright © 2004, Blue Coat Systems, Inc. All rights reserved.' and the text 'Next Generation Web Filtering'.

- 3 Type the web site's URL in the field and click **Submit** to have the web site reviewed.





# CHAPTER 18

## Introduction to IPSec

This chapter introduces the basics of IPSec VPNs.

### 18.1 VPN Overview

A VPN (Virtual Private Network) provides secure communications between sites without the expense of leased site-to-site lines. A secure VPN is a combination of tunneling, encryption, authentication, access control and auditing technologies/services used to transport traffic over the Internet or any insecure network that uses the TCP/IP protocol suite for communication.

#### 18.1.1 IPSec

Internet Protocol Security (IPSec) is a standards-based VPN that offers flexible solutions for secure data communications across a public network like the Internet. IPSec is built around a number of standardized cryptographic techniques to provide confidentiality, data integrity and authentication at the IP layer.

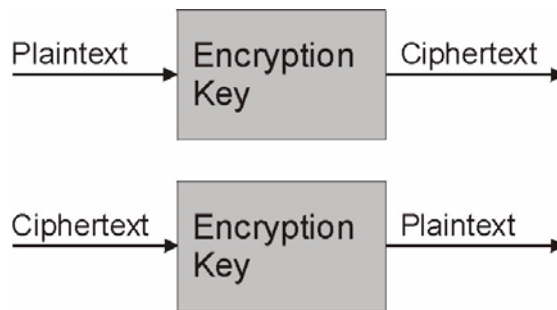
#### 18.1.2 Security Association

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

#### 18.1.3 Other Terminology

##### 18.1.3.1 Encryption

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

**Figure 143** Encryption and Decryption

### 18.1.3.2 Data Confidentiality

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

### 18.1.3.3 Data Integrity

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

### 18.1.3.4 Data Origin Authentication

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

## 18.1.4 VPN Applications

The ZyWALL supports the following VPN applications.

### 18.1.4.1 Linking Two or More Private Networks Together

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

### 18.1.4.2 Accessing Network Resources When NAT Is Enabled

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

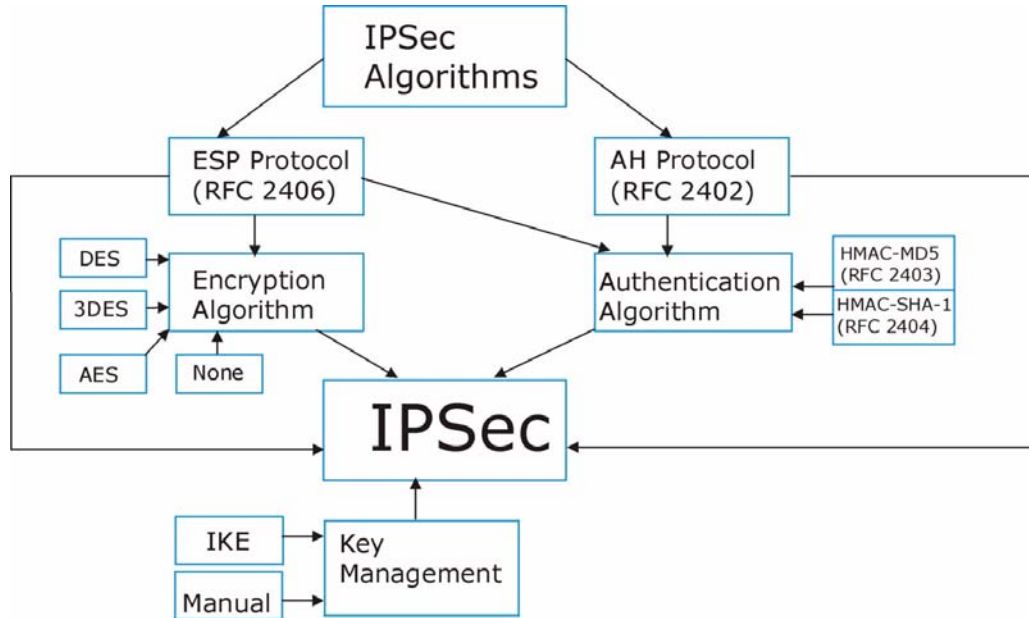
### 18.1.4.3 Unsupported IP Applications

A VPN tunnel may be created to add support for unsupported emerging IP applications. See [Chapter 1 on page 54](#) for an example of a VPN application.

## 18.2 IPsec Architecture

The overall IPsec architecture is shown as follows.

**Figure 144** IPsec Architecture



### 18.2.1 IPsec Algorithms

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

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

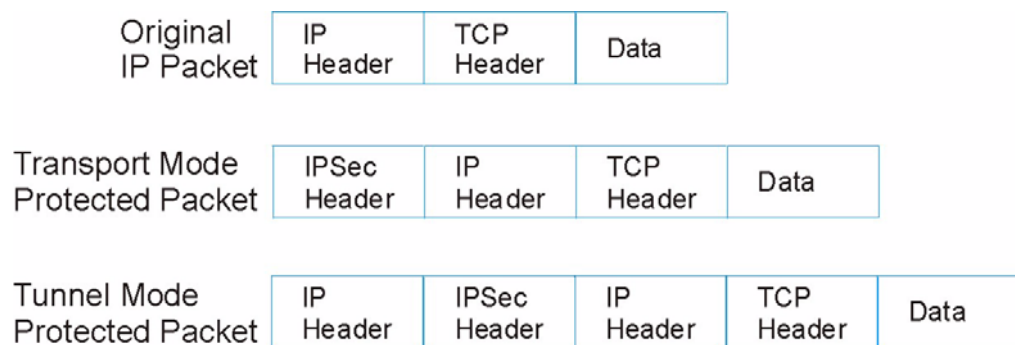
The Authentication Algorithms, HMAC-MD5 (RFC 2403) and HMAC-SHA-1 (RFC 2404), provide an authentication mechanism for the **AH** and **ESP** protocols. Refer to [Section 19.2 on page 308](#) for more information.

### 18.2.2 Key Management

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

## 18.3 Encapsulation

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

**Figure 145** Transport and Tunnel Mode IPSec Encapsulation

### 18.3.1 Transport Mode

**Transport** mode is used to protect upper layer protocols and only affects the data in the IP packet. In **Transport** mode, the IP packet contains the security protocol (**AH** or **ESP**) located after the original IP header and options, but before any upper layer protocols contained in the packet (such as TCP and UDP).

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

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

### 18.3.2 Tunnel Mode

**Tunnel** mode encapsulates the entire IP packet to transmit it securely. A **Tunnel** mode is required for gateway services to provide access to internal systems. **Tunnel** mode is fundamentally an IP tunnel with authentication and encryption. This is the most common mode of operation. **Tunnel** mode is required for gateway to gateway and host to gateway communications. **Tunnel** mode communications have two sets of IP headers:

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

## 18.4 IPSec and NAT

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

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

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

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

**Tunnel** mode **ESP** with authentication is compatible with NAT because integrity checks are performed over the combination of the "original header plus original payload," which is unchanged by a NAT device. **Transport** mode **ESP** with authentication is not compatible with NAT, although NAT traversal provides a way to use **Transport** mode **ESP** when there is a NAT router between the IPSec endpoints (See [Section 19.6 on page 310](#) for details).

**Table 93** VPN and NAT

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



# CHAPTER 19

## VPN Screens

This chapter introduces the VPN Web Configurator. See [Chapter 30 on page 472](#) for information on viewing logs and [Appendix S on page 774](#) for IPSec log descriptions.

### 19.1 VPN/IPSec Overview

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

### 19.2 IPSec Algorithms

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

#### 19.2.1 AH (Authentication Header) Protocol

**AH** protocol (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not for confidentiality, for which the **ESP** was designed.

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

#### 19.2.2 ESP (Encapsulating Security Payload) Protocol

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

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



**Table 94** ESP and AH

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

## 19.3 My ZyWALL

**My ZyWALL** identifies the WAN IP address or domain name of the ZyWALL (if it has one) or leave the field set to **0.0.0.0** when the ZyWALL is in router mode. This field displays the ZyWALL's IP address when the ZyWALL is in bridge mode. The ZyWALL has to rebuild the VPN tunnel if the **My ZyWALL** IP address changes after setup.

## 19.4 Remote Gateway Address

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

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

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

### 19.4.1 Dynamic Remote Gateway Address

If the remote secure gateway has a dynamic WAN IP address and does not use DDNS, enter 0.0.0.0 as the remote gateway's address. In this case only the remote secure gateway can initiate SAs. This may be useful for telecommuters initiating a VPN tunnel to the company network. See [Section 19.18 on page 337](#) for configuration examples.

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

## 19.5 Nailed Up

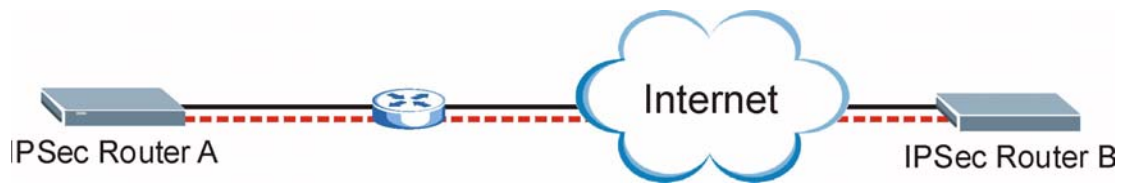
When you initiate an IPSec tunnel with nailed up enabled, the ZyWALL automatically renegotiates the tunnel when the IPSec SA lifetime period expires (see [Section 19.8 on page 313](#) for more on the IPSec SA lifetime). In effect, the IPSec tunnel becomes an always on connection after you initiate it. Both IPSec routers must have a ZyWALL-compatible nailed up feature enabled in order for this feature to work.

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

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

## 19.6 NAT Traversal

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

**Figure 146** NAT Router Between IPSec Routers

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

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

### 19.6.1 NAT Traversal Configuration

For NAT traversal to work you must:

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

In order for IPSec router A (see [Figure 146 on page 311](#)) to receive an initiating IPSec packet from IPSec router B, set the NAT router to forward UDP port 500 to IPSec router A.

## 19.7 ID Type and Content

With aggressive negotiation mode (see [Section 19.8.1 on page 314](#)), the ZyWALL identifies incoming SAs by ID type and content since this identifying information is not encrypted. This enables the ZyWALL to distinguish between multiple rules for SAs that connect from remote IPSec routers that have dynamic WAN IP addresses. Telecommuters can use separate passwords to simultaneously connect to the ZyWALL from IPSec routers with dynamic IP addresses (see [Section 19.18.2 on page 338](#) for a telecommuter configuration example).

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

With main mode (see [Section 19.8.1 on page 314](#)), the ID type and content are encrypted to provide identity protection. In this case the ZyWALL can only distinguish between up to 12 different incoming SAs that connect from remote IPSec routers that have dynamic WAN IP addresses. The ZyWALL can distinguish up to 12 incoming SAs because you can select

between three encryption algorithms (DES, 3DES and AES), two authentication algorithms (MD5 and SHA1) and two key groups (DH1 and DH2) when you configure a VPN rule (see [Section 19.12 on page 324](#)). The ID type and content act as an extra level of identification for incoming SAs.

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

**Table 95** Local ID Type and Content Fields

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

**Table 96** Peer ID Type and Content Fields

PEER ID TYPE=	CONTENT=
IP	Type the IP address of the computer with which you will make the VPN connection or leave the field blank to have the ZyWALL automatically use the address in the <b>Remote Gateway Address</b> field.
DNS	Type a domain name (up to 31 characters) by which to identify the remote IPsec router.
E-mail	Type an e-mail address (up to 31 characters) by which to identify the remote IPsec router.
Subject Name	Type the subject name (up to 255 characters) by which to identify the remote IPsec router. This option is available only when you set <b>Authentication Key to Certificate</b> .
The domain name or e-mail address that you use in the <b>Content</b> field is used for identification purposes only and does not need to be a real domain name or e-mail address. The domain name also does not have to match the remote router's IP address or what you configure in the <b>Remote Gateway Address</b> field below.	

### 19.7.1 ID Type and Content Examples

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

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

**Table 97** Matching ID Type and Content Configuration Example

ZYWALL A	ZYWALL B
Local ID type: E-mail	Local ID type: IP
Local ID content: tom@yourcompany.com	Local ID content: 1.1.1.2

**Table 97** Matching ID Type and Content Configuration Example

ZYWALL A	ZYWALL B
Peer ID type: IP	Peer ID type: E-mail
Peer ID content: 1.1.1.2	Peer ID content: tom@yourcompany.com

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

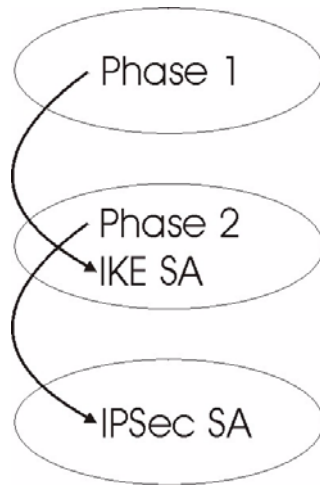
**Table 98** Mismatching ID Type and Content Configuration Example

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

## 19.8 IKE Phases

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

**Figure 147** Two Phases to Set Up the IPSec SA



In phase 1 you must:

- Choose a negotiation mode.
- Authenticate the connection by entering a pre-shared key.
- Choose an encryption algorithm.

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

In phase 2 you must:

- Choose which protocol to use (**ESP** or **AH**) for the IKE key exchange.
- Choose an encryption algorithm.
- Choose an authentication algorithm
- Choose whether to enable Perfect Forward Secrecy (PFS) using Diffie-Hellman public-key cryptography – see [Section 19.8.4 on page 315](#). Select **None** (the default) to disable PFS.
- Choose **Tunnel** mode or **Transport** mode.
- Set the IPSec SA lifetime. This field allows you to determine how long the IPSec SA should stay up before it times out. The ZyWALL automatically renegotiates the IPSec SA if there is traffic when the IPSec SA lifetime period expires. The ZyWALL also automatically renegotiates the IPSec SA if both IPSec routers have keep alive enabled, even if there is no traffic. If an IPSec SA times out, then the IPSec router must renegotiate the SA the next time someone attempts to send traffic.

### 19.8.1 Negotiation Mode

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

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

### 19.8.2 Pre-Shared Key

A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called pre-shared because you have to share it with another party before you can communicate with them over a secure connection.

### 19.8.3 Diffie-Hellman (DH) Key Groups

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

### 19.8.4 Perfect Forward Secrecy (PFS)

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

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

## 19.9 X-Auth (Extended Authentication)

Extended authentication provides added security by allowing you to use usernames and passwords for VPN connections. This is especially helpful when multiple ZyWALLs use one VPN rule to connect to a single ZyWALL. An attacker cannot make a VPN connection without a valid username and password.

The extended authentication server checks the user names and passwords of the extended authentication clients before completing the IPSec connection (see [Chapter 21 on page 370](#)).

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

### 19.9.1 Authentication Server

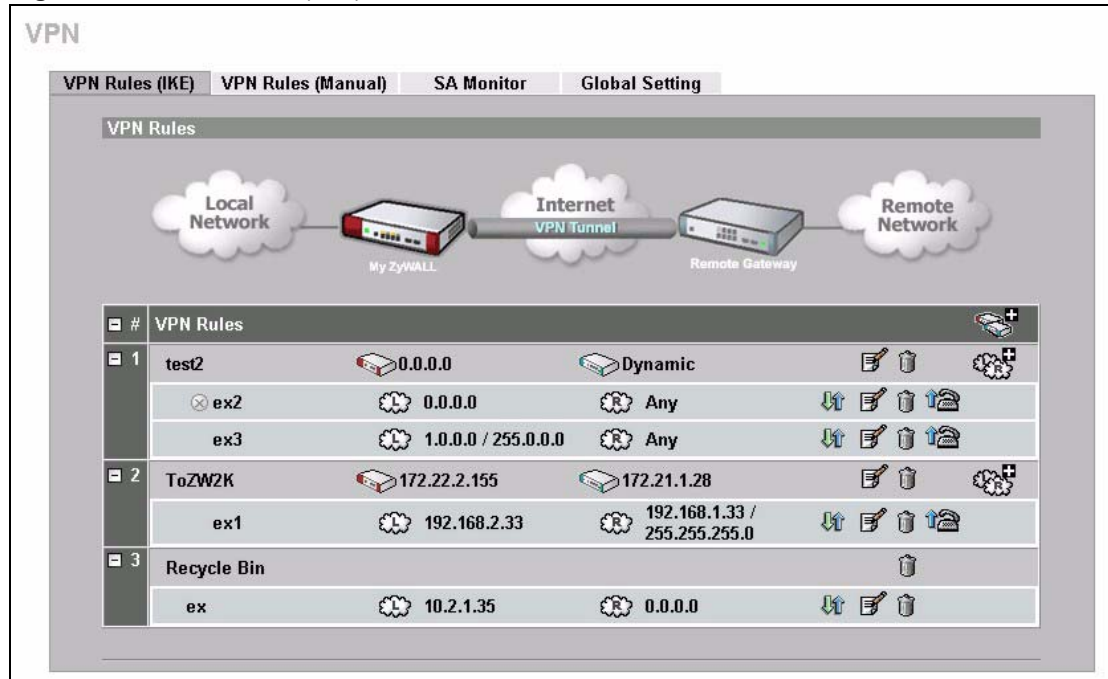
A ZyWALL set to be a VPN extended authentication server can use either the local user database internal to the ZyWALL or an external RADIUS server for an unlimited number of users. The ZyWALL uses the same local user database for VPN extended authentication and wireless LAN security.

## 19.10 VPN Rules (IKE)

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

Refer to [Table 100 on page 317](#) for descriptions of the icons used in this screen.

**Figure 148** VPN Rules (IKE)



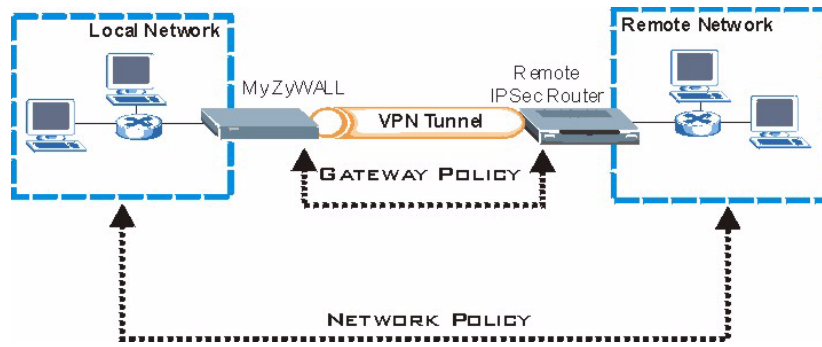
The following table introduces some of the general IPsec terms used in the **VPN** screens.

**Table 99** IPsec Fields Summary

LABEL	DESCRIPTION
VPN Tunnel	A VPN (Virtual Private Network) tunnel gives you a secure connection to another computer or network.
Gateway Policy	A gateway policy identifies the IPsec routers at either end of a VPN tunnel and specifies the authentication, encryption and other settings needed to negotiate a phase 1 IKE SA.
Network Policy	A network policy identifies the devices behind the IPsec routers at either end of a VPN tunnel and specifies the authentication, encryption and other settings needed to negotiate a phase 2 IPsec SA.
My ZyWALL	This is the WAN IP address or the domain name of your ZyWALL in router mode or the ZyWALL's IP address in bridge mode.
Local Network	This is the network behind the ZyWALL.
Remote Gateway Address	This is the WAN IP address or domain name of the IPsec router with which you're making the VPN connection.
Remote Network	This is the remote network behind the remote IPsec router.

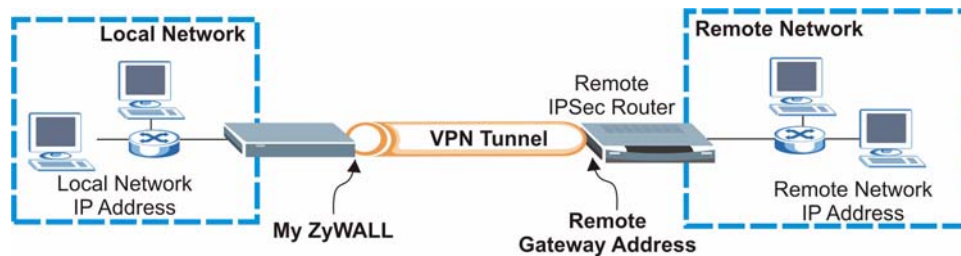


**Figure 149** Gateway and Network Policies



This figure helps explain the main fields in the VPN setup.










**Figure 150** IPsec Fields Summary





**Note:** Local and remote network IP addresses must be static.

The following table describes the icons used in the VPN screens.

**Table 100** VPN screen Icons Key



ICON	DESCRIPTION
	This represents your ZyWALL.
	This represents the remote secure gateway.
	This represents the local network.
	This represents the remote network.
	Click this icon to add a VPN gateway policy (or IPsec rule).
	Click this icon to add a VPN network policy.
	Click this icon to display a screen in which you can associate a network policy to a gateway policy.
	Click this icon to display a screen in which you can change the settings of a gateway or network policy.
	Click this icon to delete a gateway or network policy. When you delete a gateway policy, the ZyWALL automatically deletes the network policy(ies) associated to that gateway policy.

**Table 100** VPN screen Icons Key

ICON	DESCRIPTION
	Click this icon to establish a VPN connection to a remote network.
	This indicates that a gateway or network policy is not active.

**Note:** The **Recycle Bin** gateway policy is a virtual placeholder for any network policy(ies) without an associated gateway policy. When there is a network policy in the **Recycle Bin**, the **Recycle Bin** gateway policy automatically displays in this screen. See [Section 19.13 on page 328](#) for more information.

## 19.11 VPN Rules (IKE) Gateway Policy Edit

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

**Figure 151** VPN Rules (IKE): Gateway Policy: Edit


### VPN - GATEWAY POLICY - EDIT

**Property**

Name


NAT Traversal

**Gateway Policy Information**

 My ZyWALL

My Address  (Domain Name or IP Address)

My Domain Name  (See [DDNS](#))

 Remote Gateway Address

**Authentication Key**

Pre-Shared Key

Certificate  (See [My Certificates](#))

Local ID Type

Content

Peer ID Type

Content

**Extended Authentication**

Enable Extended Authentication

Server Mode (Search [Local User](#) first then [RADIUS](#))

Client Mode

User Name

Password

**IKE Proposal**

Negotiation Mode

Encryption Algorithm



Authentication Algorithm

SA Life Time (Seconds)

Key Group

Enable Multiple Proposals

**Associated Network Policies**

#	Name	Local Network	Remote Network
1	test	 172.11.1.3	 192.168.2.33

The following table describes the labels in this screen.

**Table 101** VPN Rules (IKE): Gateway Policy: Edit

LABEL	DESCRIPTION
Property	
Name	Type up to 32 characters to identify this VPN gateway policy. You may use any character, including spaces, but the ZyWALL drops trailing spaces.
NAT Traversal	<p>Select this check box to enable NAT traversal. NAT traversal allows you to set up a VPN connection when there are NAT routers between the two IPSec routers.</p> <p><b>Note:</b> The remote IPSec router must also have NAT traversal enabled. See <a href="#">Section 19.6 on page 310</a> for more information.</p> <p>You can use NAT traversal with <b>ESP</b> protocol using <b>Transport</b> or <b>Tunnel</b> mode, but not with <b>AH</b> protocol nor with manual key management. In order for an IPSec router behind a NAT router to receive an initiating IPSec packet, set the NAT router to forward UDP port 500 to the IPSec router behind the NAT router.</p>
Gateway Policy Information	
My ZyWALL	<p>When the ZyWALL is in router mode, this field identifies the WAN IP address or domain name of the ZyWALL. You can select <b>My Address</b> and enter the ZyWALL's static WAN IP address (if it has one) or leave the field set to 0.0.0.0. For a ZyWALL with multiple WAN ports, the following applies if the <b>My ZyWALL</b> field is configured as <b>0.0.0.0</b>:</p> <ul style="list-style-type: none"> <li>• When the WAN port operation mode is set to <b>Active/Passive</b>, the ZyWALL uses the IP address (static or dynamic) of the WAN port that is in use.</li> <li>• When the WAN port operation mode is set to <b>Active/Active</b>, the ZyWALL uses the IP address (static or dynamic) of the primary (highest priority) WAN port to set up the VPN tunnel as long as the corresponding WAN1 or WAN2 connection is up. If the corresponding WAN1 or WAN2 connection goes down, the ZyWALL uses the IP address of the other WAN port.</li> <li>• If both WAN connections go down, the ZyWALL uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect. See the chapter on WAN for details on dial backup and traffic redirect.</li> </ul> <p>A ZyWALL with a single WAN port uses its current WAN IP address (static or dynamic) in setting up the VPN tunnel if you leave this field as <b>0.0.0.0</b>. If the WAN connection goes down, the ZyWALL uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect.</p> <p>Otherwise, you can select <b>My Domain Name</b> and choose one of the dynamic domain names that you have configured (in the <b>DDNS</b> screen) to have the ZyWALL use that dynamic domain name's IP address.</p> <p>When the ZyWALL is in bridge mode, this field is read-only and displays the ZyWALL's IP address.</p> <p>The VPN tunnel has to be rebuilt if the <b>My ZyWALL</b> IP address changes after setup.</p>

**Table 101** VPN Rules (IKE): Gateway Policy: Edit (continued)

LABEL	DESCRIPTION
Remote Gateway Address	<p>Type the WAN IP address or the domain name (up to 31 characters) of the IPSec router with which you're making the VPN connection. Set this field to <b>0.0.0.0</b> if the remote IPSec router has a dynamic WAN IP address.</p> <p>In order to have more than one active rule with the <b>Remote Gateway Address</b> field set to <b>0.0.0.0</b>, the ranges of the local IP addresses cannot overlap between rules.</p> <p>If you configure an active rule with <b>0.0.0.0</b> in the <b>Remote Gateway Address</b> field and the LAN's full IP address range as the local IP address, then you cannot configure any other active rules with the <b>Remote Gateway Address</b> field set to <b>0.0.0.0</b>.</p>
Authentication Key	
Pre-Shared Key	<p>Select the <b>Pre-Shared Key</b> radio button and type your pre-shared key in this field. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection.</p> <p>Type from 8 to 31 case-sensitive ASCII characters or from 16 to 62 hexadecimal ("0-9", "A-F") characters. You must precede a hexadecimal key with a "0x (zero x)", which is not counted as part of the 16 to 62 character range for the key. For example, in "0x0123456789ABCDEF", 0x denotes that the key is hexadecimal and 0123456789ABCDEF is the key itself.</p> <p>Both ends of the VPN tunnel must use the same pre-shared key. You will receive a PYLD_MALFORMED (payload malformed) packet if the same pre-shared key is not used on both ends.</p>
Certificate	<p>Select the <b>Certificate</b> radio button to identify the ZyWALL by a certificate. Use the drop-down list box to select the certificate to use for this VPN tunnel. You must have certificates already configured in the <b>My Certificates</b> screen. Click <b>My Certificates</b> to go to the <b>My Certificates</b> screen where you can view the ZyWALL's list of certificates.</p>
Local ID Type	<p>Select <b>IP</b> to identify this ZyWALL by its IP address.</p> <p>Select <b>DNS</b> to identify this ZyWALL by a domain name.</p> <p>Select <b>E-mail</b> to identify this ZyWALL by an e-mail address.</p> <p>You do not configure the local ID type and content when you set <b>Authentication Key</b> to <b>Certificate</b>. The ZyWALL takes them from the certificate you select.</p>
Content	<p>When you select <b>IP</b> in the <b>Local ID Type</b> field, type the IP address of your computer in the local <b>Content</b> field. The ZyWALL automatically uses the IP address in the <b>My ZyWALL</b> field (refer to the <b>My ZyWALL</b> field description) if you configure the local <b>Content</b> field to <b>0.0.0.0</b> or leave it blank.</p> <p>It is recommended that you type an IP address other than <b>0.0.0.0</b> in the local <b>Content</b> field or use the <b>DNS</b> or <b>E-mail</b> ID type in the following situations.</p> <ul style="list-style-type: none"> <li>• When there is a NAT router between the two IPSec routers.</li> <li>• When you want the remote IPSec router to be able to distinguish between VPN connection requests that come in from IPSec routers with dynamic WAN IP addresses.</li> </ul> <p>When you select <b>DNS</b> or <b>E-mail</b> in the <b>Local ID Type</b> field, type a domain name or e-mail address by which to identify this ZyWALL in the local <b>Content</b> field. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string.</p>


**Table 101** VPN Rules (IKE): Gateway Policy: Edit (continued)

LABEL	DESCRIPTION
Peer ID Type	<p>Select from the following when you set <b>Authentication Key</b> to <b>Pre-shared Key</b>.</p> <ul style="list-style-type: none"> <li>• Select <b>IP</b> to identify the remote IPSec router by its IP address.</li> <li>• Select <b>DNS</b> to identify the remote IPSec router by a domain name.</li> <li>• Select <b>E-mail</b> to identify the remote IPSec router by an e-mail address.</li> </ul> <p>Select from the following when you set <b>Authentication Key</b> to <b>Certificate</b>.</p> <ul style="list-style-type: none"> <li>• Select <b>IP</b> to identify the remote IPSec router by the IP address in the subject alternative name field of the certificate it uses for this VPN connection.</li> <li>• Select <b>DNS</b> to identify the remote IPSec router by the domain name in the subject alternative name field of the certificate it uses for this VPN connection.</li> <li>• Select <b>E-mail</b> to identify the remote IPSec router by the e-mail address in the subject alternative name field of the certificate it uses for this VPN connection.</li> <li>• Select <b>Subject Name</b> to identify the remote IPSec router by the subject name of the certificate it uses for this VPN connection.</li> <li>• Select <b>Any</b> to have the ZyWALL not check the remote IPSec router's ID.</li> </ul>
Content	<p>The configuration of the peer content depends on the peer ID type.</p> <p>Do the following when you set <b>Authentication Key</b> to <b>Pre-shared Key</b>.</p> <ul style="list-style-type: none"> <li>• For <b>IP</b>, type the IP address of the computer with which you will make the VPN connection. If you configure this field to <b>0.0.0.0</b> or leave it blank, the ZyWALL will use the address in the <b>Remote Gateway Address</b> field (refer to the <b>Remote Gateway Address</b> field description).</li> <li>• For <b>DNS</b> or <b>E-mail</b>, type a domain name or e-mail address by which to identify the remote IPSec router. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string.</li> </ul> <p>It is recommended that you type an IP address other than <b>0.0.0.0</b> or use the <b>DNS</b> or <b>E-mail</b> ID type in the following situations:</p> <ul style="list-style-type: none"> <li>• When there is a NAT router between the two IPSec routers.</li> <li>• When you want the ZyWALL to distinguish between VPN connection requests that come in from remote IPSec routers with dynamic WAN IP addresses.</li> </ul> <p>Do the following when you set <b>Authentication Key</b> to <b>Certificate</b>.</p> <ul style="list-style-type: none"> <li>• For <b>IP</b>, type the IP address from the subject alternative name field of the certificate the remote IPSec router will use for this VPN connection. If you configure this field to <b>0.0.0.0</b> or leave it blank, the ZyWALL will use the address in the <b>Remote Gateway Address</b> field (refer to the <b>Remote Gateway Address</b> field description).</li> <li>• For <b>DNS</b> or <b>E-mail</b>, type the domain name or e-mail address from the subject alternative name field of the certificate the remote IPSec router will use for this VPN connection.</li> <li>• For <b>Subject Name</b>, type the subject name of the certificate the remote IPSec router will use for this VPN connection. Use up to 255 ASCII characters including spaces.</li> <li>• For <b>Any</b>, the peer <b>Content</b> field is not available.</li> <li>• Regardless of how you configure the <b>ID Type</b> and <b>Content</b> fields, two active SAs cannot have both the local and remote IP address ranges overlap between rules.</li> </ul>
Extended Authentication	
Enable Extended Authentication	Select this check box to activate extended authentication.


**Table 101** VPN Rules (IKE): Gateway Policy: Edit (continued)

LABEL	DESCRIPTION
Server Mode	<p>Select <b>Server Mode</b> to have this ZyWALL authenticate extended authentication clients that request this VPN connection.</p> <p>You must also configure the extended authentication clients' usernames and passwords in the authentication server's local user database or a RADIUS server (see <a href="#">Chapter 21 on page 370</a>).</p> <p>Click <b>Local User</b> to go to the <b>Local User Database</b> screen where you can view and/or edit the list of user names and passwords. Click <b>RADIUS</b> to go to the <b>RADIUS</b> screen where you can configure the ZyWALL to check an external RADIUS server.</p> <p>During authentication, if the ZyWALL (in server mode) does not find the extended authentication clients' user name in its internal user database and an external RADIUS server has been enabled, it attempts to authenticate the client through the RADIUS server.</p>
Client Mode	<p>Select <b>Client Mode</b> to have your ZyWALL use a username and password when initiating this VPN connection to the extended authentication server ZyWALL. Only a VPN extended authentication client can initiate this VPN connection.</p>
User Name	<p>Enter a user name for your ZyWALL to be authenticated by the VPN peer (in server mode). The user name can be up to 31 case-sensitive ASCII characters, but spaces are not allowed. You must enter a user name and password when you select client mode.</p>
Password	<p>Enter the corresponding password for the above user name. The password can be up to 31 case-sensitive ASCII characters, but spaces are not allowed.</p>
IKE Proposal	
Negotiation Mode	<p>Select <b>Main</b> or <b>Aggressive</b> from the drop-down list box. Multiple SAs connecting through a secure gateway must have the same negotiation mode.</p>
Encryption Algorithm	<p>Select <b>DES</b>, <b>3DES</b> or <b>AES</b> from the drop-down list box.</p> <p>When you use one of these encryption algorithms for data communications, both the sending device and the receiving device must use the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (<b>3DES</b>) is a variation on DES that uses a 168-bit key. As a result, <b>3DES</b> is more secure than <b>DES</b>. It also requires more processing power, resulting in increased latency and decreased throughput. This implementation of AES uses a 128-bit key. <b>AES</b> is faster than <b>3DES</b>.</p>
Authentication Algorithm	<p>Select <b>SHA1</b> or <b>MD5</b> from the drop-down list box. <b>MD5</b> (Message Digest 5) and <b>SHA1</b> (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The <b>SHA1</b> algorithm is generally considered stronger than <b>MD5</b>, but is slower. Select <b>MD5</b> for minimal security and <b>SHA-1</b> for maximum security.</p>
SA Life Time (Seconds)	<p>Define the length of time before an IKE SA automatically renegotiates in this field. It may range from 180 to 3,000,000 seconds (almost 35 days).</p> <p>A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.</p>
Key Group	<p>You must choose a key group for phase 1 IKE setup. <b>DH1</b> (default) refers to Diffie-Hellman Group 1 a 768 bit random number. <b>DH2</b> refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number.</p>

**Table 101** VPN Rules (IKE): Gateway Policy: Edit (continued)

LABEL	DESCRIPTION
Enable Multiple Proposals	<p>Select this check box to allow the ZyWALL to use any of its phase 1 or phase 2 encryption and authentication algorithms when negotiating an IPSec SA.</p> <p>When you enable multiple proposals, the ZyWALL allows the remote IPSec router to select which encryption and authentication algorithms to use for the VPN tunnel, even if they are less secure than the ones you configure for the VPN rule.</p> <p>Clear this check box to have the ZyWALL use only the phase 1 or phase 2 encryption and authentication algorithms configured below when negotiating an IPSec SA.</p>
Associated Network Policies	<p>The following table shows the policy(ies) you configure for this rule.</p> <p>To add a VPN policy, click the add network policy (  ) icon in the <b>VPN Rules (IKE)</b> screen (see <a href="#">Figure 148 on page 316</a>). Refer to <a href="#">Section 19.12 on page 324</a> for more information.</p>
#	This field displays the policy index number.
Name	This field displays the policy name.
Local Network	This field displays one or a range of IP address(es) of the computer(s) behind the ZyWALL.
Remote Network	This field displays one or a range of IP address(es) of the remote network behind the remote IPsec router.
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

## 19.12 VPN Rules (IKE): Network Policy Edit

Click **VPN** and the add network policy (  ) icon in the **VPN Rules (IKE)** screen to display the **VPN-Network Policy -Edit** screen. Use this screen to configure a network policy.



**Figure 152** VPN Rules (IKE): Network Policy Edit

### VPN - NETWORK POLICY - EDIT

**Property**

Active

Name

Protocol

Nailed-Up

Allow NetBIOS Traffic Through IPSec Tunnel

Check IPSec Tunnel Connectivity  Log

Ping this Address

**Gateway Policy Information**

Gateway Policy

**Local Network**

Address Type

Starting IP Address

Ending IP Address / Subnet Mask

Local Port Start  End

**Remote Network**

Address Type

Starting IP Address

Ending IP Address / Subnet Mask

Remote Port Start  End

**IPSec Proposal**

Encapsulation Mode

Active Protocol

Encryption Algorithm

Authentication Algorithm

SA Life Time (Seconds)

Perfect Forward Secrecy (PFS)

Enable Replay Detection

Enable Multiple Proposals

The following table describes the labels in this screen.

**Table 102** VPN Rules (IKE): Network Policy Edit

LABEL	DESCRIPTION
Active	<p>If the <b>Active</b> check box is selected, packets for the tunnel trigger the ZyWALL to build the tunnel.</p> <p>Clear the <b>Active</b> check box to turn the network policy off. The ZyWALL does not apply the policy. Packets for the tunnel do not trigger the tunnel.</p> <p>If you clear the <b>Active</b> check box while the tunnel is up (and click <b>Apply</b>), you turn off the network policy and the tunnel goes down.</p>
Name	Type a name to identify this VPN network policy. You may use any character, including spaces, but the ZyWALL drops trailing spaces.
Protocol	Enter 1 for ICMP, 6 for TCP, 17 for UDP, etc. 0 is the default and signifies any protocol.
Nailed-Up	<p>Select this check box to turn on the nailed up feature for this SA.</p> <p>Turn on nailed up to have the ZyWALL automatically reinitiate the SA after the SA lifetime times out, even if there is no traffic. The ZyWALL also reinitiates the SA when it restarts.</p> <p>The ZyWALL also rebuilds the tunnel if it was disconnected due to the output or input idle timer.</p>
Allow NetBIOS Traffic Through IPsec Tunnel	<p>This field is not available when the ZyWALL is in bridge mode.</p> <p>NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to connect to and communicate with a LAN. It may sometimes be necessary to allow NetBIOS packets to pass through VPN tunnels in order to allow local computers to find computers on the remote network and vice versa.</p> <p>Select this check box to send NetBIOS packets through the VPN connection.</p>
Check IPsec Tunnel Connectivity	<p>Select the check box and configure an IP address in the <b>Ping this Address</b> field to have the ZyWALL periodically test the VPN tunnel to the remote IPsec router.</p> <p>The ZyWALL pings the IP address every minute. The ZyWALL starts the IPsec connection idle timeout timer when it sends the ping packet. If there is no traffic from the remote IPsec router by the time the timeout period expires, the ZyWALL disconnects the VPN tunnel.</p>
Log	Select this check box to set the ZyWALL to create logs when it cannot ping the remote device.
Ping this Address	If you select <b>Check IPsec Tunnel Connectivity</b> , enter the IP address of a computer at the remote IPsec network. The computer's IP address must be in this IP policy's remote range (see the <b>Remote Network</b> fields).
Gateway Policy Information	
Gateway Policy	Select the gateway policy with which you want to use the VPN policy.
Local Network	<p>Local IP addresses must be static and correspond to the remote IPsec router's configured remote IP addresses.</p> <p>Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.</p>
Address Type	Use the drop-down list box to choose <b>Single Address</b> , <b>Range Address</b> , or <b>Subnet Address</b> . Select <b>Single Address</b> for a single IP address. Select <b>Range Address</b> for a specific range of IP addresses. Select <b>Subnet Address</b> to specify IP addresses on a network by their subnet mask.


**Table 102** VPN Rules (IKE): Network Policy Edit (continued)

LABEL	DESCRIPTION
Starting IP Address	When the <b>Address Type</b> field is configured to <b>Single Address</b> , enter a (static) IP address on the LAN behind your ZyWALL. When the <b>Address Type</b> field is configured to <b>Range Address</b> , enter the beginning (static) IP address, in a range of computers on the LAN behind your ZyWALL. When the <b>Address Type</b> field is configured to <b>Subnet Address</b> , this is a (static) IP address on the LAN behind your ZyWALL.
Ending IP Address/ Subnet Mask	When the <b>Address Type</b> field is configured to <b>Single Address</b> , this field is N/A. When the <b>Address Type</b> field is configured to <b>Range Address</b> , enter the end (static) IP address, in a range of computers on the LAN behind your ZyWALL. When the <b>Address Type</b> field is configured to <b>Subnet Address</b> , this is a subnet mask on the LAN behind your ZyWALL.
Local Port	0 is the default and signifies any port. Type a port number from 0 to 65535 in the <b>Start</b> and <b>End</b> fields. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.
Remote Network	Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses.  Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.
Address Type	Use the drop-down list box to choose <b>Single Address</b> , <b>Range Address</b> , or <b>Subnet Address</b> . Select <b>Single Address</b> with a single IP address. Select <b>Range Address</b> for a specific range of IP addresses. Select <b>Subnet Address</b> to specify IP addresses on a network by their subnet mask.
Starting IP Address	When the <b>Address Type</b> field is configured to <b>Single Address</b> , enter a (static) IP address on the network behind the remote IPSec router. When the <b>Addr Type</b> field is configured to <b>Range Address</b> , enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. When the <b>Address Type</b> field is configured to <b>Subnet Address</b> , enter a (static) IP address on the network behind the remote IPSec router.
Ending IP Address/ Subnet Mask	When the <b>Address Type</b> field is configured to <b>Single Address</b> , this field is N/A. When the <b>Address Type</b> field is configured to <b>Range Address</b> , enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the <b>Address Type</b> field is configured to <b>Subnet Address</b> , enter a subnet mask on the network behind the remote IPSec router.
Remote Port	0 is the default and signifies any port. Type a port number from 0 to 65535 in the <b>Start</b> and <b>End</b> fields. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.
IPSec Proposal	
Encapsulation Mode	Select <b>Tunnel</b> mode or <b>Transport</b> mode.
Active Protocol	Select the security protocols used for an SA.  Both <b>AH</b> and <b>ESP</b> increase processing requirements and communications latency (delay).
Encryption Algorithm	When <b>DES</b> is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES ( <b>3DES</b> ) is a variation on DES that uses a 168-bit key. As a result, <b>3DES</b> is more secure than <b>DES</b> . It also requires more processing power, resulting in increased latency and decreased throughput. This implementation of <b>AES</b> uses a 128-bit key. <b>AES</b> is faster than <b>3DES</b> . Select <b>NULL</b> to set up a tunnel without encryption. When you select <b>NULL</b> , you do not enter an encryption key.

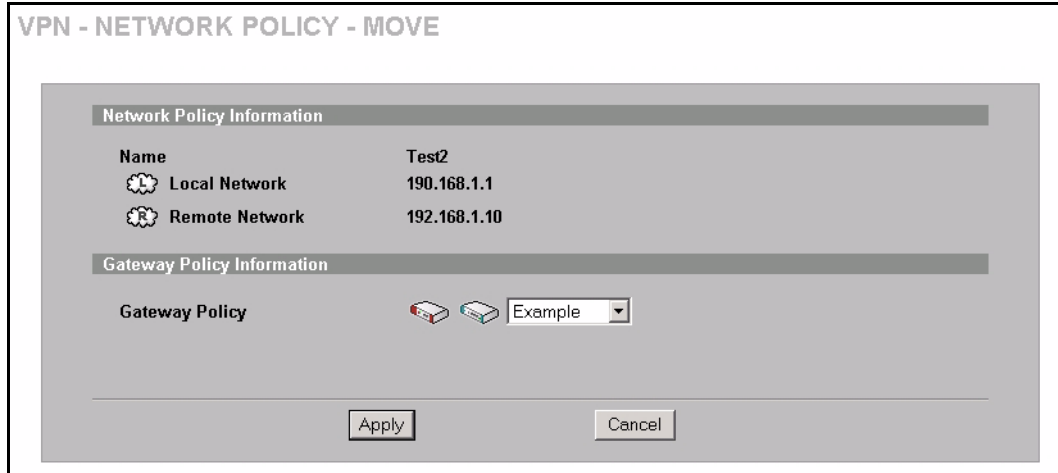
**Table 102** VPN Rules (IKE): Network Policy Edit (continued)

LABEL	DESCRIPTION
Authentication Algorithm	<b>MD5</b> (Message Digest 5) and <b>SHA1</b> (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The <b>SHA1</b> algorithm is generally considered stronger than <b>MD5</b> , but is slower. Select <b>MD5</b> for minimal security and <b>SHA-1</b> for maximum security.
SA Life Time (Seconds)	Define the length of time before an IKE SA automatically renegotiates in this field. The minimum value is 180 seconds. A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Perfect Forward Secret (PFS)	Perfect Forward Secret (PFS) is disabled ( <b>NONE</b> ) by default in phase 2 IPsec SA setup. This allows faster IPsec setup, but is not so secure. Select <b>DH1</b> or <b>DH2</b> to enable PFS. <b>DH1</b> refers to Diffie-Hellman Group 1 a 768 bit random number. <b>DH2</b> refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number (more secure, yet slower).
Enable Replay Detection	As a VPN setup is processing intensive, the system is vulnerable to Denial of Service (DOS) attacks. The IPsec receiver can detect and reject old or duplicate packets to protect against replay attacks. Enable replay detection by selecting this check box.
Enable Multiple Proposals	Select this check box to allow the ZyWALL to use any of its phase 1 or phase 2 encryption and authentication algorithms when negotiating an IPsec SA. When you enable multiple proposals, the ZyWALL allows the remote IPsec router to select which encryption and authentication algorithms to use for the VPN tunnel, even if they are less secure than the ones you configure for the VPN rule. Clear this check box to have the ZyWALL use only the phase 1 or phase 2 encryption and authentication algorithms configured below when negotiating an IPsec SA.
Apply	Click <b>Apply</b> to save the changes.
Cancel	Click <b>Cancel</b> to discard all changes and return to the main VPN screen.

## 19.13 VPN Rules (IKE): Network Policy Move

Click the move (  ) icon in the **VPN Rules (IKE)** screen to display the **VPN Rules (IKE): Network Policy Move** screen. Use this screen to associate a network policy to a gateway rule.

**Figure 153** VPN Rules (IKE): Network Policy Move



The following table describes the labels in this screen.

**Table 103** VPN Rules (IKE): Network Policy Move

LABEL	DESCRIPTION
Network Policy Information	The following fields display the general network settings of this VPN policy.
Name	This field displays the policy name.
Local Network	This field displays one or a range of IP address(es) of the computer(s) behind the ZyWALL.
Remote Network	This field displays one or a range of IP address(es) of the remote network behind the remote IPsec router.
Gateway Policy Information	
Gateway Policy	Select the name of a VPN rule (or gateway policy) to which you want to associate this VPN network policy. If you do not want to associate a network policy to any gateway policy, select <b>Recycle Bin</b> from the drop-down list box. The <b>Recycle Bin</b> gateway policy is a virtual placeholder for any network policy(ies) without an associated gateway policy. When there is a network policy in <b>Recycle Bin</b> , the <b>Recycle Bin</b> gateway policy automatically displays in the <b>VPN Rules (IKE)</b> screen.
Apply	Click <b>Apply</b> to save the changes.
Cancel	Click <b>Cancel</b> to discard all changes and return to the main VPN screen.

## 19.14 VPN Rules (Manual)

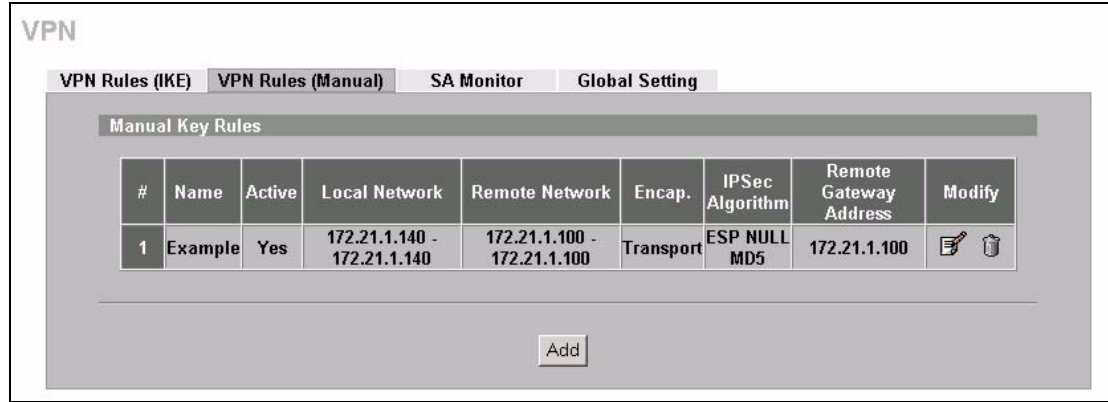
Refer to [Figure 150 on page 317](#) for a graphical representation of the fields in the web configurator.

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

You may want to configure a VPN rule that uses manual key management if you are having problems with IKE key management.

Refer to [Table 100 on page 317](#) for descriptions of the icons used in this screen.

**Figure 154** VPN Rules (Manual)



The following table describes the labels in this screen.

**Table 104** VPN Rules (Manual)

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

**Table 104** VPN Rules (Manual) (continued)

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

## 19.15 VPN Rules (Manual): Edit

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

### 19.15.1 Security Parameter Index (SPI)

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

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

Click the edit icon on the **VPN Rules (Manual)** screen to edit VPN rules.

**Figure 155** VPN Rules (Manual): Edit

The following table describes the labels in this screen.

**Table 105** VPN Rules (Manual) Edit

LABEL	DESCRIPTION
Property	
Active	Select this check box to activate this VPN policy.
Name	Type up to 32 characters to identify this VPN policy. You may use any character, including spaces, but the ZyWALL drops trailing spaces.
Allow NetBIOS Traffic Through IPSec Tunnel	This field is not available when the ZyWALL is in bridge mode. NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to find other computers. It may sometimes be necessary to allow NetBIOS packets to pass through VPN tunnels in order to allow local computers to find computers on the remote network and vice versa. Select this check box to send NetBIOS packets through the VPN connection.



**Table 105** VPN Rules (Manual) Edit (continued)

LABEL	DESCRIPTION
Local Network	<p>Local IP addresses must be static and correspond to the remote IPSec router's configured remote IP addresses.</p> <p>Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.</p>
Address Type	<p>Use the drop-down list box to choose <b>Single Address</b>, <b>Range Address</b>, or <b>Subnet Address</b>. Select <b>Single Address</b> for a single IP address. Select <b>Range Address</b> for a specific range of IP addresses. Select <b>Subnet Address</b> to specify IP addresses on a network by their subnet mask.</p>
Starting IP Address	<p>When the <b>Address Type</b> field is configured to <b>Single Address</b>, enter a (static) IP address on the LAN behind your ZyWALL. When the <b>Address Type</b> field is configured to <b>Range Address</b>, enter the beginning (static) IP address, in a range of computers on the LAN behind your ZyWALL. When the <b>Address Type</b> field is configured to <b>Subnet Address</b>, this is a (static) IP address on the LAN behind your ZyWALL.</p>
Ending IP Address/Subnet Mask	<p>When the <b>Address Type</b> field is configured to <b>Single Address</b>, this field is N/A. When the <b>Address Type</b> field is configured to <b>Range Address</b>, enter the end (static) IP address, in a range of computers on the LAN behind your ZyWALL. When the <b>Address Type</b> field is configured to <b>Subnet Address</b>, this is a subnet mask on the LAN behind your ZyWALL.</p>
Remote Network	<p>Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses.</p> <p>Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.</p>
Address Type	<p>Use the drop-down list box to choose <b>Single Address</b>, <b>Range Address</b>, or <b>Subnet Address</b>. Select <b>Single Address</b> with a single IP address. Select <b>Range Address</b> for a specific range of IP addresses. Select <b>Subnet Address</b> to specify IP addresses on a network by their subnet mask.</p>
Starting IP Address	<p>When the <b>Address Type</b> field is configured to <b>Single Address</b>, enter a (static) IP address on the network behind the remote IPSec router. When the <b>Addr Type</b> field is configured to <b>Range Address</b>, enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. When the <b>Address Type</b> field is configured to <b>Subnet Address</b>, enter a (static) IP address on the network behind the remote IPSec router.</p>
Ending IP Address/Subnet Mask	<p>When the <b>Address Type</b> field is configured to <b>Single Address</b>, this field is N/A. When the <b>Address Type</b> field is configured to <b>Range Address</b>, enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the <b>Address Type</b> field is configured to <b>Subnet Address</b>, enter a subnet mask on the network behind the remote IPSec router.</p>
Gateway Policy Information	

**Table 105** VPN Rules (Manual) Edit (continued)

LABEL	DESCRIPTION
My ZyWALL	<p>When the ZyWALL is in router mode, enter the WAN IP address or the domain name of your ZyWALL or leave the field set to <b>0.0.0.0</b>.</p> <p>For a ZyWALL with multiple WAN ports, the following applies if the <b>My ZyWALL</b> field is configured as <b>0.0.0.0</b>:</p> <ul style="list-style-type: none"> <li>• When the WAN port operation mode is set to <b>Active/Passive</b>, the ZyWALL uses the IP address (static or dynamic) of the WAN port that is in use.</li> <li>• When the WAN port operation mode is set to <b>Active/Active</b>, the ZyWALL uses the IP address (static or dynamic) of the primary (highest priority) WAN port to set up the VPN tunnel as long as the corresponding WAN1 or WAN2 connection is up. If the corresponding WAN1 or WAN2 connection goes down, the ZyWALL uses the IP address of the other WAN port.</li> <li>• If both WAN connections go down, the ZyWALL uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect. See the chapter on WAN for details on dial backup and traffic redirect.</li> </ul> <p>A ZyWALL with a single WAN port uses its current WAN IP address (static or dynamic) in setting up the VPN tunnel if you leave this field as <b>0.0.0.0</b>. If the WAN connection goes down, the ZyWALL uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect. The VPN tunnel has to be rebuilt if this IP address changes.</p> <p>When the ZyWALL is in bridge mode, this field is read-only and displays the ZyWALL's IP address.</p>
Remote Gateway Addr	Type the WAN IP address or the domain name (up to 31 characters) of the IPSec router with which you're making the VPN connection.
Manual Proposal	
SPI	Type a unique <b>SPI</b> (Security Parameter Index) from one to four characters long. Valid Characters are "0, 1, 2, 3, 4, 5, 6, 7, 8, and 9".
Encapsulation Mode	Select <b>Tunnel</b> mode or <b>Transport</b> mode from the drop-down list box.
Active Protocol	<p>Select <b>ESP</b> if you want to use ESP (Encapsulation Security Payload). The ESP protocol (RFC 2406) provides encryption as well as some of the services offered by <b>AH</b>. If you select <b>ESP</b> here, you must select options from the <b>Encryption Algorithm</b> and <b>Authentication Algorithm</b> fields (described next).</p> <p>Select <b>AH</b> if you want to use AH (Authentication Header Protocol). The AH protocol (RFC 2402) was designed for integrity, authentication, sequence integrity (reply resistance), and non-repudiation but not for confidentiality, for which the ESP was designed. If you select <b>AH</b> here, you must select options from the <b>Authentication Algorithm</b> field (described next).</p>
Encryption Algorithm	<p>Select <b>DES</b>, <b>3DES</b> or <b>NULL</b> from the drop-down list box.</p> <p>When <b>DES</b> is used for data communications, both sender and receiver must know the <b>Encryption Key</b>, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (<b>3DES</b>) is a variation on DES that uses a 168-bit key. As a result, <b>3DES</b> is more secure than <b>DES</b>. It also requires more processing power, resulting in increased latency and decreased throughput. Select <b>NULL</b> to set up a tunnel without encryption. When you select <b>NULL</b>, you do not enter an encryption key.</p>
Authentication Algorithm	Select <b>SHA1</b> or <b>MD5</b> from the drop-down list box. <b>MD5</b> (Message Digest 5) and <b>SHA1</b> (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The <b>SHA1</b> algorithm is generally considered stronger than <b>MD5</b> , but is slower. Select <b>MD5</b> for minimal security and <b>SHA-1</b> for maximum security.

**Table 105** VPN Rules (Manual) Edit (continued)

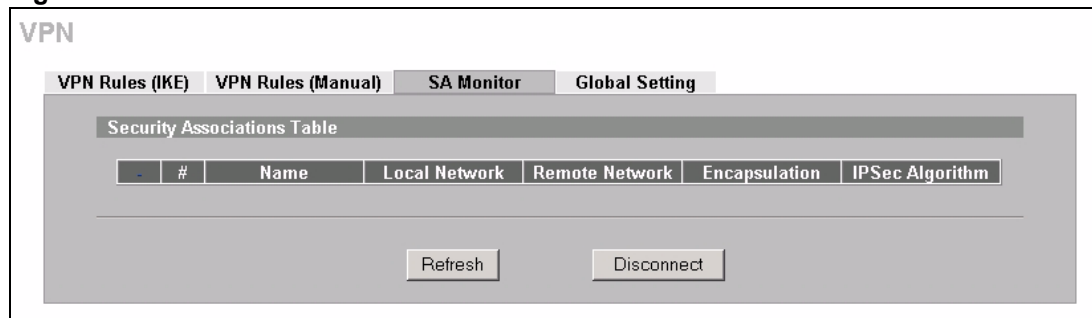
LABEL	DESCRIPTION
Encryption Key	This field is applicable when you select <b>ESP</b> in the <b>Active Protocol</b> field above. With <b>DES</b> , type a unique key 8 characters long. With <b>3DES</b> , type a unique key 24 characters long. Any characters may be used, including spaces, but trailing spaces are truncated.
Authentication Key	Type a unique authentication key to be used by IPSec if applicable. Enter 16 characters for <b>MD5</b> authentication or 20 characters for <b>SHA-1</b> authentication. Any characters may be used, including spaces, but trailing spaces are truncated.
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

## 19.16 VPN SA Monitor

In the web configurator, click **VPN** and the **SA Monitor** tab. Use this screen to display and manage active VPN connections.

A Security Association (SA) is the group of security settings related to a specific VPN tunnel. This screen displays active VPN connections. Use **Refresh** to display active VPN connections. This screen is read-only.

**Figure 156** VPN: SA Monitor



The following table describes the labels in this screen.

**Table 106** VPN: SA Monitor

LABEL	DESCRIPTION
#	This is the security association index number.
Name	This field displays the identification name for this VPN policy.
Local Network	This field displays the IP address of the computer using the VPN IPSec feature of your ZyWALL.
Remote Network	This field displays IP address (in a range) of computers on the remote network behind the remote IPSec router.
Encapsulation	This field displays <b>Tunnel</b> or <b>Transport</b> mode.

**Table 106** VPN: SA Monitor (continued)

LABEL	DESCRIPTION
IPSec Algorithm	This field displays the security protocols used for an SA. Both AH and ESP increase ZyWALL processing requirements and communications latency (delay).
Refresh	Click <b>Refresh</b> to display the current active VPN connection(s).
Disconnect	Select a security association index number that you want to disconnect and then click <b>Disconnect</b> .

## 19.17 VPN Global Setting

Click **VPN**, then the **Global Setting** tab to open the **VPN Global Setting** screen. Use this screen to change your ZyWALL's global settings.

**Figure 157** VPN: Global Setting

The following table describes the labels in this screen.

**Table 107** VPN: Global Setting

LABEL	DESCRIPTION
Output Idle Timer	When traffic is sent to a remote IPSec router from which no reply is received after the specified time period, the ZyWALL checks the VPN connectivity. If the remote IPSec router does not reply, the ZyWALL automatically disconnects the VPN tunnel. Enter the time period (between 30 and 3600 seconds) to wait before the ZyWALL checks all of the VPN connections to remote IPSec routers. Enter <b>0</b> to disable this feature.
Input Idle Timer	When no traffic is received from a remote IPSec router after the specified time period, the ZyWALL checks the VPN connectivity. If the remote IPSec router does not reply, the ZyWALL automatically disconnects the VPN tunnel. Enter the time period (between 30 and 3600 seconds) to wait before the ZyWALL checks all of the VPN connections to remote IPSec routers. Enter <b>0</b> to disable this feature.

**Table 107** VPN: Global Setting (continued)

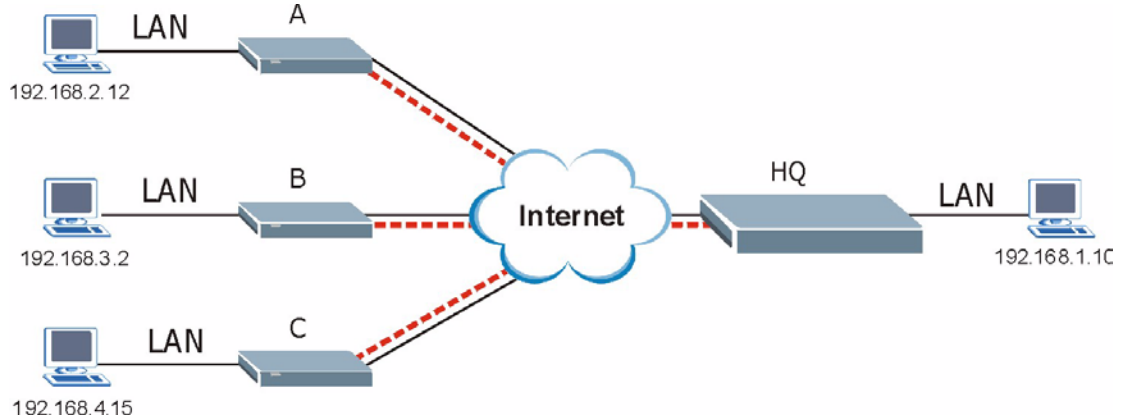
LABEL	DESCRIPTION
Gateway Domain Name Update Timer	This field is applicable when you enter a domain name to identify the ZyWALL and/or the remote secure gateway. Enter the time period (between 2 and 60 minutes) to wait before the ZyWALL updates the domain name and IP address mapping through a DNS server. The ZyWALL rebuilds the VPN tunnel if it finds that the domain name is now using a different IP address (any users of the VPN tunnel will be temporarily disconnected). Enter <b>0</b> to disable this feature.
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 19.18 Telecommuter VPN/IPSec Examples

The following examples show how multiple telecommuters can make VPN connections to a single ZyWALL at headquarters. The telecommuters use IPSec routers with dynamic WAN IP addresses. The ZyWALL at headquarters has a static public IP address.

### 19.18.1 Telecommuters Sharing One VPN Rule Example

See the following figure and table for an example configuration that allows multiple telecommuters (**A**, **B** and **C** in the figure) to use one VPN rule to simultaneously access a ZyWALL at headquarters (**HQ** in the figure). The telecommuters do not have domain names mapped to the WAN IP addresses of their IPSec routers. The telecommuters must all use the same IPSec parameters but the local IP addresses (or ranges of addresses) should not overlap.

**Figure 158** Telecommuters Sharing One VPN Rule Example**Table 108** Telecommuters Sharing One VPN Rule Example

FIELDS	TELECOMMUTERS	HEADQUARTERS
My ZyWALL:	0.0.0.0 (dynamic IP address assigned by the ISP)	Public static IP address
Remote Gateway Address:	Public static IP address	0.0.0.0 With this IP address only the telecommuter can initiate the IPSec tunnel.
Local Network - Single IP Address:	Telecommuter A: 192.168.2.12 Telecommuter B: 192.168.3.2 Telecommuter C: 192.168.4.15	192.168.1.10
Remote Network - Single IP Address:	192.168.1.10	Not Applicable

## 19.18.2 Telecommuters Using Unique VPN Rules Example

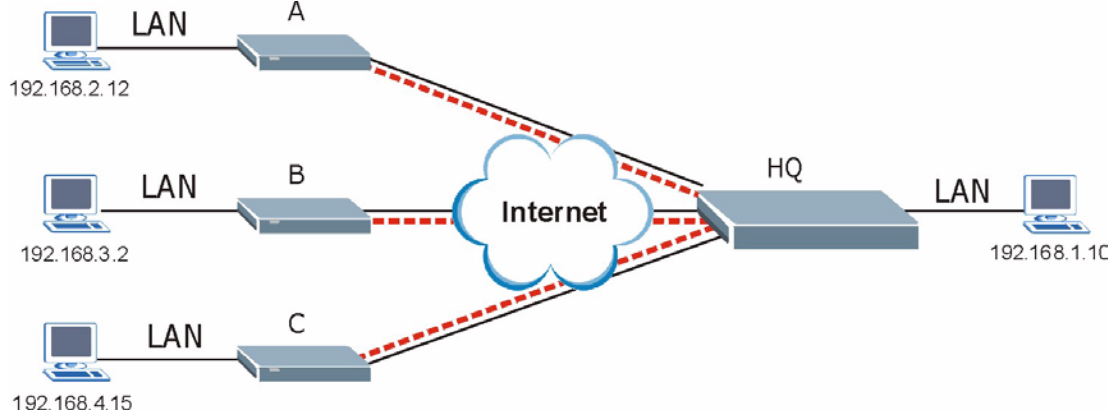
In this example the telecommuters (A, B and C in the figure) use IPSec routers with domain names that are mapped to their dynamic WAN IP addresses (use Dynamic DNS to do this).

With aggressive negotiation mode (see [Section 19.8.1 on page 314](#)), the ZyWALL can use the ID types and contents to distinguish between VPN rules. Telecommuters can each use a separate VPN rule to simultaneously access a ZyWALL at headquarters. They can use different IPSec parameters. The local IP addresses (or ranges of addresses) of the rules configured on the ZyWALL at headquarters can overlap. The local IP addresses of the rules configured on the telecommuters' IPSec routers should not overlap.

See the following table and figure for an example where three telecommuters each use a different VPN rule for a VPN connection with a ZyWALL located at headquarters. The ZyWALL at headquarters (HQ in the figure) identifies each incoming SA by its ID type and content and uses the appropriate VPN rule to establish the VPN connection.

The ZyWALL at headquarters can also initiate VPN connections to the telecommuters since it can find the telecommuters by resolving their domain names.

**Figure 159** Telecommuters Using Unique VPN Rules Example



**Table 109** Telecommuters Using Unique VPN Rules Example

TELECOMMUTERS	HEADQUARTERS
<b>All Telecommuter Rules:</b>	All Headquarters Rules:
My ZyWALL 0.0.0.0	My ZyWALL: bigcompanyhq.com
Remote Gateway Address: bigcompanyhq.com	Local Network - Single IP Address: 192.168.1.10
Remote Network - Single IP Address: 192.168.1.10	Local ID Type: E-mail
Peer ID Type: E-mail	Local ID Content: bob@bigcompanyhq.com
Peer ID Content: bob@bigcompanyhq.com	
<b>Telecommuter A (telecommutera.dydns.org)</b>	Headquarters ZyWALL Rule 1:
Local ID Type: IP	Peer ID Type: IP
Local ID Content: 192.168.2.12	Peer ID Content: 192.168.2.12
Local IP Address: 192.168.2.12	Remote Gateway Address: telecommutera.dydns.org
	Remote Address 192.168.2.12
<b>Telecommuter B (telecommuterb.dydns.org)</b>	Headquarters ZyWALL Rule 2:
Local ID Type: DNS	Peer ID Type: DNS
Local ID Content: telecommuterb.com	Peer ID Content: telecommuterb.com
Local IP Address: 192.168.3.2	Remote Gateway Address: telecommuterb.dydns.org
	Remote Address 192.168.3.2
<b>Telecommuter C (telecommuterc.dydns.org)</b>	Headquarters ZyWALL Rule 3:
Local ID Type: E-mail	Peer ID Type: E-mail
Local ID Content: myVPN@myplace.com	Peer ID Content: myVPN@myplace.com

**Table 109** Telecommuters Using Unique VPN Rules Example

TELECOMMUTERS	HEADQUARTERS
Local IP Address: 192.168.4.15	Remote Gateway Address: telecommuterc.dydns.org
	Remote Address 192.168.4.15

## 19.19 VPN and Remote Management

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





# CHAPTER 20

## Certificates

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

### 20.1 Certificates Overview

The ZyWALL can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. You can use the ZyWALL to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

In public-key encryption and decryption, each host has two keys. One key is public and can be made openly available; the other key is private and must be kept secure. Public-key encryption in general works as follows.

- 1 Tim wants to send a private message to Jenny. Tim generates a public key pair. What is encrypted with one key can only be decrypted using the other.
- 2 Tim keeps the private key and makes the public key openly available.
- 3 Tim uses his private key to encrypt the message and sends it to Jenny.
- 4 Jenny receives the message and uses Tim's public key to decrypt it.
- 5 Additionally, Jenny uses her own private key to encrypt a message and Tim uses Jenny's public key to decrypt the message.

The ZyWALL uses certificates based on public-key cryptology to authenticate users attempting to establish a connection, not to encrypt the data that you send after establishing a connection. The method used to secure the data that you send through an established connection depends on the type of connection. For example, a VPN tunnel might use the triple DES encryption algorithm.

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

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

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

### 20.1.1 Advantages of Certificates

Certificates offer the following benefits.

- The ZyWALL only has to store the certificates of the certification authorities that you decide to trust, no matter how many devices you need to authenticate.
- Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

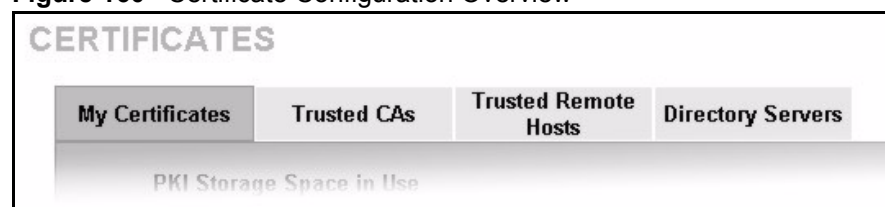
## 20.2 Self-signed Certificates

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

## 20.3 Configuration Summary

This section summarizes how to manage certificates on the ZyWALL.

**Figure 160** Certificate Configuration Overview



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

Use the **Trusted CA** screens to save CA certificates to the ZyWALL.

Use the **Trusted Remote Hosts** screens to import self-signed certificates.

Use the **Directory Servers** screen to configure a list of addresses of directory servers (that contain lists of valid and revoked certificates).

## 20.4 My Certificates

Click **SECURITY, CERTIFICATES, My Certificates** to open the **My Certificates** screen. This is the ZyWALL's summary list of certificates and certification requests. Certificates display in black and certification requests display in gray.

**Figure 161** My Certificates

**CERTIFICATES**

My Certificates    Trusted CAs    Trusted Remote Hosts    Directory Servers

PKI Storage Space in Use

0%  2%  100%

Replace Factory Default Certificate

Factory Default Certificate Name: auto\_generated\_self\_signed\_cert

The factory default certificate is common to all ZyWALL models. Click Replace to create a certificate using your ZyWALL's MAC address that will be specific to this device.

Replace

My Certificates

#	Name	Type	Subject	Issuer	Valid From	Valid To	Modify
1	auto_generated_self_signed_cert	*SELF	CN=ZyWALL 70 Factory Default Certificate	CN=ZyWALL 70 Factory Default Certificate	2000 Jan 1st, 00:00:00 GMT	2030 Jan 1st, 00:00:00 GMT	
2	Corey_ser	REQ	CN=172.1.2.3, O=ZyXEL, C=TW	N/A	N/A	N/A	
3	John_Smith	SELF	CN=johns@bigcompany.com, OU=Sales, O=Big Company, C=USA	CN=johns@bigcompany.com, OU=Sales, O=Big Company, C=USA	2004 Jun 28th, 02:09:06 GMT	2007 Jun 29th, 02:09:06 GMT	

Import    Create    Refresh

The following table describes the labels in this screen.

**Table 110** My Certificates

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the ZyWALL's PKI storage space that is currently in use. The bar turns from green to red when the maximum is being approached. When the bar is red, you should consider deleting expired or unnecessary certificates before adding more certificates.
Replace	This button displays when the ZyWALL has the factory default certificate. The factory default certificate is common to all ZyWALLs that use certificates. ZyXEL recommends that you use this button to replace the factory default certificate with one that uses your ZyWALL's MAC address.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.

**Table 110** My Certificates (continued)

LABEL	DESCRIPTION
Type	<p>This field displays what kind of certificate this is.</p> <p><b>REQ</b> represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the <b>My Certificate Import</b> screen to import the certificate and replace the request.</p> <p><b>SELF</b> represents a self-signed certificate.</p> <p><b>*SELF</b> represents the default self-signed certificate, which the ZyWALL uses to sign imported trusted remote host certificates.</p> <p><b>CERT</b> represents a certificate issued by a certification authority.</p>
Subject	<p>This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.</p>
Issuer	<p>This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the <b>Subject</b> field.</p>
Valid From	<p>This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.</p>
Valid To	<p>This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.</p>
Modify	<p>Click the details icon to open a screen with an in-depth list of information about the certificate.</p> <p>Click the delete icon to remove the certificate. A window displays asking you to confirm that you want to delete the certificate.</p> <p>You cannot delete a certificate that one or more features is configured to use.</p> <p>Do the following to delete a certificate that shows <b>*SELF</b> in the <b>Type</b> field.</p> <ol style="list-style-type: none"> <li>1. Make sure that no other features, such as HTTPS, VPN, SSH are configured to use the <b>*SELF</b> certificate.</li> <li>2. Click the details icon next to another self-signed certificate (see the description on the <b>Create</b> button if you need to create a self-signed certificate).</li> <li>3. Select the <b>Default self-signed certificate which signs the imported remote host certificates</b> check box.</li> <li>4. Click <b>Apply</b> to save the changes and return to the <b>My Certificates</b> screen.</li> <li>5. The certificate that originally showed <b>*SELF</b> displays <b>SELF</b> and you can delete it now.</li> </ol> <p>Note that subsequent certificates move up by one when you take this action</p>
Import	<p>Click <b>Import</b> to open a screen where you can save the certificate that you have enrolled from a certification authority from your computer to the ZyWALL.</p>
Create	<p>Click <b>Create</b> to go to the screen where you can have the ZyWALL generate a certificate or a certification request.</p>
Refresh	<p>Click <b>Refresh</b> to display the current validity status of the certificates.</p>

## 20.5 My Certificate Import

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

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

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

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

### 20.5.1 Certificate File Formats

The certification authority certificate that you want to import has to be in one of these file formats:

- **Binary X.509:** This is an ITU-T recommendation that defines the formats for X.509 certificates.
- **PEM (Base-64) encoded X.509:** This Privacy Enhanced Mail format uses 64 ASCII characters to convert a binary X.509 certificate into a printable form.
- **Binary PKCS#7:** This is a standard that defines the general syntax for data (including digital signatures) that may be encrypted. The ZyWALL currently allows the importation of a PKCS#7 file that contains a single certificate.
- **PEM (Base-64) encoded PKCS#7:** This Privacy Enhanced Mail (PEM) format uses 64 ASCII characters to convert a binary PKCS#7 certificate into a printable form.

**Figure 162** My Certificate Import



The following table describes the labels in this screen.

**Table 111** My Certificate Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click <b>Browse</b> to find it.
Browse	Click <b>Browse</b> to find the certificate file you want to upload.
Apply	Click <b>Apply</b> to save the certificate on the ZyWALL.
Cancel	Click <b>Cancel</b> to quit and return to the <b>My Certificates</b> screen.

## 20.6 My Certificate Create

Click **SECURITY, CERTIFICATES, My Certificates** and then **Create** to open the **My Certificate Create** screen. Use this screen to have the ZyWALL create a self-signed certificate, enroll a certificate with a certification authority or generate a certification request.

**Figure 163** My Certificate Create

**CERTIFICATES - MY CERTIFICATE - CREATE**

Certificate Name

**Subject Information**

Common Name

Host IP Address

Host Domain Name

E-Mail

Organizational Unit

Organization

Country

Key Length  bits

**Enrollment Options**

Create a self-signed certificate

Create a certification request and save it locally for later manual enrollment

Create a certification request and enroll for a certificate immediately online

Enrollment Protocol

CA Server Address

CA Certificate  (See [Trusted CAs](#))

Request Authentication Key

The following table describes the labels in this screen.

**Table 112** My Certificate Create

LABEL	DESCRIPTION
Certificate Name	Type up to 31 ASCII characters (not including spaces) to identify this certificate.
Subject Information	Use these fields to record information that identifies the owner of the certificate. You do not have to fill in every field, although the <b>Common Name</b> is mandatory. The certification authority may add fields (such as a serial number) to the subject information when it issues a certificate. It is recommended that each certificate have unique subject information.
Common Name	Select a radio button to identify the certificate's owner by IP address, domain name or e-mail address. Type the IP address (in dotted decimal notation), domain name or e-mail address in the field provided. The domain name or e-mail address can be up to 31 ASCII characters. The domain name or e-mail address is for identification purposes only and can be any string.
Organizational Unit	Type up to 127 characters to identify the organizational unit or department to which the certificate owner belongs. You may use any character, including spaces, but the ZyWALL drops trailing spaces.
Organization	Type up to 127 characters to identify the company or group to which the certificate owner belongs. You may use any character, including spaces, but the ZyWALL drops trailing spaces.



**Table 112** My Certificate Create (continued)

LABEL	DESCRIPTION
Country	Type up to 127 characters to identify the nation where the certificate owner is located. You may use any character, including spaces, but the ZyWALL drops trailing spaces.
Key Length	Select a number from the drop-down list box to determine how many bits the key should use (512 to 2048). The longer the key, the more secure it is. A longer key also uses more PKI storage space.
Enrollment Options	These radio buttons deal with how and when the certificate is to be generated.
Create a self-signed certificate	Select <b>Create a self-signed certificate</b> to have the ZyWALL generate the certificate and act as the Certification Authority (CA) itself. This way you do not need to apply to a certification authority for certificates.
Create a certification request and save it locally for later manual enrollment	Select <b>Create a certification request and save it locally for later manual enrollment</b> to have the ZyWALL generate and store a request for a certificate. Use the <b>My Certificate Details</b> screen to view the certification request and copy it to send to the certification authority. Copy the certification request from the <b>My Certificate Details</b> screen (see <a href="#">Section 20.7 on page 350</a> ) and then send it to the certification authority.
Create a certification request and enroll for a certificate immediately online	Select <b>Create a certification request and enroll for a certificate immediately online</b> to have the ZyWALL generate a request for a certificate and apply to a certification authority for a certificate. You must have the certification authority's certificate already imported in the <b>Trusted CAs</b> screen. When you select this option, you must select the certification authority's enrollment protocol and the certification authority's certificate from the drop-down list boxes and enter the certification authority's server address. You also need to fill in the <b>Reference Number</b> and <b>Key</b> if the certification authority requires them.
Enrollment Protocol	Select the certification authority's enrollment protocol from the drop-down list box. <b>Simple Certificate Enrollment Protocol (SCEP)</b> is a TCP-based enrollment protocol that was developed by VeriSign and Cisco. <b>Certificate Management Protocol (CMP)</b> is a TCP-based enrollment protocol that was developed by the Public Key Infrastructure X.509 working group of the Internet Engineering Task Force (IETF) and is specified in RFC 2510.
CA Server Address	Enter the IP address (or URL) of the certification authority server.
CA Certificate	Select the certification authority's certificate from the <b>CA Certificate</b> drop-down list box. You must have the certification authority's certificate already imported in the <b>Trusted CAs</b> screen. Click <b>Trusted CAs</b> to go to the <b>Trusted CAs</b> screen where you can view (and manage) the ZyWALL's list of certificates of trusted certification authorities.
Request Authentication	When you select <b>Create a certification request and enroll for a certificate immediately online</b> , the certification authority may want you to include a reference number and key to identify you when you send a certification request. Fill in both the <b>Reference Number</b> and the <b>Key</b> fields if your certification authority uses CMP enrollment protocol. Just fill in the <b>Key</b> field if your certification authority uses the SCEP enrollment protocol.
Key	Type the key that the certification authority gave you.
Apply	Click <b>Apply</b> to begin certificate or certification request generation.
Cancel	Click <b>Cancel</b> to quit and return to the <b>My Certificates</b> screen.

After you click **Apply** in the **My Certificate Create** screen, you see a screen that tells you the ZyWALL is generating the self-signed certificate or certification request.

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

If you configured the **My Certificate Create** screen to have the ZyWALL enroll a certificate and the certificate enrollment is not successful, you see a screen with a **Return** button that takes you back to the **My Certificate Create** screen. Click **Return** and check your information in the **My Certificate Create** screen. Make sure that the certification authority information is correct and that your Internet connection is working properly if you want the ZyWALL to enroll a certificate online.

## 20.7 My Certificate Details

Click **SECURITY, CERTIFICATES**, and then **My Certificates** to open the **My Certificates** screen (see [Figure 161 on page 344](#)). Click the details icon to open the **My Certificate Details** screen. You can use this screen to view in-depth certificate information and change the certificate's name. In the case of a self-signed certificate, you can set it to be the one that the ZyWALL uses to sign the trusted remote host certificates that you import to the ZyWALL.



The following table describes the labels in this screen.

**Table 113** My Certificate Details

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this certificate. You may use any character (not including spaces).
Property Default self-signed certificate which signs the imported remote host certificates.	Select this check box to have the ZyWALL use this certificate to sign the trusted remote host certificates that you import to the ZyWALL. This check box is only available with self-signed certificates.  If this check box is already selected, you cannot clear it in this screen, you must select this check box in another self-signed certificate's details screen. This automatically clears the check box in the details screen of the certificate that was previously set to sign the imported trusted remote host certificates.
Certification Path	Click the <b>Refresh</b> button to have this read-only text box display the hierarchy of certification authorities that validate the certificate (and the certificate itself).  If the issuing certification authority is one that you have imported as a trusted certification authority, it may be the only certification authority in the list (along with the certificate itself). If the certificate is a self-signed certificate, the certificate itself is the only one in the list. The ZyWALL does not trust the certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.
Refresh	Click <b>Refresh</b> to display the certification path.
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). "X.509" means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority or generated by the ZyWALL.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country.  With self-signed certificates, this is the same as the <b>Subject Name</b> field.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. The ZyWALL uses rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Some certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the ZyWALL uses RSA encryption) and the length of the key set in bits (1024 bits for example).

**Table 113** My Certificate Details (continued)

LABEL	DESCRIPTION
Subject Alternative Name	This field displays the certificate owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path.
MD5 Fingerprint	This is the certificate's message digest that the ZyWALL calculated using the MD5 algorithm.
SHA1 Fingerprint	This is the certificate's message digest that the ZyWALL calculated using the SHA1 algorithm.
Certificate in PEM (Base-64) Encoded Format	<p>This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form.</p> <p>You can copy and paste a certification request into a certification authority's web page, an e-mail that you send to the certification authority or a text editor and save the file on a management computer for later manual enrollment.</p> <p>You can copy and paste a certificate into an e-mail to send to friends or colleagues or you can copy and paste a certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).</p>
Export	Click this button and then <b>Save</b> in the <b>File Download</b> screen. The <b>Save As</b> screen opens, browse to the location that you want to use and click <b>Save</b> .
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL. You can only change the name, except in the case of a self-signed certificate, which you can also set to be the default self-signed certificate that signs the imported trusted remote host certificates.
Cancel	Click <b>Cancel</b> to quit and return to the <b>My Certificates</b> screen.

## 20.8 Trusted CAs

Click **SECURITY, CERTIFICATES, Trusted CAs** to open the **Trusted CAs** screen. This screen displays a summary list of certificates of the certification authorities that you have set the ZyWALL to accept as trusted. The ZyWALL accepts any valid certificate signed by a certification authority on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certification authorities.

Figure 165 Trusted CAs

The screenshot shows the 'CERTIFICATES' management interface with the 'Trusted CAs' tab selected. At the top, there are four tabs: 'My Certificates', 'Trusted CAs', 'Trusted Remote Hosts', and 'Directory Servers'. Below the tabs is a 'PKI Storage Space in Use' progress bar showing 4% usage. A table titled 'Trusted CA Certificates' lists two certificates. The first certificate is 'SSH-CA' with a valid period from 2001 Aug 1st to 2004 Aug 1st. The second certificate is 'ZyXEL-RootCA' with a valid period from 2003 Mar 13th to 2004 Mar 13th, which is marked as expired. Below the table are 'Import' and 'Refresh' buttons.

#	Name	Subject	Issuer	Valid From	Valid To	CRL Issuer	Modify
1	SSH-CA	CN=SSH Test CA 1 No Liabilities, O=SSH Communications Security Corp, C=FI	CN=SSH Test CA 1 No Liabilities, O=SSH Communications Security Corp, C=FI	2001 Aug 1st, 07:08:32 GMT	2004 Aug 1st, 07:08:32 GMT	No	
2	ZyXEL-RootCA	OU=RootCA, OU=VPN Department, O=Zyxel, C=TW	OU=RootCA, OU=VPN Department, O=Zyxel, C=TW	2003 Mar 13th, 03:13:31 GMT	2004 Mar 13th, 03:13:31 GMT (Expired!)	No	

The following table describes the labels in this screen.

Table 114 Trusted CAs

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the ZyWALL's PKI storage space that is currently in use. The bar turns from green to red when the maximum is being approached. When the bar is red, you should consider deleting expired or unnecessary certificates before adding more certificates.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. With self-signed certificates, this is the same information as in the <b>Subject</b> field.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.

**Table 114** Trusted CAs (continued)

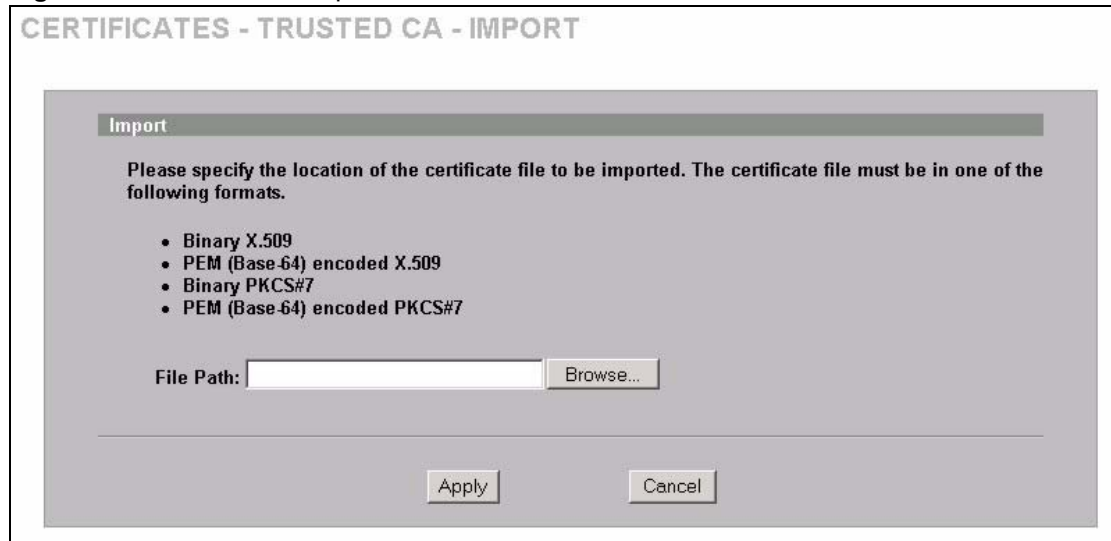
LABEL	DESCRIPTION
CRL Issuer	This field displays Yes if the certification authority issues Certificate Revocation Lists for the certificates that it has issued and you have selected the <b>Issues certificate revocation lists (CRL)</b> check box in the certificate's details screen to have the ZyWALL check the CRL before trusting any certificates issued by the certification authority. Otherwise the field displays "No".
Modify	Click the details icon to open a screen with an in-depth list of information about the certificate. Click the delete icon to remove the certificate. A window displays asking you to confirm that you want to delete the certificates. Note that subsequent certificates move up by one when you take this action.
Import	Click <b>Import</b> to open a screen where you can save the certificate of a certification authority that you trust, from your computer to the ZyWALL.
Refresh	Click this button to display the current validity status of the certificates.

## 20.9 Trusted CA Import

Click **SECURITY, CERTIFICATES, Trusted CAs** to open the **Trusted CAs** screen and then click **Import** to open the **Trusted CA Import** screen. Follow the instructions in this screen to save a trusted certification authority's certificate to the ZyWALL.

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

**Figure 166** Trusted CA Import



The following table describes the labels in this screen.

**Table 115** Trusted CA Import

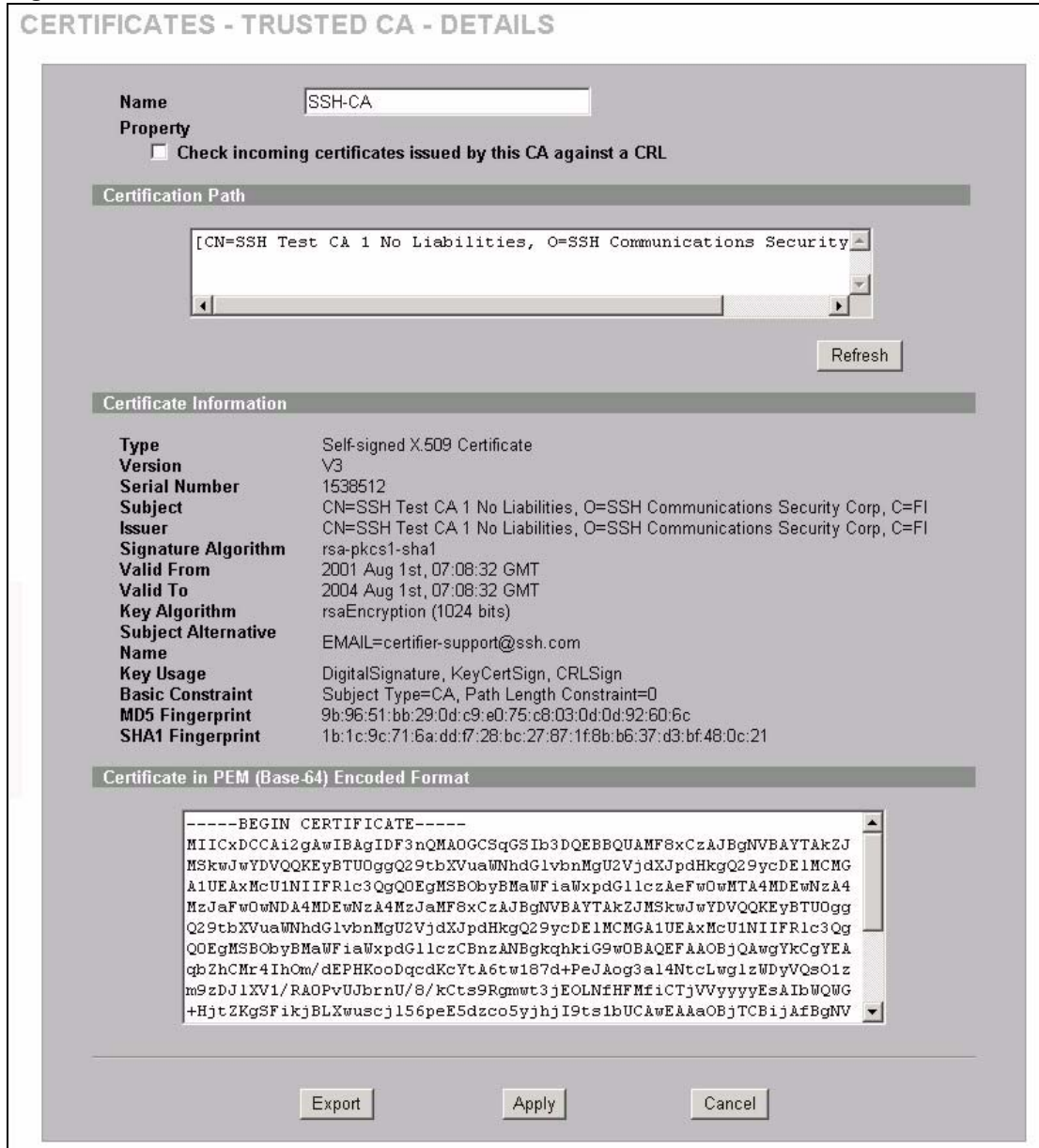
<b>LABEL</b>	<b>DESCRIPTION</b>
File Path	Type in the location of the file you want to upload in this field or click <b>Browse</b> to find it.
Browse	Click <b>Browse</b> to find the certificate file you want to upload.
Apply	Click <b>Apply</b> to save the certificate on the ZyWALL.
Cancel	Click <b>Cancel</b> to quit and return to the <b>Trusted CAs</b> screen.

## 20.10 Trusted CA Details

Click **SECURITY, CERTIFICATES, Trusted CAs** to open the **Trusted CAs** screen. Click the details icon to open the **Trusted CA Details** screen. Use this screen to view in-depth information about the certification authority's certificate, change the certificate's name and set whether or not you want the ZyWALL to check a certification authority's list of revoked certificates before trusting a certificate issued by the certification authority.



**Figure 167** Trusted CA Details



The following table describes the labels in this screen.

**Table 116** Trusted CA Details

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this key certificate. You may use any character (not including spaces).
Property Check incoming certificates issued by this CA against a CRL	Select this check box to have the ZyWALL check incoming certificates that are issued by this certification authority against a Certificate Revocation List (CRL). Clear this check box to have the ZyWALL not check incoming certificates that are issued by this certification authority against a Certificate Revocation List (CRL).

**Table 116** Trusted CA Details (continued)

LABEL	DESCRIPTION
Certification Path	Click the <b>Refresh</b> button to have this read-only text box display the end entity's certificate and a list of certification authority certificates that shows the hierarchy of certification authorities that validate the end entity's certificate. If the issuing certification authority is one that you have imported as a trusted certification authority, it may be the only certification authority in the list (along with the end entity's own certificate). The ZyWALL does not trust the end entity's certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.
Refresh	Click <b>Refresh</b> to display the certification path.
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the certificate's owner signed the certificate (not a certification authority). X.509 means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the certification authority.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as Common Name, Organizational Unit, Organization and Country. With self-signed certificates, this is the same information as in the <b>Subject Name</b> field.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. Some certification authorities use rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Other certification authorities may use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the ZyWALL uses RSA encryption) and the length of the key set in bits (1024 bits for example).
Subject Alternative Name	This field displays the certificate's owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path.

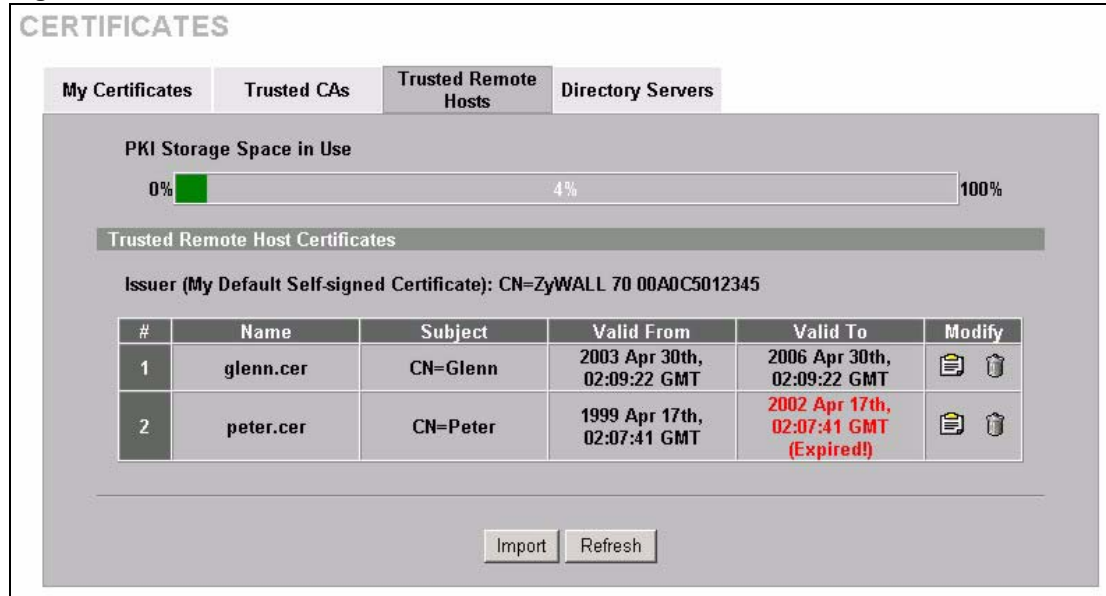
**Table 116** Trusted CA Details (continued)

LABEL	DESCRIPTION
CRL Distribution Points	This field displays how many directory servers with Lists of revoked certificates the issuing certification authority of this certificate makes available. This field also displays the domain names or IP addresses of the servers.
MD5 Fingerprint	This is the certificate's message digest that the ZyWALL calculated using the MD5 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate.
SHA1 Fingerprint	This is the certificate's message digest that the ZyWALL calculated using the SHA1 algorithm. You can use this value to verify with the certification authority (over the phone for example) that this is actually their certificate.
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form.  You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Export	Click this button and then <b>Save</b> in the <b>File Download</b> screen. The <b>Save As</b> screen opens, browse to the location that you want to use and click <b>Save</b> .
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL. You can only change the name and/or set whether or not you want the ZyWALL to check the CRL that the certification authority issues before trusting a certificate issued by the certification authority.
Cancel	Click <b>Cancel</b> to quit and return to the <b>Trusted CAs</b> screen.

## 20.11 Trusted Remote Hosts

Click **SECURITY, CERTIFICATES, Trusted Remote Hosts** to open the **Trusted Remote Hosts** screen. This screen displays a list of the certificates of peers that you trust but which are not signed by one of the certification authorities on the **Trusted CAs** screen.

You do not need to add any certificate that is signed by one of the certification authorities on the **Trusted CAs** screen since the ZyWALL automatically accepts any valid certificate signed by a trusted certification authority as being trustworthy.

**Figure 168** Trusted Remote Hosts

The following table describes the labels in this screen.

**Table 117** Trusted Remote Hosts

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the ZyWALL's PKI storage space that is currently in use. The bar turns from green to red when the maximum is being approached. When the bar is red, you should consider deleting expired or unnecessary certificates before adding more certificates.
Issuer (My Default Self-signed Certificate)	This field displays identifying information about the default self-signed certificate on the ZyWALL that the ZyWALL uses to sign the trusted remote host certificates.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Modify	Click the details icon to open a screen with an in-depth list of information about the certificate. Click the delete icon to remove the certificate. A window displays asking you to confirm that you want to delete the certificate. Note that subsequent certificates move up by one when you take this action.

**Table 117** Trusted Remote Hosts (continued)

LABEL	DESCRIPTION
Import	Click <b>Import</b> to open a screen where you can save the certificate of a remote host (which you trust) from your computer to the ZyWALL.
Refresh	Click this button to display the current validity status of the certificates.

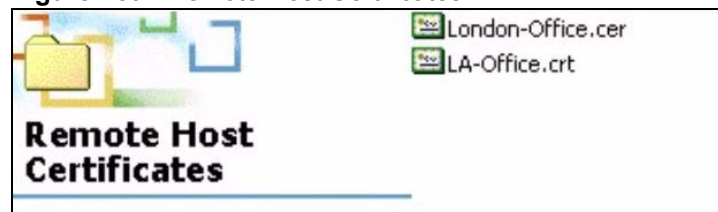
## 20.12 Verifying a Trusted Remote Host's Certificate

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

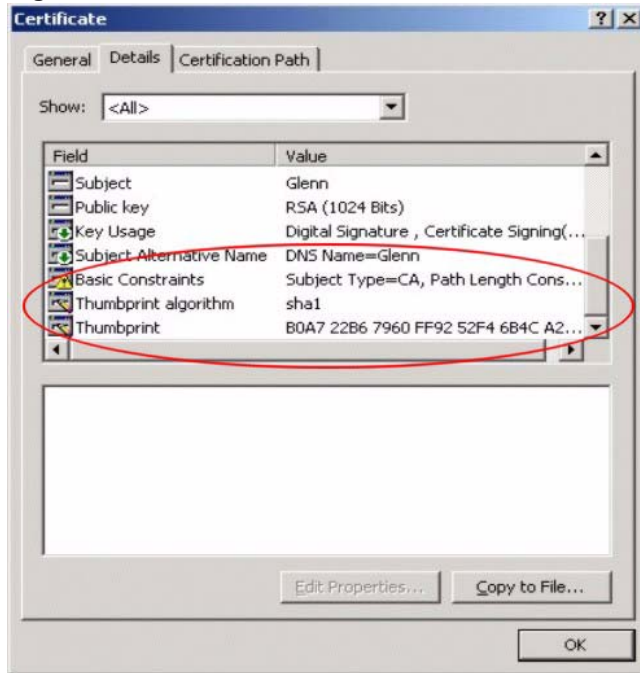
### 20.12.1 Trusted Remote Host Certificate Fingerprints

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

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

**Figure 169** Remote Host Certificates

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

**Figure 170** Certificate Details

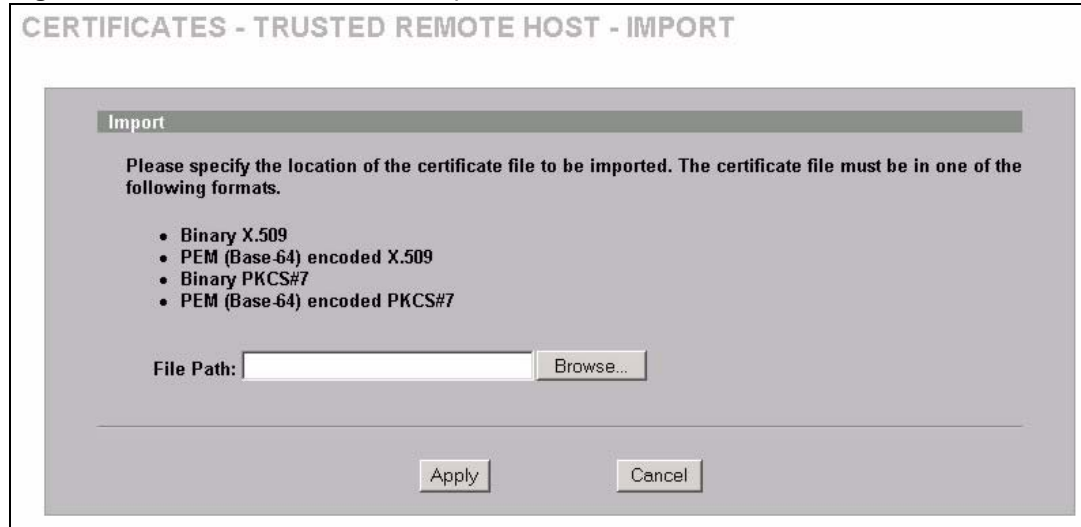
Verify (over the phone for example) that the remote host has the same information in the **Thumbprint Algorithm** and **Thumbprint** fields.

## 20.13 Trusted Remote Hosts Import

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

**Note:** The trusted remote host certificate must be a self-signed certificate; and you must remove any spaces from its filename before you can import it.

**Figure 171** Trusted Remote Host Import



The following table describes the labels in this screen.

**Table 118** Trusted Remote Host Import

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click <b>Browse</b> to find it.
Browse	Click <b>Browse</b> to find the certificate file you want to upload.
Apply	Click <b>Apply</b> to save the certificate on the ZyWALL.
Cancel	Click <b>Cancel</b> to quit and return to the <b>Trusted Remote Hosts</b> screen.

## 20.14 Trusted Remote Host Certificate Details

Click **SECURITY, CERTIFICATES, Trusted Remote Hosts** to open the **Trusted Remote Hosts** screen. Click the details icon to open the **Trusted Remote Host Details** screen. You can use this screen to view in-depth information about the trusted remote host's certificate and/or change the certificate's name.

Figure 172 Trusted Remote Host Details

**CERTIFICATES - TRUSTED REMOTE HOST - DETAILS**

**Name**

**Certification Path**

**Certificate Information**

<b>Type</b>	CA-signed X.509 Certificate
<b>Version</b>	V3
<b>Serial Number</b>	105175496253
<b>Subject</b>	CN=Glenn
<b>Issuer</b>	CN=ZyWALL 70 00A0C5012345
<b>Signature Algorithm</b>	rsa-pkcs1-sha1
<b>Valid From</b>	2003 Apr 30th, 02:09:22 GMT
<b>Valid To</b>	2006 Apr 30th, 02:09:22 GMT
<b>Key Algorithm</b>	rsaEncryption (1024 bits)
<b>Subject Alternative Name</b>	DNS=Glenn
<b>Key Usage</b>	DigitalSignature
<b>Basic Constraint</b>	Path Length Constraint=10
<b>MD5 Fingerprint</b>	ff:68:66:15:de:04:a5:35:a9:4a:49:97:fd:e9:55:13
<b>SHA1 Fingerprint</b>	c1:c1:38:34:70:a2:67:61:73:51:9b:71:7b:3d:ec:2d:26:70:b6:45

**Certificate in PEM (Base-64) Encoded Format**

The following table describes the labels in this screen.

Table 119 Trusted Remote Host Details

LABEL	DESCRIPTION
Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this key certificate. You may use any character (not including spaces).
Certification Path	Click the <b>Refresh</b> button to have this read-only text box display the end entity's own certificate and a list of certification authority certificates in the hierarchy of certification authorities that validate a certificate's issuing certification authority. For a trusted host, the list consists of the end entity's own certificate and the default self-signed certificate that the ZyWALL uses to sign remote host certificates.
Refresh	Click <b>Refresh</b> to display the certification path.



**Table 119** Trusted Remote Host Details (continued)

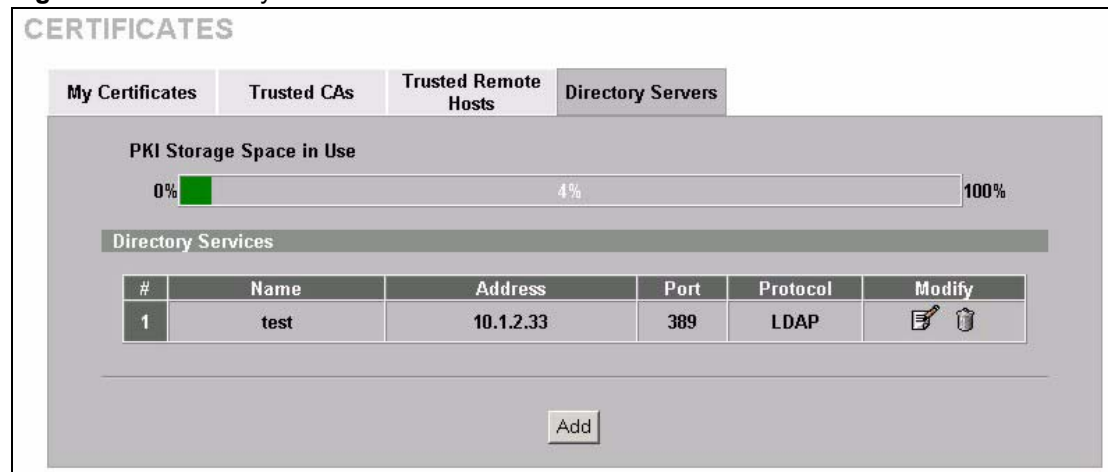
LABEL	DESCRIPTION
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. With trusted remote host certificates, this field always displays CA-signed. The ZyWALL is the Certification Authority that signed the certificate. X.509 means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate's identification number given by the device that created the certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).
Issuer	This field displays identifying information about the default self-signed certificate on the ZyWALL that the ZyWALL uses to sign the trusted remote host certificates.
Signature Algorithm	This field displays the type of algorithm that the ZyWALL used to sign the certificate, which is rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate's key pair (the ZyWALL uses RSA encryption) and the length of the key set in bits (1024 bits for example).
Subject Alternative Name	This field displays the certificate's owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate's key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority's certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certificate's path.
MD5 Fingerprint	This is the certificate's message digest that the ZyWALL calculated using the MD5 algorithm. You cannot use this value to verify that this is the remote host's actual certificate because the ZyWALL has signed the certificate; thus causing this value to be different from that of the remote hosts actual certificate. See <a href="#">Section 20.12 on page 361</a> for how to verify a remote host's certificate.
SHA1 Fingerprint	This is the certificate's message digest that the ZyWALL calculated using the SHA1 algorithm. You cannot use this value to verify that this is the remote host's actual certificate because the ZyWALL has signed the certificate; thus causing this value to be different from that of the remote hosts actual certificate. See <a href="#">Section 20.12 on page 361</a> for how to verify a remote host's certificate.

**Table 119** Trusted Remote Host Details (continued)

LABEL	DESCRIPTION
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form.  You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Export	Click this button and then <b>Save</b> in the <b>File Download</b> screen. The <b>Save As</b> screen opens, browse to the location that you want to use and click <b>Save</b> .
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL. You can only change the name of the certificate.
Cancel	Click <b>Cancel</b> to quit configuring this screen and return to the <b>Trusted Remote Hosts</b> screen.

## 20.15 Directory Servers

Click **SECURITY, CERTIFICATES, Directory Servers** to open the **Directory Servers** screen. This screen displays a summary list of directory servers (that contain lists of valid and revoked certificates) that have been saved into the ZyWALL. If you decide to have the ZyWALL check incoming certificates against the issuing certification authority's list of revoked certificates, the ZyWALL first checks the server(s) listed in the **CRL Distribution Points** field of the incoming certificate. If the certificate does not list a server or the listed server is not available, the ZyWALL checks the servers listed here.

**Figure 173** Directory Servers

The following table describes the labels in this screen.

**Table 120** Directory Servers

LABEL	DESCRIPTION
PKI Storage Space in Use	This bar displays the percentage of the ZyWALL's PKI storage space that is currently in use. The bar turns from green to red when the maximum is being approached. When the bar is red, you should consider deleting expired or unnecessary certificates before adding more certificates.
#	The index number of the directory server. The servers are listed in alphabetical order.
Name	This field displays the name used to identify this directory server.
Address	This field displays the IP address or domain name of the directory server.
Port	This field displays the port number that the directory server uses.
Protocol	This field displays the protocol that the directory server uses.
Modify	Click the details icon to open a screen where you can change the information about the directory server. Click the delete icon to remove the directory server entry. A window displays asking you to confirm that you want to delete the directory server. Note that subsequent certificates move up by one when you take this action.
Add	Click <b>Add</b> to open a screen where you can configure information about a directory server so that the ZyWALL can access it.

## 20.16 Directory Server Add or Edit

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

**Figure 174** Directory Server Add

**CERTIFICATES - DIRECTORY SERVER - ADD**

**Directory Service Setting**

Name

Access Protocol

Server Address  (Host Name or IP Address)

Server Port

**Login Setting**

Login

Password

The following table describes the labels in this screen.

**Table 121** Directory Server Add

LABEL	DESCRIPTION
Directory Service Setting	
Name	Type up to 31 ASCII characters (spaces are not permitted) to identify this directory server.
Access Protocol	Use the drop-down list box to select the access protocol used by the directory server. <b>LDAP</b> (Lightweight Directory Access Protocol) is a protocol over TCP that specifies how clients access directories of certificates and lists of revoked certificates. <sup>a</sup>
Server Address	Type the IP address (in dotted decimal notation) or the domain name of the directory server.
Server Port	This field displays the default server port number of the protocol that you select in the <b>Access Protocol</b> field. You may change the server port number if needed, however you must use the same server port number that the directory server uses. 389 is the default server port number for LDAP.
Login Setting	
Login	The ZyWALL may need to authenticate itself in order to assess the directory server. Type the login name (up to 31 ASCII characters) from the entity maintaining the directory server (usually a certification authority).
Password	Type the password (up to 31 ASCII characters) from the entity maintaining the directory server (usually a certification authority).
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Cancel	Click <b>Cancel</b> to quit configuring this screen and return to the <b>Directory Servers</b> screen.

- a. At the time of writing, LDAP is the only choice of directory server access protocol.



# CHAPTER 21

## Authentication Server

This chapter discusses how to configure the ZyWALL's authentication server feature.

### 21.1 Authentication Server Overview

A ZyWALL set to be a VPN extended authentication server can use either the local user database internal to the ZyWALL or an external RADIUS server for an unlimited number of users. The ZyWALL uses the same local user database for VPN extended authentication and wireless LAN security. See [Section 9.14 on page 189](#) for more information about RADIUS.

#### 21.1.1 Local User Database

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

#### 21.1.2 RADIUS

The ZyWALL can use an external RADIUS server to authenticate an unlimited number of users.

### 21.2 Local User Database

Click **SECURITY** and then **AUTH SERVER** to open the **Local User Database** screen. Use this screen to change your ZyWALL's local user list.

**Figure 175** Local User Database

**AUTHENTICATION SERVER**

Local User Database      RADIUS

User Database

#	Active	User Name	Password
1	<input type="checkbox"/>		
2	<input type="checkbox"/>		
3	<input type="checkbox"/>		
4	<input type="checkbox"/>		
5	<input type="checkbox"/>		
6	<input type="checkbox"/>		
7	<input type="checkbox"/>		
8	<input type="checkbox"/>		
9	<input type="checkbox"/>		
10	<input type="checkbox"/>		
11	<input type="checkbox"/>		
12	<input type="checkbox"/>		
13	<input type="checkbox"/>		
14	<input type="checkbox"/>		
15	<input type="checkbox"/>		
16	<input type="checkbox"/>		
17	<input type="checkbox"/>		
18	<input type="checkbox"/>		
19	<input type="checkbox"/>		
20	<input type="checkbox"/>		
21	<input type="checkbox"/>		
22	<input type="checkbox"/>		
23	<input type="checkbox"/>		
24	<input type="checkbox"/>		
25	<input type="checkbox"/>		
26	<input type="checkbox"/>		
27	<input type="checkbox"/>		
28	<input type="checkbox"/>		
29	<input type="checkbox"/>		
30	<input type="checkbox"/>		
31	<input type="checkbox"/>		
32	<input type="checkbox"/>		

Apply      Reset

The following table describes the labels in this screen.

**Table 122** Local User Database

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

## 21.3 RADIUS

Use RADIUS to authenticate users using an external server.

Click **SECURITY**, **AUTH SERVER**, then the **RADIUS** tab to open the **RADIUS** screen. Use this screen to set up your ZyWALL's RADIUS server settings.

**Figure 176** RADIUS

The screenshot shows the RADIUS configuration interface. At the top, there are two tabs: 'Local User Database' and 'RADIUS'. The 'RADIUS' tab is selected. Below the tabs, there are two main sections: 'Authentication Server' and 'Accounting Server'. Each section contains an 'Active' checkbox, a 'Server IP Address' input field (with '0.0.0.0' entered), a 'Port Number' input field (with '1812' for Authentication and '1813' for Accounting), and a 'Key' input field. At the bottom of the screen, there are two buttons: 'Apply' and 'Reset'.



The following table describes the labels in this screen.

**Table 123** RADIUS

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

# CHAPTER 22

## Network Address Translation (NAT)

This chapter discusses how to configure NAT on the ZyWALL.

### 22.1 NAT Overview

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

#### 22.1.1 NAT Definitions

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

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

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

**Table 124** NAT Definitions

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

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

## 22.1.2 What NAT Does

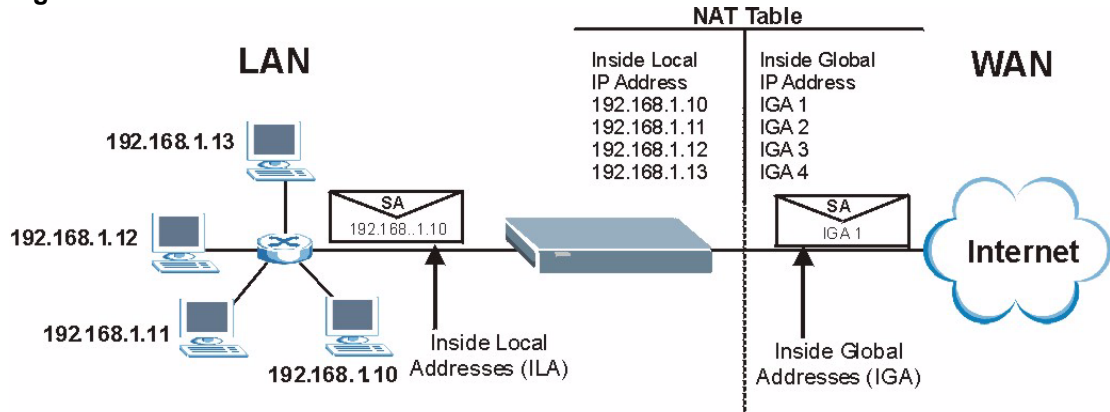
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address)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

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers (for example a web server and a telnet server) on your local network and make them accessible to the outside world. Although you can make designated servers on the LAN accessible to the outside world, it is strongly recommended that you attach those servers to the DMZ port instead. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping), NAT offers the additional benefit of firewall protection. With no servers defined, your ZyWALL filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631, The IP Network Address Translator (NAT)*.

## 22.1.3 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.

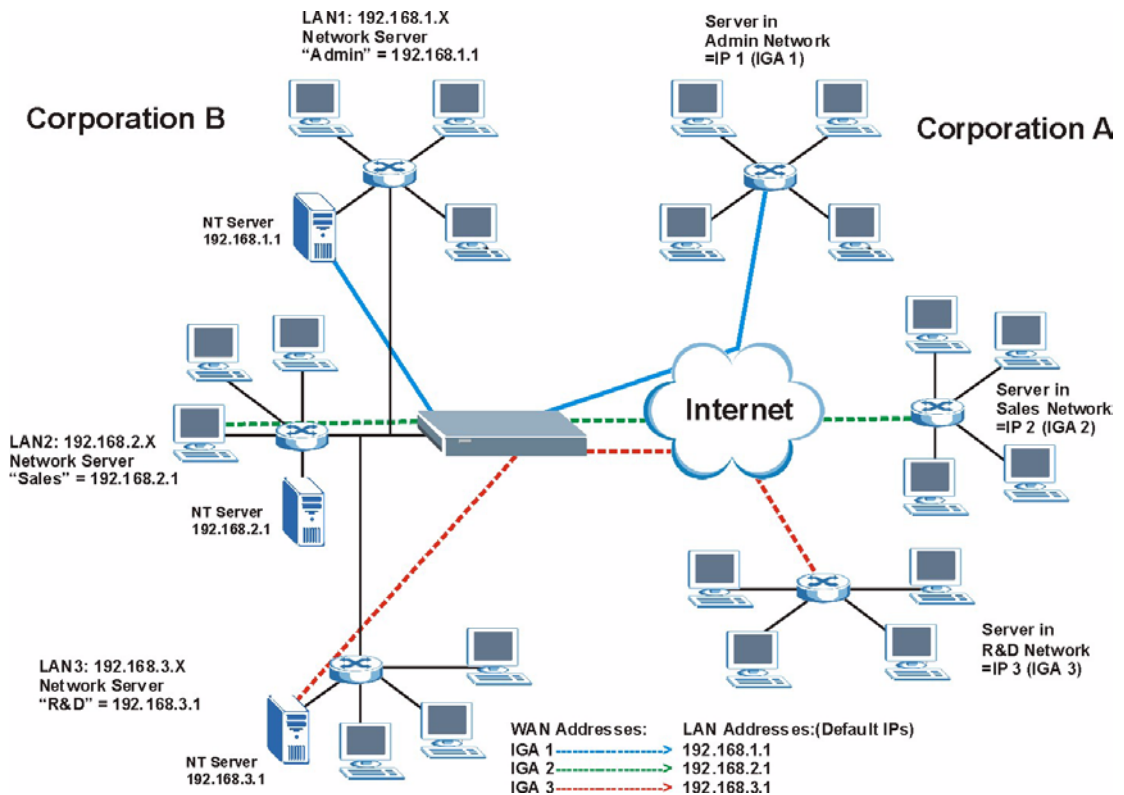
Figure 177 How NAT Works



### 22.1.4 NAT Application

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

Figure 178 NAT Application With IP Alias



## 22.1.5 Port Restricted Cone NAT

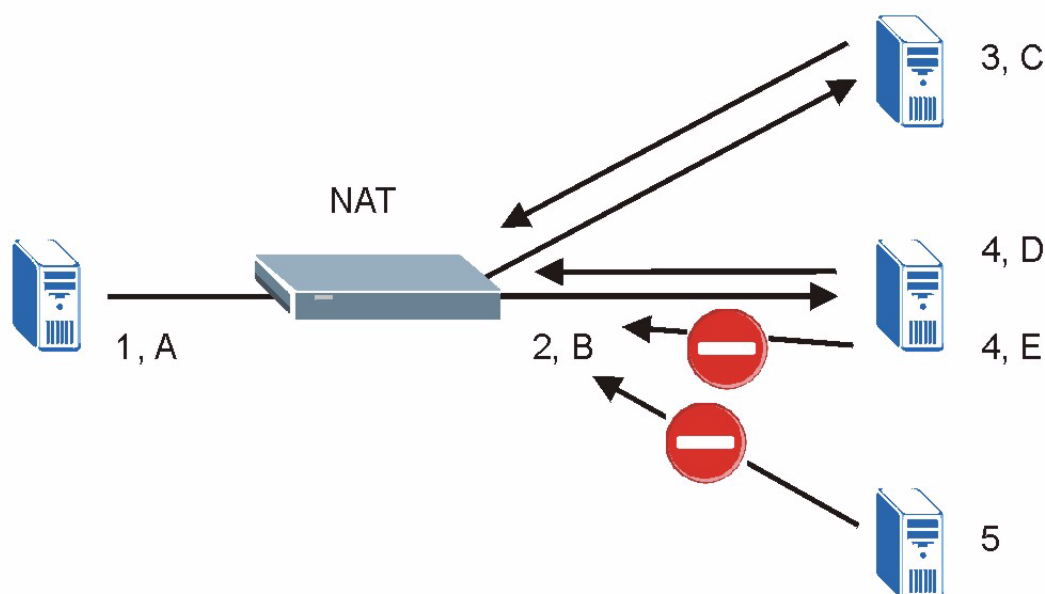
At the time of writing ZyWALL ZyNOS version 4.00 uses port restricted cone NAT. Port restricted cone NAT maps all outgoing packets from an internal IP address and port to a single IP address and port on the external network. In the following example, the ZyWALL maps the source address of all packets sent from internal IP address **1** and port **A** to IP address **2** and port **B** on the external network. A host on the external network (IP address **3** and Port **C** for example) can only send packets to the internal host if the internal host has already sent a packet to the external host's IP address and port.

A server with IP address **1** and port **A** sends packets to IP address **3**, port **C** and IP address **4**, port **D**. The ZyWALL changes the server's IP address to **2** and port to **B**.

Since **1, A** has already sent packets to **3, C** and **4, D**, they can send packets back to **2, B** and the ZyWALL will perform NAT on them and send them to the server at IP address **1**, port **A**.

Packets have not been sent from **1, A** to **4, E** or **5**, so they cannot send packets to **1, A**.

**Figure 179** Port Restricted Cone NAT Example



## 22.1.6 NAT Mapping Types

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

- **One to One:** In One-to-One mode, the ZyWALL maps one local IP address to one global IP address.
- **Many to One:** In Many-to-One mode, the ZyWALL maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature (the SUA option).
- **Many to Many Overload:** In Many-to-Many Overload mode, the ZyWALL maps the multiple local IP addresses to shared global IP addresses.
- **Many One to One:** In Many-One-to-One mode, the ZyWALL maps each local IP address to a unique global IP address.

- **Server:** This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world although, it is highly recommended that you use the DMZ port for these servers instead.

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

The following table summarizes these types.

**Table 125** 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-One-to-One	ILA1 ↔ IGA1 ILA2 ↔ IGA2 ILA3 ↔ IGA3 ...	M-1-1
Server	Server 1 IP ↔ IGA1 Server 2 IP ↔ IGA1 Server 3 IP ↔ IGA1	Server

## 22.2 Using NAT

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

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

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

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

## 22.3 NAT Overview

Click **ADVANCED, NAT** to open the **NAT Overview** screen. Not all fields are available on all models.

**Figure 180** NAT Overview

The following table describes the labels in this screen.

**Table 126** NAT Overview

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

**Table 126** NAT Overview (continued)

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

## 22.4 NAT Address Mapping

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

To change your ZyWALL's address mapping settings, click **ADVANCED**, **NAT** and then the **Address Mapping** tab. The screen appears as shown (some of the screen's blank rows are not shown). Not all fields are available on all models.



**Figure 181** NAT Address Mapping

**NAT**

**NAT Overview** | **Address Mapping** | Port Forwarding | Port Triggering

**SUA Address Mapping Rules**

#	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	N/A	M-1
2	N/A	N/A	0.0.0.0	N/A	Server

**Full Feature Address Mapping Rules**

WAN Interface:  | Go To Page:

#	Local Start IP	Local End IP	Global Start IP	Global End IP	Type	Modify
1	192.168. 1. 10	N/A	10.132. 50. 1	N/A	1-1	
2	192.168. 1. 11	192.168. 1. 25	10.132. 50. 2	10.132. 50. 23	M-M Ov	
3	0. 0. 0. 0	255.255.255.255	0. 0. 0. 0	N/A	M-1	
4	N/A	N/A	0. 0. 0. 0	N/A	Server	
5	...	...	...	...	-	
6	...	...	...	...	-	
7	...	...	...	...	-	
8	...	...	...	...	-	
9	...	...	...	...	-	
10	...	...	...	...	-	

new rule before rule  (rule number).

The following table describes the labels in this screen.

**Table 127** NAT Address Mapping

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

**Table 127** NAT Address Mapping (continued)

LABEL	DESCRIPTION
Global Start IP	This refers to the Inside Global IP Address (IGA), that is the starting global IP address. 0.0.0.0 is for a dynamic IP address from your ISP with <b>Many-to-One</b> and <b>Server</b> mapping types.
Global End IP	This is the ending Inside Global Address (IGA). This field is <b>N/A</b> for <b>One-to-One</b> , <b>Many-to-One</b> and <b>Server</b> mapping types.
Type	<ol style="list-style-type: none"> <li>1. <b>One-to-One</b> mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-One NAT mapping type.</li> <li>2. <b>Many-to-One</b> mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported only.</li> <li>3. <b>Many-to-Many Overload</b> mode maps multiple local IP addresses to shared global IP addresses.</li> <li>4. <b>Many One-to-One</b> mode maps each local IP address to unique global IP addresses.</li> <li>5. <b>Server</b> allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.</li> </ol>
Modify	Click the edit icon to go to the screen where you can edit the address mapping rule. Click the delete icon to delete an existing address mapping rule. A window display asking you to confirm that you want to delete the address mapping rule. Note that subsequent address mapping rules move up by one when you take this action.
Insert	Click <b>Insert</b> to insert a new mapping rule before an existing one.

## 22.4.1 NAT Address Mapping Edit

Click the **Edit** button to display the **NAT Address Mapping Edit** screen. Use this screen to edit an address mapping rule.

**Figure 182** NAT Address Mapping Edit

The screenshot shows the 'NAT - ADDRESS MAPPING' window. The title bar reads 'NAT - ADDRESS MAPPING'. Inside the window, there is a section titled 'Address Mapping Rule'. Below this title, there are several fields:

- Type:** A dropdown menu currently showing 'One-to-One'.
- Local Start IP:** An input field containing '0 . 0 . 0 . 0'.
- Local End IP:** A field containing 'N/A'.
- Global Start IP:** An input field containing '0 . 0 . 0 . 0'.
- Global End IP:** A field containing 'N/A'.

At the bottom of the window, there are two buttons: 'Apply' and 'Cancel'.

The following table describes the labels in this screen.

**Table 128** NAT Address Mapping Edit

LABEL	DESCRIPTION
Type	Choose the port mapping type from one of the following. <ol style="list-style-type: none"> <li>1. <b>One-to-One</b>: One-to-One mode maps one local IP address to one global IP address. Note that port numbers do not change for One-to-One NAT mapping type.</li> <li>2. <b>Many-to-One</b>: Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature.</li> <li>3. <b>Many-to-Many Overload</b>: Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses.</li> <li>4. <b>Many One-to-One</b>: Many One-to-One mode maps each local IP address to unique global IP addresses.</li> <li>5. <b>Server</b>: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.</li> </ol>
Local Start IP	This is the starting Inside Local IP Address (ILA). Local IP addresses are <b>N/A</b> for <b>Server</b> port mapping.
Local End IP	This is the end Inside Local IP Address (ILA). If your rule is for all local IP addresses, then enter 0.0.0.0 as the <b>Local Start IP</b> address and 255.255.255.255 as the <b>Local End IP</b> address. This field is <b>N/A</b> for <b>One-to-One</b> and <b>Server</b> mapping types.
Global Start IP	This is the starting Inside Global IP Address (IGA). Enter <b>0.0.0.0</b> here if you have a dynamic IP address from your ISP.
Global End IP	This is the ending Inside Global IP Address (IGA). This field is <b>N/A</b> for <b>One-to-One</b> , <b>Many-to-One</b> and <b>Server</b> mapping types.
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

## 22.5 Port Forwarding

A port forwarding set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though NAT makes your whole inside network appear as a single computer to the outside world.

You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports.

Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

## 22.5.1 Default Server IP Address

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

**Note:** If you do not assign a **Default Server IP** address, the ZyWALL discards all packets received for ports that are not specified here or in the remote management setup.

## 22.5.2 Port Forwarding: Services and Port Numbers

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

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

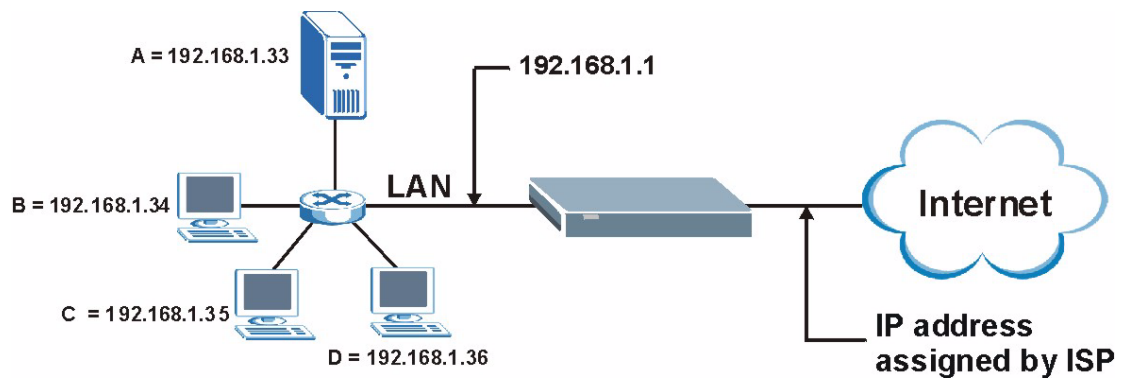
The most often used port numbers are shown in the following table. Please refer to RFC 1700 for further information about port numbers. Please also refer to the Supporting CD for more examples and details on port forwarding and NAT.

**Table 129** Services and Port Numbers

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

## 22.5.3 Configuring Servers Behind Port Forwarding (Example)

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a third (**C** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

**Figure 183** Multiple Servers Behind NAT Example

## 22.5.4 NAT and Multiple WAN

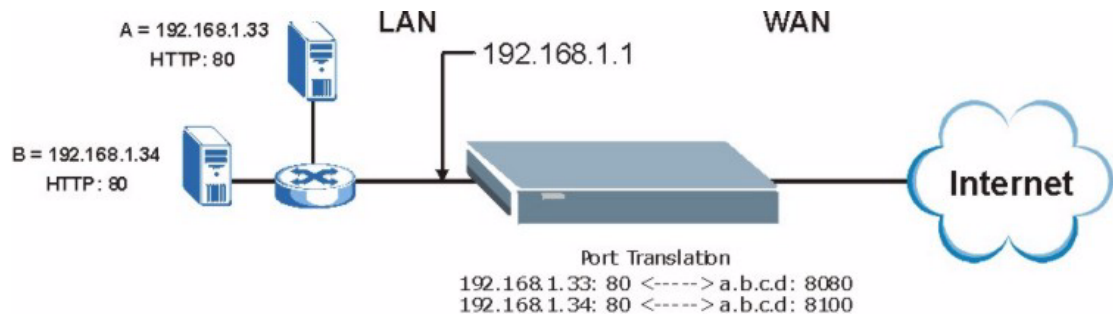
The ZyWALL has two WAN ports. You can configure port forwarding and trigger port rule sets for the first WAN port and separate sets of rules for the second WAN port.

## 22.5.5 Port Translation

The ZyWALL can translate the destination port number or a range of port numbers of packets coming from the WAN to another destination port number or range of port numbers on the LAN (or DMZ). When you use port forwarding without port translation, a single server on the LAN or DMZ can use a specific port number and be accessible to the outside world through a single WAN IP address. When you use port translation with port forwarding, multiple servers on the LAN or DMZ can use the same port number and still be accessible to the outside world through a single WAN IP address.

The following example has two web servers on a LAN. Server **A** uses IP address 192.168.1.33 and server **B** uses 192.168.1.34. Both servers use port 80. The letters a.b.c.d represent the WAN port's IP address. The ZyWALL translates port 8080 of traffic received on the WAN port (IP address a.b.c.d) to port 80 and sends it to server **A** (IP address 192.168.1.33). The ZyWALL also translates port 8100 of traffic received on the WAN port (also IP address a.b.c.d) to port 80, but sends it to server **B** (IP address 192.168.1.34).

**Note:** In this example, anyone wanting to access server A from the Internet must use port 8080. Anyone wanting to access server B from the Internet must use port 8100.

**Figure 184** Port Translation Example

## 22.6 Port Forwarding

**Note:** If you do not assign a **Default Server** IP address, the ZyWALL discards all packets received for ports that are not specified here or in the remote management setup.

Click **ADVANCED**, **NAT** and **Port Forwarding** to open the **Port Forwarding** screen. Not all fields are available on all models.

Refer to [Figure 129 on page 384](#) for port numbers commonly used for particular services.

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

**Figure 185** Port Forwarding

**NAT**

NAT Overview | Address Mapping | **Port Forwarding** | Port Triggering

**Port Forwarding Rules**

WAN Interface: WAN 1

Default Server: 0 . 0 . 0 . 0      Go To Page: 1

#	Active	Name	Incoming Port(s)	Port Translation	Server IP Address
1	<input checked="" type="checkbox"/>	1	80 - 80	0 - 0	192 . 168 . 1 . 21
2	<input checked="" type="checkbox"/>	2	25 - 25	0 - 0	192 . 168 . 1 . 20
3	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0
4	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0
5	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0
6	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0
7	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0
8	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0
9	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0
10	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0

**Note 1:** You may also need to create a [Firewall](#) rule.  
**Note 2:** Port Translation is optional.

Apply      Reset

The following table describes the labels in this screen.

**Table 130** Port Forwarding

LABEL	DESCRIPTION
WAN Interface	Select the WAN port for which you want to view or configure address mapping rules.
Default Server	In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in this screen. If you do not assign a <b>Default Server</b> IP address, the ZyWALL discards all packets received for ports that are not specified here or in the remote management setup.
Go To Page	Choose a page from the drop-down list box to display the corresponding summary page of the port forwarding servers.
#	This is the number of an individual port forwarding server entry.
Active	Select this check box to enable the port forwarding server entry. Clear this check box to disallow forwarding of these ports to an inside server without having to delete the entry.
Name	Enter a name to identify this port-forwarding rule.
Incoming Port(s)	Enter a port number here. To forward only one port, enter it again in the second field. To specify a range of ports, enter the last port to be forwarded in the second field.
Port Translation	Enter the port number here to which you want the ZyWALL to translate the incoming port. For a range of ports, you only need to enter the first number of the range to which you want the incoming ports translated, the ZyWALL automatically calculates the last port of the translated port range.

**Table 130** Port Forwarding

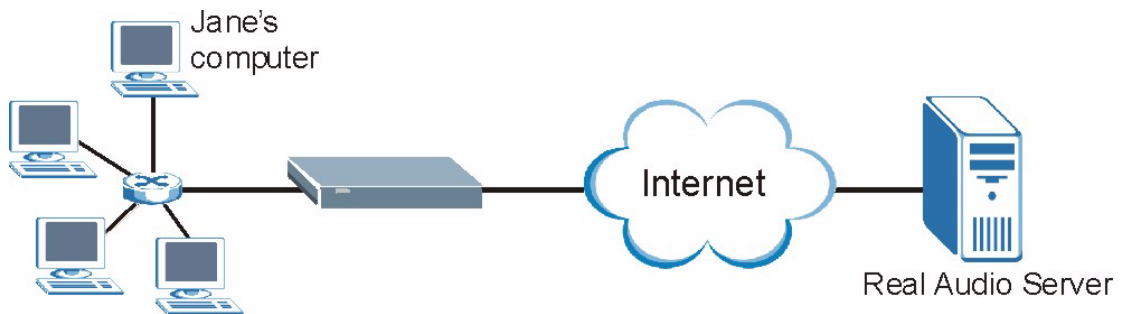
LABEL	DESCRIPTION
Server IP Address	Enter the inside IP address of the server here.
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 22.7 Port Triggering

Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address.

Trigger port forwarding solves this problem by allowing computers on the LAN to dynamically take turns using the service. The ZyWALL records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a "trigger" port). When the ZyWALL's WAN port receives a response with a specific port number and protocol ("incoming" port), the ZyWALL forwards the traffic to the LAN IP address of the computer that sent the request. After that computer's connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

For example:

**Figure 186** Trigger Port Forwarding Process: Example

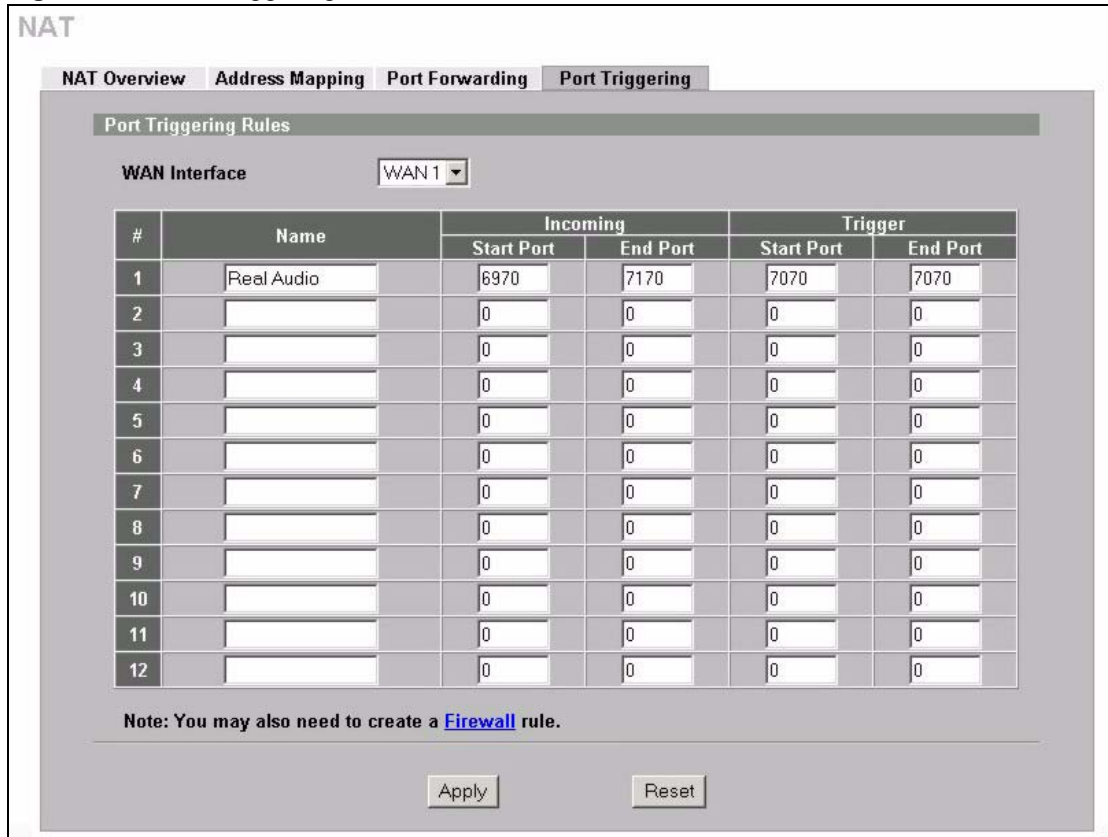
- 1 Jane requests a file from the Real Audio server (port 7070).
- 2 Port 7070 is a "trigger" port and causes the ZyWALL to record Jane's computer IP address. The ZyWALL associates Jane's computer IP address with the "incoming" port range of 6970-7170.
- 3 The Real Audio server responds using a port number ranging between 6970-7170.



- 4 The ZyWALL forwards the traffic to Jane's computer IP address.
- 5 Only Jane can connect to the Real Audio server until the connection is closed or times out. The ZyWALL times out in three minutes with UDP (User Datagram Protocol) or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

To change your ZyWALL's trigger port settings, click **ADVANCED**, **NAT** and the **Port Triggering** tab. The screen appears as shown. Not all fields are available on all models.

**Figure 187** Port Triggering



The following table describes the labels in this screen.

**Table 131** Port Triggering

LABEL	DESCRIPTION
WAN Interface	Select the WAN port for which you want to view or configure address mapping rules.
#	This is the rule index number (read-only).
Name	Type a unique name (up to 15 characters) for identification purposes. All characters are permitted - including spaces.
Incoming	Incoming is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The ZyWALL forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.
Start Port	Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.

**Table 131** Port Triggering

LABEL	DESCRIPTION
Trigger	The trigger port is a port (or a range of ports) that causes (or triggers) the ZyWALL to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Start Port	Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.



# CHAPTER 23

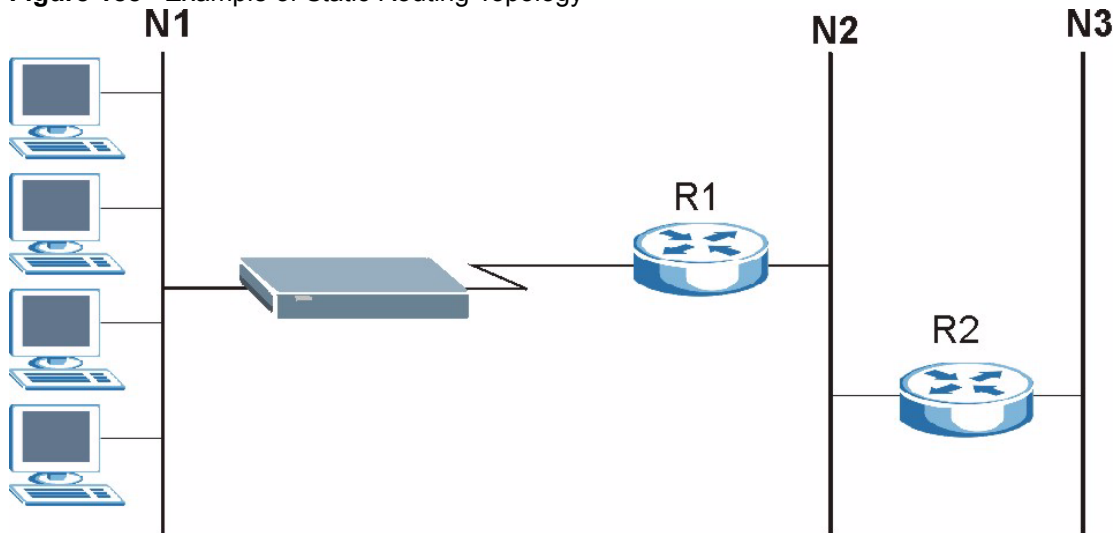
## Static Route

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

### 23.1 IP Static Route

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

**Figure 188** Example of Static Routing Topology



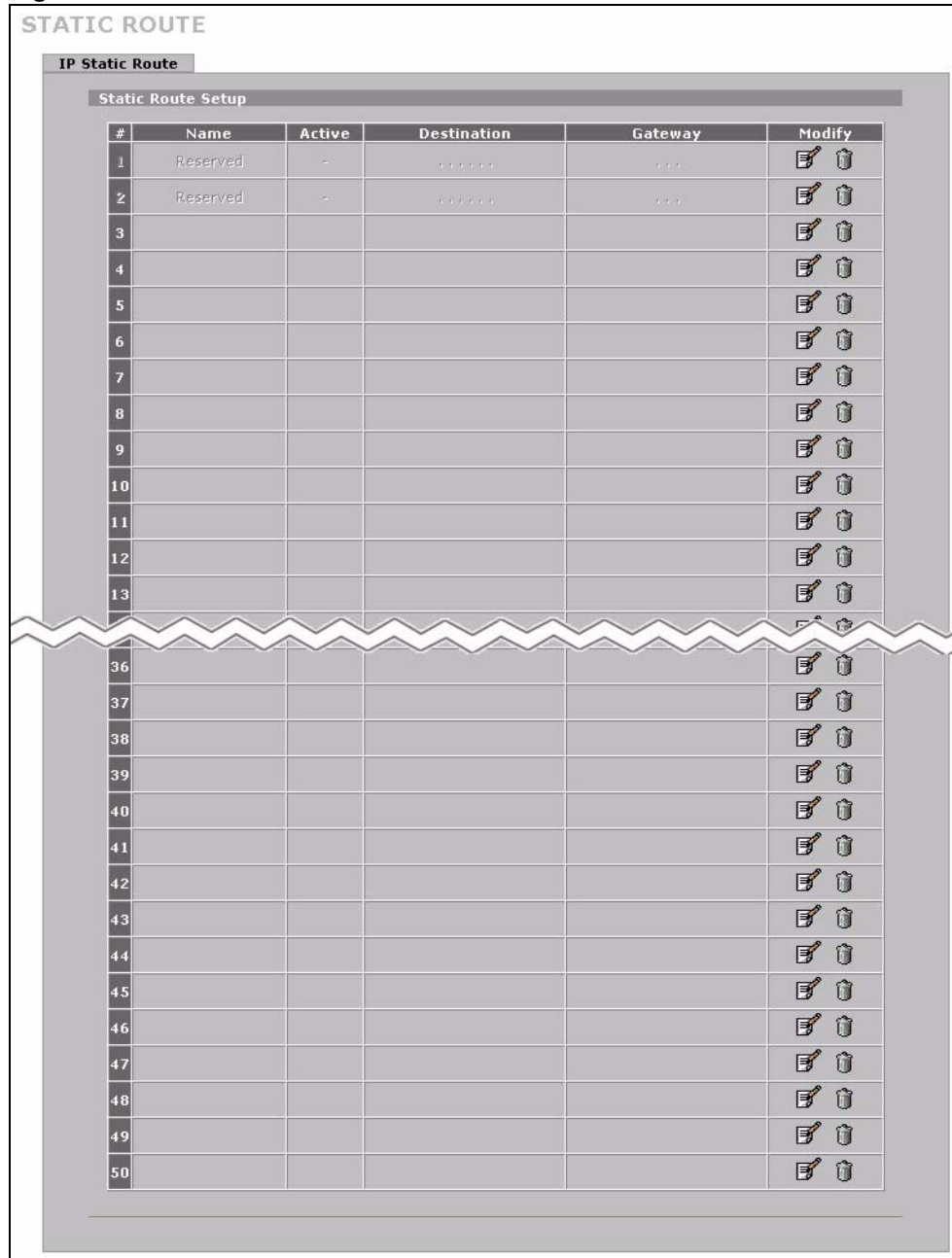
### 23.2 IP Static Route

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

**Note:** The first two static route entries are for default WAN1 and WAN2 routes on a ZyWALL with multiple WAN ports; the first static route entry is for the default WAN route on a ZyWALL with a single WAN port. You cannot modify or delete a static default route. The name of the default static route is left blank unless you configure a static WAN IP address.

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

**Figure 189** IP Static Route



The following table describes the labels in this screen.

**Table 132** IP Static Route

LABEL	DESCRIPTION
#	This is the number of an individual static route.
Name	This is the name that describes or identifies this route.

**Table 132** IP Static Route

LABEL	DESCRIPTION
Active	This field shows whether this static route is active ( <b>Yes</b> ) or not ( <b>No</b> ).
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Gateway	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Modify	Click the edit icon to go to the screen where you can set up a static route on the ZyWALL. Click the delete icon to remove a static route from the ZyWALL. A window displays asking you to confirm that you want to delete the route.

### 23.2.1 IP Static Route Edit

Select a static route index number and click **Edit**. The screen shown next appears. Use this screen to configure the required information for a static route.

**Figure 190** IP Static Route Edit

The following table describes the labels in this screen.

**Table 133** IP Static Route Edit

LABEL	DESCRIPTION
Route Name	Enter the name of the IP static route. Leave this field blank to delete this static route.
Active	This field allows you to activate/deactivate this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask here.

**Table 133** IP Static Route Edit

LABEL	DESCRIPTION
Gateway IP Address	Enter the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Metric	Metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Private	This parameter determines if the ZyWALL will include this route to a remote node in its RIP broadcasts. Select this check box to keep this route private and not included in RIP broadcasts. Clear this check box to propagate this route to other hosts through RIP broadcasts.
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

# CHAPTER 24

## Policy Route

This chapter covers setting and applying policies used for IP routing. This chapter applies to the ZyWALL 35 and ZyWALL 70.

### 24.1 Policy Route

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

### 24.2 Benefits

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

### 24.3 Routing Policy

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

The actions that can be taken include:

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



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

## 24.4 IP Routing Policy Setup

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

**Figure 191** Policy Route Summary

**POLICY ROUTE**

**Policy Route Summary**

**Policy Route Setup**

#	Active	Source Address/Port	Destination Address/Port	Gateway	Protocol	Action	Modify
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
37							
38							
39							
40							
41							
42							
43							
44							
45							
46							
47							
48							

Move rule 1 to rule 1 (rule number)

The following table describes the labels in this screen.

**Table 134** Policy Route Summary

LABEL	DESCRIPTION
#	This is the number of an individual policy route.
Active	This field shows whether the policy is active or inactive.
Source Address/ Port	This is the source IP address range and/or port number range.
Destination Address/Port	This is the destination IP address range and/or port number range.
Gateway	Enter the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Protocol	This is the IP protocol and can be <b>ALL(0)</b> , <b>ICMP(1)</b> , <b>IGMP(2)</b> , <b>TCP(6)</b> , <b>UDP(17)</b> , <b>GRE(47)</b> , <b>ESP(50)</b> or <b>AH(51)</b> .
Action	This field specifies whether action should be taken on criteria <b>Matched</b> or <b>Not Matched</b> .
Modify	Click the edit icon to go to the screen where you can edit the routing policy on the ZyWALL. Click the delete icon to remove an existing routing policy from the ZyWALL. A window display asking you to confirm that you want to delete the routing policy.
Move	Type a policy route's index number and the number for where you want to put that rule. Click <b>Move</b> to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering.

## 24.5 Policy Route Edit

Click **POLICY ROUTE** to open the **Policy Route Summary** screen. Then click the edit icon to open the **Edit IP Policy Route** screen.

**Figure 192** Edit IP Policy Route

The following table describes the labels in this screen.

**Table 135** Edit IP Policy Route

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

**Table 135** Edit IP Policy Route (continued)

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



# CHAPTER 25

## Bandwidth Management

This chapter describes the functions and configuration of bandwidth management with multiple levels of sub-classes.

### 25.1 Bandwidth Management Overview

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

Bandwidth management addresses questions such as:

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

Bandwidth management also allows you to configure the allowed output for an interface to match what the network can handle. This helps reduce delays and dropped packets at the next routing device. For example, you can set the WAN interface speed to 1024 kbps (or less) if the broadband device connected to the WAN port has an upstream speed of 1024 kbps.

### 25.2 Bandwidth Classes and Filters

Use bandwidth classes and sub-classes to allocate specific amounts of bandwidth capacity (bandwidth budgets). Configure a bandwidth filter to define a bandwidth class (or sub-class) based on a specific application and/or subnet. Use the **Class Setup** screen (see [Section 25.11.1 on page 411](#)) to set up a bandwidth class's name, bandwidth allotment, and bandwidth filter. You can configure up to one bandwidth filter per bandwidth class. You can also configure bandwidth classes without bandwidth filters. However, it is recommended that you configure sub-classes with filters for any classes that you configure without filters. The ZyWALL leaves the bandwidth budget allocated and unused for a class that does not have a filter or sub-classes with filters. View your configured bandwidth classes and sub-classes in the **Class Setup** screen (see [Section 25.11 on page 410](#) for details).

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

## 25.3 Proportional Bandwidth Allocation

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

## 25.4 Application-based Bandwidth Management

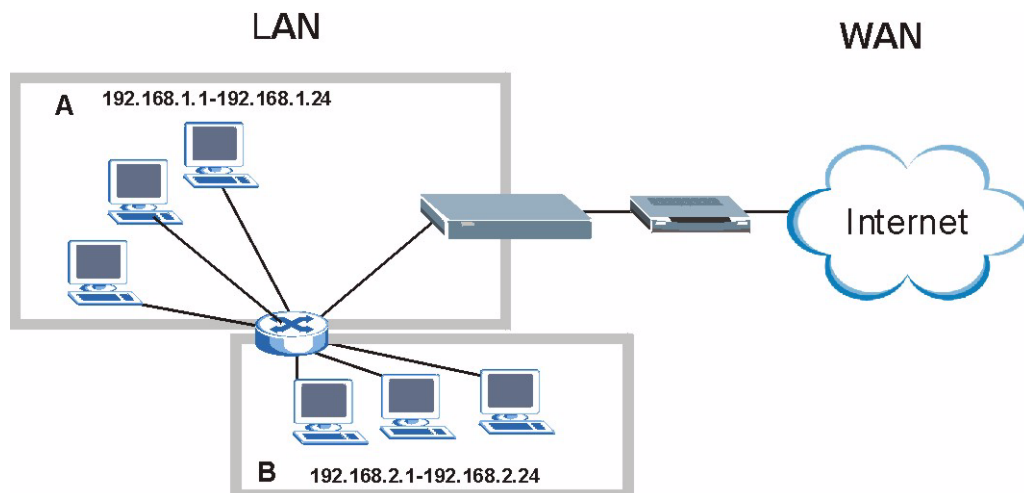
You can create bandwidth classes based on individual applications (like VoIP, Web, FTP, E-mail and Video for example).

## 25.5 Subnet-based Bandwidth Management

You can create bandwidth classes based on subnets.

The following figure shows LAN subnets. You could configure one bandwidth class for subnet A and another for subnet B.

**Figure 193** Subnet-based Bandwidth Management Example



## 25.6 Application and Subnet-based Bandwidth Management

You could also create bandwidth classes based on a combination of a subnet and an application. The following example table shows bandwidth allocations for application specific traffic from separate LAN subnets.

**Table 136** Application and Subnet-based Bandwidth Management Example

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

## 25.7 Scheduler

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

### 25.7.1 Priority-based Scheduler

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

### 25.7.2 Fairness-based Scheduler

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

### 25.7.3 Maximize Bandwidth Usage

The maximize bandwidth usage option (see [Figure 194 on page 409](#)) allows the ZyWALL to divide up any available bandwidth on the interface (including unallocated bandwidth and any allocated bandwidth that a class is not using) among the bandwidth classes that require more bandwidth.



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

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

### 25.7.4 Reserving Bandwidth for Non-Bandwidth Class Traffic

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

- 1 Leave some of the interface's bandwidth unbudgeted.
- 2 Do not enable the interface's **Maximize Bandwidth Usage** option.
- 3 Do not enable bandwidth borrowing on the sub-classes that have the root class as their parent (see [Section 25.8 on page 407](#)).

### 25.7.5 Maximize Bandwidth Usage Example

Here is an example of a ZyWALL that has maximize bandwidth usage enabled on an interface. The following table shows each bandwidth class's bandwidth budget. The classes are set up based on subnets. The interface is set to 10240 kbps. Each subnet is allocated 2048 kbps. The unbudgeted 2048 kbps allows traffic not defined in any of the bandwidth filters to go out when you do not select the maximize bandwidth option.

**Table 137** Maximize Bandwidth Usage Example

BANDWIDTH CLASSES AND ALLOTMENTS	
Root Class: 10240 kbps	Administration: 2048 kbps
	Sales: 2048 kbps
	Marketing: 2048 kbps
	Research: 2048 kbps

The ZyWALL divides up the unbudgeted 2048 kbps among the classes that require more bandwidth. If the administration department only uses 1024 kbps of the budgeted 2048 kbps, the ZyWALL also divides the remaining 1024 kbps among the classes that require more bandwidth. Therefore, the ZyWALL divides a total of 3072 kbps of unbudgeted and unused bandwidth among the classes that require more bandwidth.

### 25.7.5.1 Priority-based Allotment of Unused and Unbudgeted Bandwidth

The following table shows the priorities of the bandwidth classes and the amount of bandwidth that each class gets.

**Table 138** Priority-based Allotment of Unused and Unbudgeted Bandwidth Example

BANDWIDTH CLASSES, PRIORITIES AND ALLOTMENTS	
Root Class: 10240 kbps	Administration: Priority 4, 1024 kbps
	Sales: Priority 6, 3584 kbps
	Marketing: Priority 6, 3584 kbps
	Research: Priority 5, 2048 kbps

Suppose that all of the classes except for the administration class need more bandwidth.

- Each class gets up to its budgeted bandwidth. The administration class only uses 1024 kbps of its budgeted 2048 kbps.
- The sales and marketing are first to get extra bandwidth because they have the highest priority (6). If they each require 1536 kbps or more of extra bandwidth, the ZyWALL divides the total 3072 kbps total of unbudgeted and unused bandwidth equally between the sales and marketing departments (1536 kbps extra to each for a total of 3584 kbps for each) because they both have the highest priority level.
- Research requires more bandwidth but only gets its budgeted 2048 kbps because all of the unbudgeted and unused bandwidth goes to the higher priority sales and marketing classes.

### 25.7.5.2 Fairness-based Allotment of Unused and Unbudgeted Bandwidth

The following table shows the amount of bandwidth that each class gets.

**Table 139** Fairness-based Allotment of Unused and Unbudgeted Bandwidth Example

BANDWIDTH CLASSES AND ALLOTMENTS	
Root Class: 10240 kbps	Administration: 1024 kbps
	Sales: 3072 kbps
	Marketing: 3072 kbps
	Research: 3072 kbps

Suppose that all of the classes except for the administration class need more bandwidth.

- Each class gets up to its budgeted bandwidth. The administration class only uses 1024 kbps of its budgeted 2048 kbps.
- The ZyWALL divides the total 3072 kbps total of unbudgeted and unused bandwidth equally among the other classes. 1024 kbps extra goes to each so the other classes each get a total of 3072 kbps.

## 25.8 Bandwidth Borrowing

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

Enable bandwidth borrowing on a sub-class to allow the sub-class to use its parent class's unused bandwidth. A parent class's unused bandwidth is given to the highest priority sub-class first. The sub-class can also borrow bandwidth from a higher parent class (grandparent class) if the sub-class's parent class is also configured to borrow bandwidth from its parent class. This can go on for as many levels as are configured to borrow bandwidth from their parent class (see [Section 25.8.1 on page 407](#)).

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

### 25.8.1 Bandwidth Borrowing Example

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

Refer to the product specifications in the appendix to see how many class levels you can configure on your ZyWALL.

**Table 140** Bandwidth Borrowing Example

BANDWIDTH CLASSES AND BANDWIDTH BORROWING SETTINGS			
Root Class:	Administration: Borrowing Enabled		
	Sales: Borrowing Disabled	Sales USA: Borrowing Enabled	Bill: Borrowing Enabled
			Amy: Borrowing Disabled
		Sales Asia: Borrowing Disabled	Tina: Borrowing Enabled
			Fred: Borrowing Disabled
	Marketing: Borrowing Enabled		
	Research: Borrowing Enabled	Software: Borrowing Enabled	
Hardware: Borrowing Enabled			

- The Bill class can borrow unused bandwidth from the Sales USA class because the Bill class has bandwidth borrowing enabled.
- The Bill class can also borrow unused bandwidth from the Sales class because the Sales USA class also has bandwidth borrowing enabled.

- The Bill class cannot borrow unused bandwidth from the Root class because the Sales class has bandwidth borrowing disabled.
- The Amy class cannot borrow unused bandwidth from the Sales USA class because the Amy class has bandwidth borrowing disabled.
- The Research Software and Hardware classes can both borrow unused bandwidth from the Research class because the Research Software and Hardware classes both have bandwidth borrowing enabled.
- The Research Software and Hardware classes can also borrow unused bandwidth from the Root class because the Research class also has bandwidth borrowing enabled.

## 25.9 Maximize Bandwidth Usage With Bandwidth Borrowing

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

- 1 The ZyWALL sends traffic according to each bandwidth class's bandwidth budget.
- 2 The ZyWALL assigns a parent class's unused bandwidth to its sub-classes that have more traffic than their budgets and have bandwidth borrowing enabled. The ZyWALL gives priority to sub-classes of higher priority and treats classes of the same priority equally.
- 3 The ZyWALL assigns any remaining unused or unbudgeted bandwidth on the interface to any class that requires it. The ZyWALL gives priority to classes of higher priority and treats classes of the same level equally.
- 4 If the bandwidth requirements of all of the traffic classes are met and there is still some unbudgeted bandwidth, the ZyWALL assigns it to traffic that does not match any of the classes.

## 25.10 Configuring Summary

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

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

**Figure 194** Bandwidth Management: Summary

Class	Active	Speed (kbps)	Scheduler	Maximize Bandwidth Usage
WAN1	<input checked="" type="checkbox"/>	100000	Fairness-Based	<input type="checkbox"/>
WAN2	<input type="checkbox"/>	100000	Fairness-Based	<input type="checkbox"/>
LAN	<input checked="" type="checkbox"/>	100000	Fairness-Based	<input type="checkbox"/>
DMZ	<input type="checkbox"/>	100000	Fairness-Based	<input type="checkbox"/>
WLAN	<input type="checkbox"/>	100000	Fairness-Based	<input type="checkbox"/>

The following table describes the labels in this screen.

**Table 141** Bandwidth Management: Summary

LABEL	DESCRIPTION
Class	These read-only labels represent the physical interfaces. Select an interface's check box to enable bandwidth management on that interface. Bandwidth management applies to all traffic flowing out of the router through the interface, regardless of the traffic's source.  Traffic redirect or IP alias may cause LAN-to-LAN or DMZ-to-DMZ traffic to pass through the ZyWALL and be managed by bandwidth management.
Active	Select an interface's check box to enable bandwidth management on that interface.
Speed (kbps)	Enter the amount of bandwidth for this interface that you want to allocate using bandwidth management.  This appears as the bandwidth budget of the interface's root class (see <a href="#">Section 25.11 on page 410</a> ). The recommendation is to set this speed to match what the device connected to the port can handle. For example, set the WAN interface speed to 1000 kbps if the broadband device connected to the WAN port has an upstream speed of 1000 kbps.
Scheduler	Select either <b>Priority-Based</b> or <b>Fairness-Based</b> from the drop-down menu to control the traffic flow. Select <b>Priority-Based</b> to give preference to bandwidth classes with higher priorities. Select <b>Fairness-Based</b> to treat all bandwidth classes equally. See <a href="#">Section 25.7 on page 404</a> .
Maximize Bandwidth Usage	Select this check box to have the ZyWALL divide up all of the interface's unallocated and/or unused bandwidth among the bandwidth classes that require bandwidth. Do not select this if you want to reserve bandwidth for traffic that does not match a bandwidth class (see <a href="#">Section 25.7.4 on page 405</a> ) or you want to limit the speed of this interface (see the <b>Speed</b> field description).
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 25.11 Configuring Class Setup

The **Class Setup** screen displays the configured bandwidth classes by individual interface. Select an interface and click the buttons to perform the actions described next. Click “+” to expand the class tree or click “-” to collapse the class tree. Each interface has a permanent root class. The bandwidth budget of the root class is equal to the speed you configured on the interface (see [Section 25.10 on page 408](#) to configure the speed of the interface). Configure sub-class layers for the root class.

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

**Figure 195** Bandwidth Management: Class Setup

**BANDWIDTH MANAGEMENT**

Summary **Class Setup** Monitor

**Class Setup**

Interface: LAN

Bandwidth Management: Active

- Root Class: 100000 kbps
  - Admin: 15000 kbps
  - COE: 5000 kbps
  - CPE: 5000 kbps

Add Sub-Class Edit Delete Statistics

**Filter List**

#	Filter Name	Service	Destination IP Address	Destination Port	Source IP Address	Source Port	Protocol ID
1	Admin	FTP	0.0.0.0/0	0	192.168.1.0/24	0	0
2	COE	H.323	0.0.0.0/0	0	192.168.2.0/24	0	0
3	CPE	SIP	0.0.0.0/0	0	192.168.3.0/24	0	0

Move filter 0 to filter 0 (filter number).

The following table describes the labels in this screen.

**Table 142** Bandwidth Management: Class Setup

LABEL	DESCRIPTION
Interface	Select an interface from the drop-down list box for which you wish to set up classes. Bandwidth management controls outgoing traffic on an interface, not incoming. So, in order to limit the download bandwidth of the LAN users, set the bandwidth management class on the LAN. In order to limit the upload bandwidth, set the bandwidth management class on the corresponding WAN interface.
Bandwidth Management	This field displays whether bandwidth management on the interface you selected in the field above is enabled ( <b>Active</b> ) or not ( <b>Inactive</b> ).
Add Sub-Class	Click <b>Add Sub-class</b> to add a sub-class.

**Table 142** Bandwidth Management: Class Setup (continued)

LABEL	DESCRIPTION
Edit	Click <b>Edit</b> to configure the selected class. You cannot edit the root class.
Delete	Click <b>Delete</b> to delete the class and all its sub-classes. You cannot delete the root class.
Statistics	Click <b>Statistics</b> to display the status of the selected class.
Filter List	This list displays the bandwidth management filters that are configured for the classes on the selected interface. The ZyWALL applies the bandwidth management filters in the order that they appear here. Once a connection matches a bandwidth management filter, the ZyWALL applies the rules of the corresponding bandwidth management class and does not check the connection against any other bandwidth management filters.
#	This is the index number of an individual bandwidth management filter.
Filter Name	This is the name that identifies a bandwidth management filter.
Service	This is the service that this bandwidth management filter is configured to manage.
Destination IP Address	This is the destination IP address for connections to which this bandwidth management filter applies.
Destination Port	This is the destination port for connections to which this bandwidth management filter applies.
Source IP Address	This is the source IP address for connections to which this bandwidth management filter applies.
Source Port	This is the source port for connections to which this bandwidth management filter applies.
Protocol ID	This is the protocol ID (service type) number for connections to which this bandwidth management filter applies. For example: 1 for ICMP, 6 for TCP or 17 for UDP.
Move	Type a filter's index number and the number for where you want to put that filter. Click <b>Move</b> to move the filter to the number that you typed. The ordering of your filters is important as they are applied in order of their numbering.

### 25.11.1 Bandwidth Manager Class Configuration

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

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

**Figure 196** Bandwidth Management: Edit Class

**BANDWIDTH MANAGEMENT - EDIT CLASS**

**Class Configuration**

Class Name: Admin

Bandwidth Budget: 15000 (Kbps)

Priority: 3 (0-7)

Borrow bandwidth from parent class

**Filter Configuration**

Enable Bandwidth Filter

Service: FTP

Destination IP Address: 0 . 0 . 0 . 0

Destination Subnet Mask: 0 . 0 . 0 . 0

Destination Port: 0

Source IP Address: 192 . 168 . 1 . 0

Source Subnet Mask: 255 . 255 . 255 . 0

Source Port: 0

Protocol ID: 0

Apply Cancel

The following table describes the labels in this screen.

**Table 143** Bandwidth Management: Edit Class

LABEL	DESCRIPTION
Class Configuration	
Class Name	Use the auto-generated name or enter a descriptive name of up to 20 alphanumeric characters, including spaces.
Bandwidth Budget (kbps)	Specify the maximum bandwidth allowed for the class in kbps. The recommendation is a setting between 20 kbps and 20000 kbps for an individual class.
Priority	Enter a number between 0 and 7 to set the priority of this class. The higher the number, the higher the priority. The default setting is 3.
Borrow bandwidth from parent class	Select this option to allow a sub-class to borrow bandwidth from its parent class if the parent class is not using up its bandwidth budget. Bandwidth borrowing is governed by the priority of the sub-classes. That is, a sub-class with the highest priority (7) is the first to borrow bandwidth from its parent class. Do not select this for the classes directly below the root class if you want to leave bandwidth available for other traffic types (see <a href="#">Section 25.7.4 on page 405</a> ) or you want to set the interface's speed to match what the next device in network can handle (see the <b>Speed</b> field description in <a href="#">Table 141 on page 409</a> ).
Filter Configuration	



**Table 143** Bandwidth Management: Edit Class (continued)

LABEL	DESCRIPTION
Enable Bandwidth Filter	<p>Select <b>Enable Bandwidth Filter</b> to have the ZyWALL use this bandwidth filter when it performs bandwidth management.</p> <p>You must enter a value in at least one of the following fields (other than the <b>Subnet Mask</b> fields which are only available when you enter the destination or source IP address).</p>
Service	<p>This field simplifies bandwidth class configuration by allowing you to select a predefined application. When you select a predefined application, you do not configure the rest of the bandwidth filter fields (other than enabling or disabling the filter).</p> <p><b>FTP</b> (File Transfer Program) is a program to enable fast transfer of files, including large files that may not be possible by e-mail. Select <b>FTP</b> from the drop-down list box to configure the bandwidth filter for FTP traffic.</p> <p><b>H.323</b> is a protocol used for multimedia communications over networks, for example NetMeeting. Select <b>H.323</b> from the drop-down list box to configure the bandwidth filter for H.323 traffic.</p> <p><b>Note:</b> If you select <b>H.323</b>, make sure you also use the <b>ALG</b> screen to turn on the H.323 ALG.</p> <p><b>SIP</b> (Session Initiation Protocol) is a signaling protocol used in Internet telephony, instant messaging, events notification and conferencing. The ZyWALL supports SIP traffic pass-through. Select <b>SIP</b> from the drop-down list box to configure this bandwidth filter for SIP traffic. This option makes it easier to manage bandwidth for SIP traffic and is useful for example when there is a VoIP (Voice over Internet Protocol) device on your LAN.</p> <p><b>Note:</b> If you select <b>SIP</b>, make sure you also use the <b>ALG</b> screen to turn on the SIP ALG.</p> <p>Select <b>Custom</b> from the drop-down list box if you do not want to use a predefined application for the bandwidth class. When you select <b>Custom</b>, you need to configure at least one of the following fields (other than the <b>Subnet Mask</b> fields which you only enter if you also enter a corresponding destination or source IP address).</p>
Destination IP Address	Enter the destination IP address in dotted decimal notation.
Destination Subnet Mask	Enter the destination subnet mask. This field is N/A if you do not specify a <b>Destination IP Address</b> . Refer to <a href="#">Appendix E on page 694</a> for more information on IP subnetting.
Destination Port	Enter the port number of the destination. See <a href="#">Section 11.11.2 on page 233</a> for a table of services and port numbers.
Source IP Address	Enter the source IP address.
Source Subnet Mask	Enter the source subnet mask. This field is N/A if you do not specify a <b>Source IP Address</b> . Refer to <a href="#">Appendix E on page 694</a> for more information on IP subnetting.
Source Port	Enter the port number of the source. See the following table for some common services and port numbers.
Protocol ID	Enter the protocol ID (service type) number, for example: 1 for ICMP, 6 for TCP or 17 for UDP.

**Table 143** Bandwidth Management: Edit Class (continued)

LABEL	DESCRIPTION
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

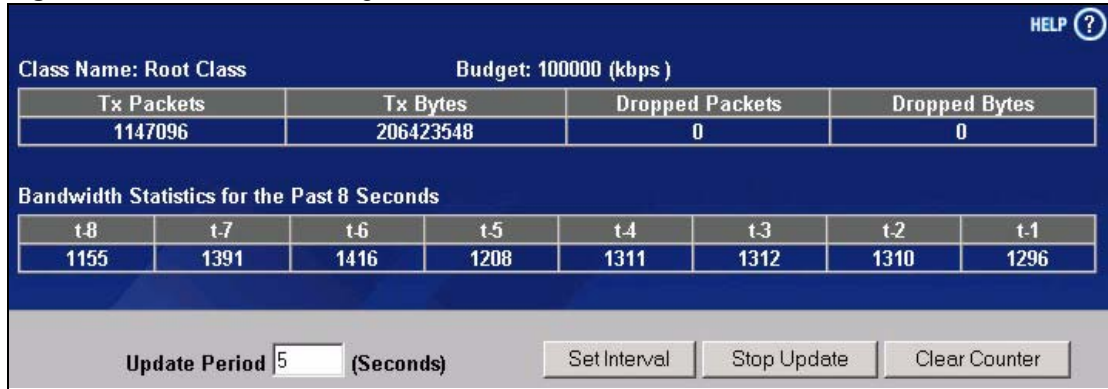
**Table 144** Services and Port Numbers

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

## 25.11.2 Bandwidth Management Statistics

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

**Figure 197** Bandwidth Management: Statistics



The following table describes the labels in this screen.

**Table 145** Bandwidth Management: Statistics

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

## 25.12 Configuring Monitor

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

**Figure 198** Bandwidth Management: Monitor

**BANDWIDTH MANAGEMENT**

Summary    Class Setup    **Monitor**

Monitor

Interface: LAN

Class	Budget (kbps)	Current Usage (kbps)
Root Class	100000	25
Admin	15000	0
COE	5000	0
CPE	5000	0
Default Class	85000	25

Refresh

The following table describes the labels in this screen.

**Table 146** Bandwidth Management: Monitor

LABEL	DESCRIPTION
Interface	Select an interface from the drop-down list box to view the bandwidth usage of its bandwidth classes.
Class	This field displays the name of the bandwidth class. A <b>Default Class</b> automatically displays for all the bandwidth in the <b>Root Class</b> that is not allocated to bandwidth classes. If you do not enable maximize bandwidth usage on an interface, the ZyWALL uses the bandwidth in this default class to send traffic that does not match any of the bandwidth classes. <sup>a</sup>
Budget (kbps)	This field displays the amount of bandwidth allocated to the bandwidth class.
Current Usage (kbps)	This field displays the amount of bandwidth that each bandwidth class is using.
Refresh	Click <b>Refresh</b> to update the page.

a.If you allocate all the root class's bandwidth to the bandwidth classes, the default class still displays a budget of 2 kbps (the minimum amount of bandwidth that can be assigned to a bandwidth class).



# CHAPTER 26

## DNS

This chapter shows you how to configure the DNS screens.

### 26.1 DNS Overview

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

### 26.2 DNS Server Address Assignment

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

- 1 The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, manually enter them in the DNS server fields.
- 2 If your ISP dynamically assigns the DNS server IP addresses (along with the ZyWALL's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.
- 3 You can manually enter the IP addresses of other DNS servers. These servers can be public or private. A DNS server could even be behind a remote IPsec router (see [Section 26.5.1 on page 419](#)).

### 26.3 DNS Servers

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

- 1 Use the **DNS System** screen to configure the ZyWALL to use a DNS server to resolve domain names for ZyWALL system features like VPN, DDNS and the time server.
- 2 Use the **DNS DHCP** screen to configure the DNS server information that the ZyWALL sends to the DHCP client devices on the LAN, DMZ or WLAN.
- 3 Use the **REMOTE MGMT DNS** screen to configure the ZyWALL (in router mode) to accept or discard DNS queries.

## 26.4 Address Record

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

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

### 26.4.1 DNS Wildcard

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

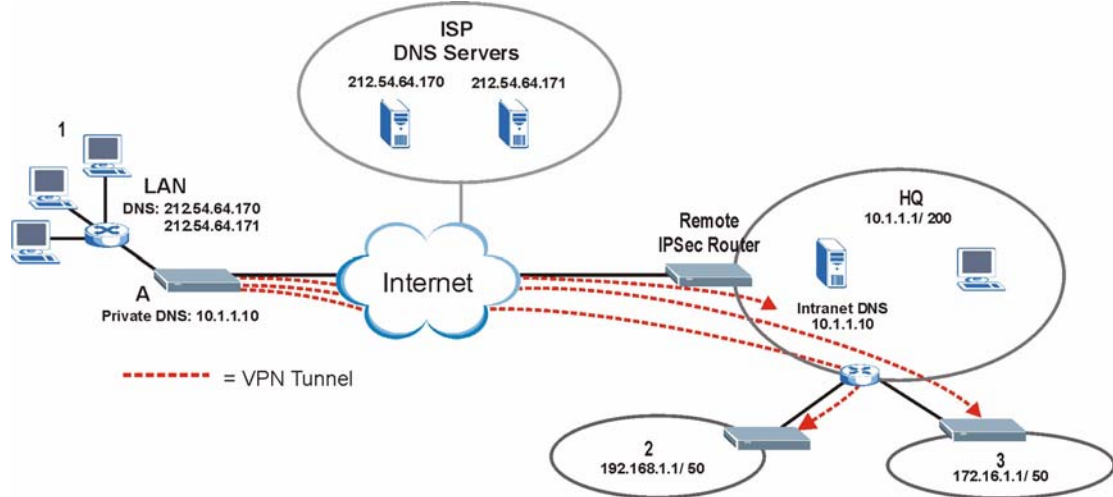
## 26.5 Name Server Record

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

### 26.5.1 Private DNS Server

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

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

**Figure 199** Private DNS Server Example

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

## 26.6 System Screen

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



**Figure 200** System DNS

### DNS

**System**
Cache
DHCP
DDNS

**Address Record**

#	FQDN	Wildcard	IP Address	Modify
1	www.zyxel.com.tw	Yes	172.23.19.78 ( WAN_1 )	
2	mail.zyxel.com.tw	No	172.21.3.200	

**Name Server Record**

#	Domain Zone	From	DNS Server	Modify
1	nctu.edu.tw	User-Defined	140.113.68.10	
2	*	WAN_1 ( 172.23.19.78 )	172.23.5.1 172.23.5.2	
-	*	Default	172.23.5.1 172.23.5.2	N/A

new record before record  (record number)

The following table describes the labels in this screen.

**Table 147** System DNS

LABEL	DESCRIPTION
Address Record	An address record specifies the mapping of a fully qualified domain name (FQDN) to an IP address. An FQDN consists of a host and domain name and includes the top-level domain. For example, www.zyxel.com.tw is a fully qualified domain name, where “www” is the host, “zyxel” is the second-level domain, and “com.tw” is the top level domain.
#	This is the index number of the address record.
FQDN	This is a host’s fully qualified domain name.
Wildcard	This column displays whether or not the DNS wildcard feature is enabled for this domain name.
IP Address	This is the IP address of a host.
Modify	Click the edit icon to go to the screen where you can edit the record. Click the delete icon to remove an existing record. A window display asking you to confirm that you want to delete the record. Note that subsequent records move up by one when you take this action.
Add	Click <b>Add</b> to open a screen where you can add a new address record. Refer to <a href="#">Table 148 on page 423</a> for information on the fields.

**Table 147** System DNS

LABEL	DESCRIPTION
Name Server Record	A name server record contains a DNS server's IP address. The ZyWALL can query the DNS server to resolve domain names for features like VPN, DDNS and the time server. When the ZyWALL needs to resolve a domain name, it checks it against the name server record entries in the order that they appear in this list. A "*" indicates a name server record without a domain zone. The default record is grayed out. The ZyWALL uses this default record if the domain name that needs to be resolved does not match any of the other name server records.
#	This is the index number of the name server record.
Domain Zone	A domain zone is a fully qualified domain name without the host. For example, zyxel.com.tw is the domain zone for the www.zyxel.com.tw fully qualified domain name.
From	This field displays whether the IP address of a DNS server is from a WAN interface (and which it is) or specified by the user.
DNS Server	This is the IP address of a DNS server.
Modify	Click a triangle icon to move the record up or down in the list. Click the edit icon to go to the screen where you can edit the record. Click the delete icon to remove an existing record. A window display asking you to confirm that you want to delete the record. Note that subsequent records move up by one when you take this action.
Insert	Click <b>Insert</b> to open a screen where you can insert a new name server record. Refer to <a href="#">Table 149 on page 424</a> for information on the fields.

## 26.6.1 Adding an Address Record

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

**Figure 201** System DNS: Add Address Record

The screenshot shows a dialog box titled "DNS - EDIT ADDRESS RECORD" with a sub-header "Address Record". The dialog contains the following fields and controls:

- FQDN:** A text input field.
- IP Address:** A dropdown menu currently showing "0.0.0.0 (WAN\_1)" and a text input field showing "0 . 0 . 0 . 0".
- WAN Interface:** A radio button that is selected.
- Custom:** A radio button that is unselected.
- Enable Wildcard:** A checkbox that is unselected.
- Buttons:** "Apply" and "Cancel" buttons at the bottom.

The following table describes the labels in this screen.

**Table 148** System DNS: Add Address Record

LABEL	DESCRIPTION
FQDN	Type a fully qualified domain name (FQDN) of a server. An FQDN starts with a host name and continues all the way up to the top-level domain name. For example, www.zyxel.com.tw is a fully qualified domain name, where “www” is the host, “zyxel” is the second-level domain, and “com.tw” is the top level domain.
IP Address	If this entry is for one of the WAN ports on a ZyWALL with multiple WAN ports, select <b>WAN Interface</b> and select WAN 1 or WAN 2 from the drop-down list box. If this entry is for the WAN port on a ZyWALL with a single WAN port, select <b>WAN Interface</b> . For entries that are not for the WAN port(s), select <b>Custom</b> and enter the IP address of the host in dotted decimal notation.
Enable Wildcard	Select the check box to enable DNS wildcard.
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

## 26.6.2 Inserting a Name Server record

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

**Figure 202** System DNS: Insert Name Server Record

**DNS - EDIT NAME SERVER RECORD**

**Name Server Record**

Domain Zone\*

\* Optional. Leave this field blank if all domain zones are served by the specified DNS server(s).

**DNS Server**

DNS Server(s) from ISP

First DNS Server	Second DNS Server	Third DNS Server
172.20.0.63	172.20.0.27	N/A

Public DNS Server

Private DNS Server

The following table describes the labels in this screen.

**Table 149** System DNS: Insert Name Server Record

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

## 26.7 DNS Cache

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

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

## 26.8 Configure DNS Cache

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

**Figure 203** DNS Cache

#	Cache Type	Domain Name	IP Address	Remaining Time (sec)	Modify
1	Positive	gfnet.zyxel.com.tw	203.160.254.59	3437	
2	Positive	ms07.spamcatcher.net	71.129.195.161	2297	

The following table describes the labels in this screen.

**Table 150** DNS Cache

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

**Table 150** DNS Cache

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

## 26.9 Configuring DNS DHCP

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

**Figure 204** DNS DHCP

The following table describes the labels in this screen.

**Table 151** DNS DHCP

LABEL	DESCRIPTION
DNS Servers Assigned by DHCP Server	The ZyWALL passes a DNS (Domain Name System) server IP address to the DHCP clients.
Selected Interface	Select an interface from the drop-down list box to configure the DNS servers for the specified interface.
DNS	These read-only labels represent the DNS servers.
IP	<p>Select <b>From ISP</b> if your ISP dynamically assigns DNS server information (and the ZyWALL's WAN IP address). Use the drop-down list box to select a DNS server IP address that the ISP assigns in the field to the right.</p> <p>Select <b>User-Defined</b> if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose <b>User-Defined</b>, but leave the IP address set to 0.0.0.0, <b>User-Defined</b> changes to <b>None</b> after you click <b>Apply</b>. If you set a second choice to <b>User-Defined</b>, and enter the same IP address, the second <b>User-Defined</b> changes to <b>None</b> after you click <b>Apply</b>.</p> <p>Select <b>DNS Relay</b> to have the ZyWALL act as a DNS proxy. The ZyWALL's LAN, DMZ or WLAN IP address displays in the field to the right (read-only). The ZyWALL tells the DHCP clients on the LAN, DMZ or WLAN that the ZyWALL itself is the DNS server. When a computer on the LAN, DMZ or WLAN sends a DNS query to the ZyWALL, the ZyWALL forwards the query to the ZyWALL's system DNS server (configured in the <b>DNS System</b> screen) and relays the response back to the computer. You can only select <b>DNS Relay</b> for one of the three servers; if you select DNS Relay for a second or third DNS server, that choice changes to <b>None</b> after you click <b>Apply</b>.</p> <p>Select <b>None</b> if you do not want to configure DNS servers. You must have another DHCP sever on your LAN, or else the computers must have their DNS server addresses manually configured. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.</p>
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 26.10 Dynamic DNS

Dynamic DNS allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with [www.dyndns.org](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 domain name. The Dynamic DNS service provider will give you a password or key.

**Note:** You must go to the Dynamic DNS service provider's website and register a user account and a domain name before you can use the Dynamic DNS service with your ZyWALL.

### 26.10.1 DYNDNS Wildcard

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

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

### 26.10.2 High Availability

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

## 26.11 Configuring Dynamic DNS

To change your ZyWALL's DDNS, click **ADVANCED**, **DNS**, then the **DDNS** tab. The screen appears as shown. Not all fields are available on all models.



**Figure 205** DDNS

The following table describes the labels in this screen.

**Table 152** DDNS

LABEL	DESCRIPTION
Account Setup	
Active	Select this check box to use dynamic DNS.
Service Provider	This is the name of your Dynamic DNS service provider.
Username	Enter your user name. You can use up to 31 alphanumeric characters (and the underscore). Spaces are not allowed.
Password	Enter the password associated with the user name above. You can use up to 31 alphanumeric characters (and the underscore). Spaces are not allowed.
My Domain Names	
Domain Name 1~5	Enter the host names in these fields.
DDNS Type	Select the type of service that you are registered for from your Dynamic DNS service provider. Select <b>Dynamic</b> if you have the Dynamic DNS service. Select <b>Static</b> if you have the Static DNS service. Select <b>Custom</b> if you have the Custom DNS service.
Offline	This option is available when <b>Custom</b> is selected in the <b>DDNS Type</b> field. Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line.
Wildcard	Select the check box to enable DYNDNS Wildcard.

**Table 152** DDNS

LABEL	DESCRIPTION
WAN Interface	Select the WAN port to use for updating the IP address of the domain name.
IP Address Update Policy	<p>Select <b>Use WAN IP Address</b> to have the ZyWALL update the domain name with the WAN port's IP address.</p> <p>Select <b>Use User-Defined</b> and enter the IP address if you have a static IP address.</p> <p>Select <b>Let DDNS Server Auto Detect</b> only when there are one or more NAT routers between the ZyWALL and the DDNS server. This feature has the DDNS server automatically detect and use the IP address of the NAT router that has a public IP address.</p> <p><b>Note:</b> The DDNS server may not be able to detect the proper IP address if there is an HTTP proxy server between the ZyWALL and the DDNS server.</p>
HA	<p>Select this check box to enable the high availability (HA) feature. High availability has the ZyWALL update a domain name with another port's IP address when the normal WAN port does not have a connection.</p> <p>If the WAN port specified in the <b>WAN Interface</b> field does not have a connection, the ZyWALL will attempt to use the IP address of another WAN port to update the domain name.</p> <p>When the WAN ports are in the active/passive operating mode, the ZyWALL will update the domain name with the IP address of whichever WAN port has a connection, regardless of the setting in the <b>WAN Interface</b> field.</p> <p>Disable this feature and the ZyWALL will only update the domain name with an IP address of the WAN port specified in the <b>WAN Interface</b> field. If that WAN port does not have a connection, the ZyWALL will not update the domain name with another port's IP address.</p> <p><b>Note:</b> If you enable high availability, DDNS can also function when the ZyWALL uses the dial backup port. DDNS does not function when the ZyWALL uses traffic redirect.</p>
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.



# CHAPTER 27

## Remote Management

This chapter provides information on the Remote Management screens.

### 27.1 Remote Management Overview

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

**Note:** When you configure remote management to allow management from the WAN, you still need to configure a firewall rule to allow access. See [Chapter 11 on page 214](#) for details on configuring firewall rules.

You may manage your ZyWALL from a remote location via:

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

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

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

You may only have one remote management session running at a time. The ZyWALL automatically disconnects a remote management session of lower priority when another remote management session of higher priority starts. The priorities for the different types of remote management sessions are as follows.

- 1 Console port
- 2 SSH
- 3 Telnet
- 4 HTTPS and HTTP

#### 27.1.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

- 1 A filter in SMT menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a Telnet, FTP or Web service.
- 2 You have disabled that service in one of the remote management screens.
- 3 The IP address in the **Secure Client IP Address** field does not match the client IP address. If it does not match, the ZyWALL will disconnect the session immediately.
- 4 There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.
- 5 There is a firewall rule that blocks it.

### 27.1.2 System Timeout

There is a default system management idle timeout of five minutes (three hundred seconds). The ZyWALL automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling. You can change the timeout period in the **System** screen.

## 27.2 Introduction to HTTPS

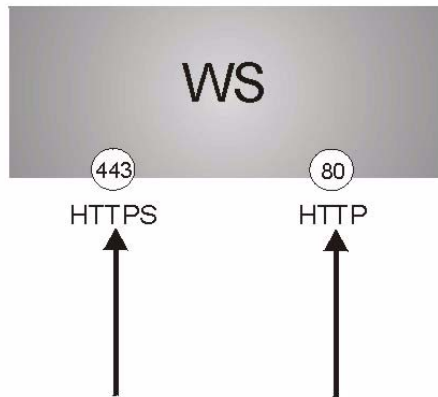
HTTPS (HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a web protocol that encrypts and decrypts web pages. Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data by ensuring confidentiality (an unauthorized party cannot read the transferred data), authentication (one party can identify the other party) and data integrity (you know if data has been changed).

It relies upon certificates, public keys, and private keys (see [Chapter 20 on page 342](#) for more information).

HTTPS on the ZyWALL is used so that you may securely access the ZyWALL using the web configurator. The SSL protocol specifies that the SSL server (the ZyWALL) must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the ZyWALL), whereas the SSL client only should authenticate itself when the SSL server requires it to do so (select **Authenticate Client Certificates** in the **REMOTE MGMT, WWW** screen). **Authenticate Client Certificates** is optional and if selected means the SSL-client must send the ZyWALL a certificate. You must apply for a certificate for the browser from a CA that is a trusted CA on the ZyWALL.

Please refer to the following figure.

- 1 HTTPS connection requests from an SSL-aware web browser go to port 443 (by default) on the ZyWALL's WS (web server).
- 2 HTTP connection requests from a web browser go to port 80 (by default) on the ZyWALL's WS (web server).

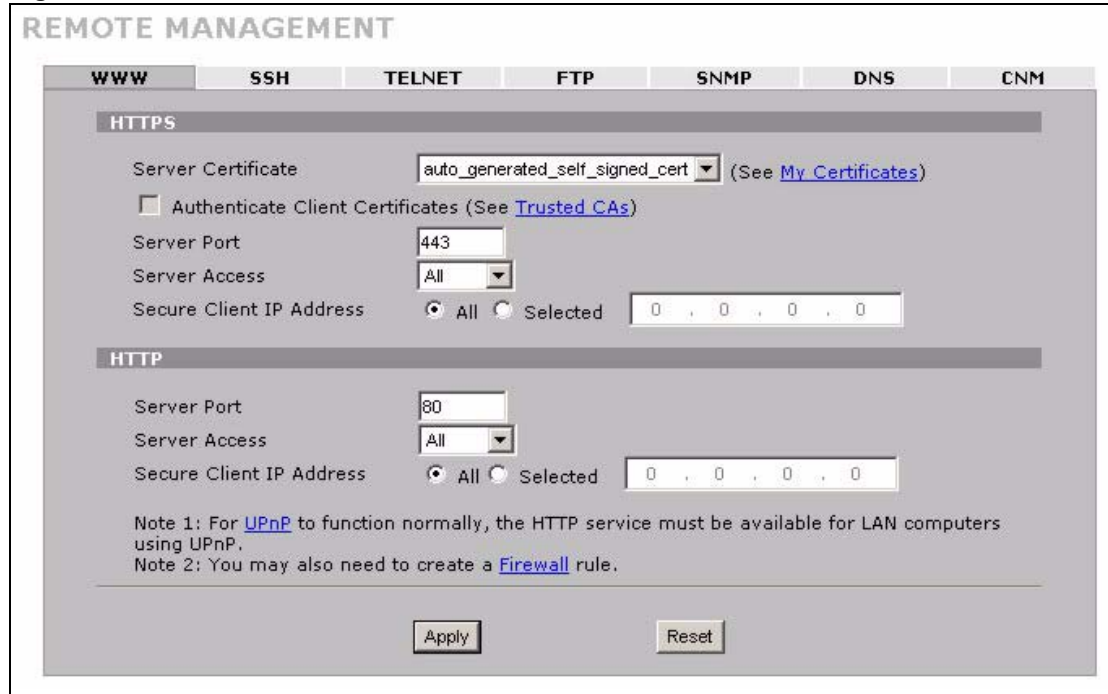
**Figure 206** HTTPS Implementation

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

## 27.3 WWW

Click **ADVANCED, REMOTE MGMT** to open the **WWW** screen. Use this screen to change your ZyWALL's web settings.

**Figure 207** WWW



The following table describes the labels in this screen.

**Table 153** WWW

LABEL	DESCRIPTION
HTTPS	
Server Certificate	Select the <b>Server Certificate</b> that the ZyWALL will use to identify itself. The ZyWALL is the SSL server and must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the ZyWALL).
Authenticate Client Certificates	Select <b>Authenticate Client Certificates</b> (optional) to require the SSL client to authenticate itself to the ZyWALL by sending the ZyWALL a certificate. To do that the SSL client must have a CA-signed certificate from a CA that has been imported as a trusted CA on the ZyWALL (see <a href="#">Appendix L on page 742</a> on importing certificates for details).
Server Port	The HTTPS proxy server listens on port 443 by default. If you change the HTTPS proxy server port to a different number on the ZyWALL, for example 8443, then you must notify people who need to access the ZyWALL web configurator to use "https://ZyWALL IP Address:8443" as the URL.
Server Access	Select a ZyWALL interface from <b>Server Access</b> on which incoming HTTPS access is allowed.  You can allow only secure web configurator access by setting the <b>HTTP Server Access</b> field to <b>Disable</b> and setting the <b>HTTPS Server Access</b> field to an interface(s).
Secure Client IP Address	A secure client is a "trusted" computer that is allowed to communicate with the ZyWALL using this service.  Select <b>All</b> to allow any computer to access the ZyWALL using this service.  Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the ZyWALL using this service.
HTTP	

**Table 153** WWW (continued)

LABEL	DESCRIPTION
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the ZyWALL using this service.
Secure Client IP Address	A secure client is a "trusted" computer that is allowed to communicate with the ZyWALL using this service. Select <b>All</b> to allow any computer to access the ZyWALL using this service. Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the ZyWALL using this service.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 27.4 HTTPS Example

If you haven't changed the default HTTPS port on the ZyWALL, then in your browser enter "https://ZyWALL IP Address/" as the web site address where "ZyWALL IP Address" is the IP address or domain name of the ZyWALL you wish to access.

### 27.4.1 Internet Explorer Warning Messages

When you attempt to access the ZyWALL HTTPS server, a Windows dialog box pops up asking if you trust the server certificate. Click **View Certificate** if you want to verify that the certificate is from the ZyWALL.

You see the following **Security Alert** screen in Internet Explorer. Select **Yes** to proceed to the web configurator login screen; if you select **No**, then web configurator access is blocked.

**Figure 208** Security Alert Dialog Box (Internet Explorer)



## 27.4.2 Netscape Navigator Warning Messages

When you attempt to access the ZyWALL HTTPS server, a **Website Certified by an Unknown Authority** screen pops up asking if you trust the server certificate. Click **Examine Certificate** if you want to verify that the certificate is from the ZyWALL.

If **Accept this certificate temporarily for this session** is selected, then click **OK** to continue in Netscape.

Select **Accept this certificate permanently** to import the ZyWALL's certificate into the SSL client.

**Figure 209** Security Certificate 1 (Netscape)



**Figure 210** Security Certificate 2 (Netscape)



### 27.4.3 Avoiding the Browser Warning Messages

The following describes the main reasons that your browser displays warnings about the ZyWALL's HTTPS server certificate and what you can do to avoid seeing the warnings.

- The issuing certificate authority of the ZyWALL's HTTPS server certificate is not one of the browser's trusted certificate authorities. The issuing certificate authority of the ZyWALL's factory default certificate is the ZyWALL itself since the certificate is a self-signed certificate.
  - For the browser to trust a self-signed certificate, import the self-signed certificate into your operating system as a trusted certificate.
  - To have the browser trust the certificates issued by a certificate authority, import the certificate authority's certificate into your operating system as a trusted certificate. Refer to [Appendix L on page 742](#) for details.
- The actual IP address of the HTTPS server (the IP address of the ZyWALL's port that you are trying to access) does not match the common name specified in the ZyWALL's HTTPS server certificate that your browser received. Do the following to check the common name specified in the certificate that your ZyWALL sends to HTTPS clients.
  - a** Click **REMOTE MGMT**. Write down the name of the certificate displayed in the **Server Certificate** field.
  - b** Click **CERTIFICATES**. Find the certificate and check its **Subject** column. CN stands for certificate's common name (see [Figure 214 on page 440](#) for an example).

Use this procedure to have the ZyWALL use a certificate with a common name that matches the ZyWALL's actual IP address. You cannot use this procedure if you need to access the WAN port and it uses a dynamically assigned IP address.

- a** Create a new certificate for the ZyWALL that uses the IP address (of the ZyWALL's port that you are trying to access) as the certificate's common name. For example, to use HTTPS to access a LAN port with IP address 192.168.1.1, create a certificate that uses 192.168.1.1 as the common name.
- b** Go to the remote management **WWW** screen and select the newly created certificate in the **Server Certificate** field. Click **Apply**.

### 27.4.4 Login Screen

After you accept the certificate, the ZyWALL login screen appears. The lock displayed in the bottom right of the browser status bar denotes a secure connection.

Figure 211 Login Screen (Internet Explorer)

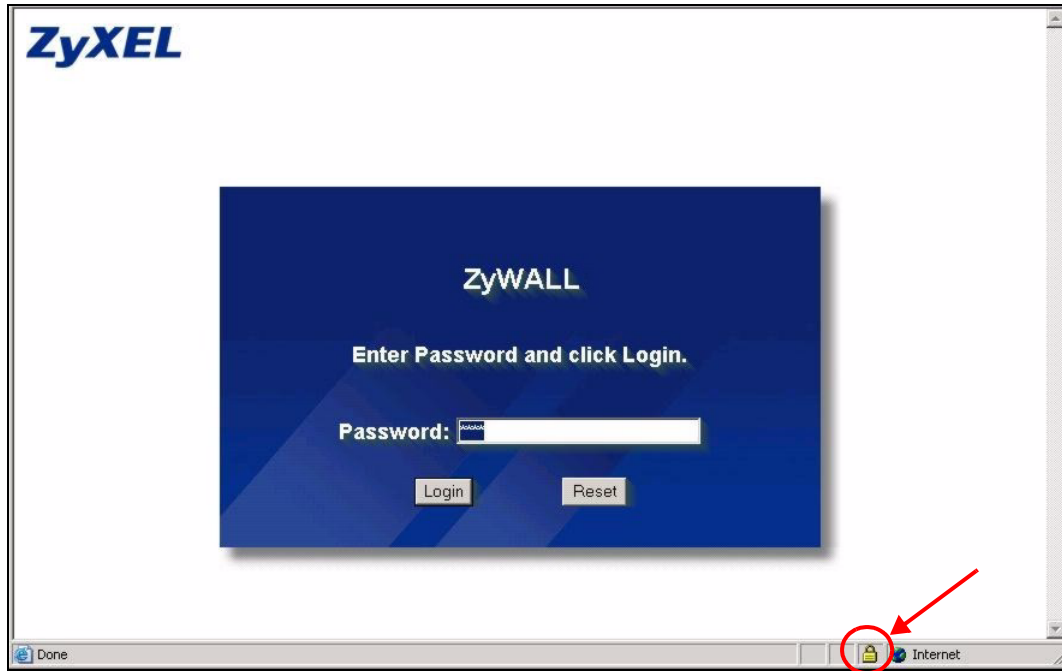


Figure 212 Login Screen (Netscape)



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

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

Figure 213 Replace Certificate



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

Figure 214 Device-specific Certificate



**CERTIFICATES**

My Certificates    Trusted CAs    Trusted Remote Hosts    Directory Servers

PKI Storage Space in Use

0%  3% 100%

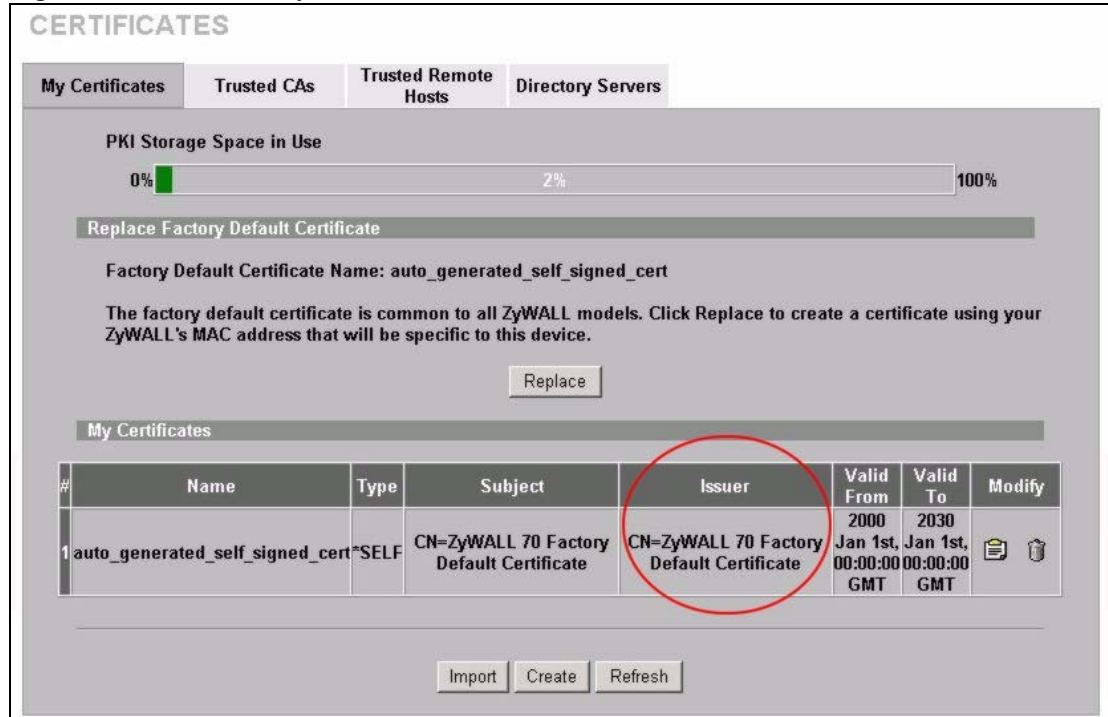
My Certificates

#	Name	Type	Subject	Issuer	Valid From	Valid To	Modify
1	auto_generated_self_signed_cert	*SELF	CN=ZyWALL 70 00A0C5012345	CN=ZyWALL 70 00A0C5012345	2000 Jan 1st, 00:00:00 GMT	2030 Jan 1st, 00:00:00 GMT	 

Import    Create    Refresh

Click **Ignore** in the **Replace Certificate** screen to use the common ZyWALL certificate. You will then see this information in the **My Certificates** screen.

**Figure 215** Common ZyWALL Certificate



## 27.5 SSH

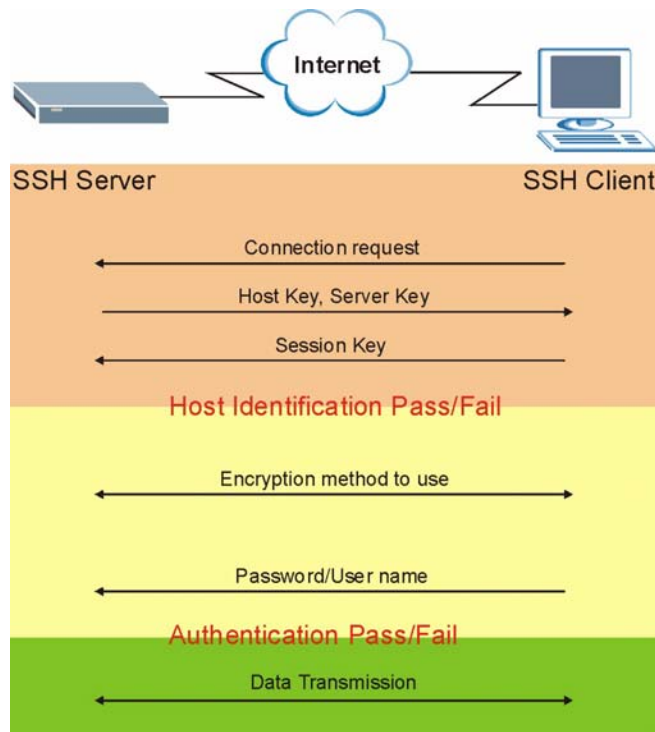
Unlike Telnet or FTP, which transmit data in clear text, SSH (Secure Shell) is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network.

**Figure 216** SSH Communication Example



## 27.6 How SSH works

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

**Figure 217** How SSH Works**1 Host Identification**

The SSH client sends a connection request to the SSH server. The server identifies itself with a host key. The client encrypts a randomly generated session key with the host key and server key and sends the result back to the server.

The client automatically saves any new server public keys. In subsequent connections, the server public key is checked against the saved version on the client computer.

**2 Encryption Method**

Once the identification is verified, both the client and server must agree on the type of encryption method to use.

**3 Authentication and Data Transmission**

After the identification is verified and data encryption activated, a secure tunnel is established between the client and the server. The client then sends its authentication information (user name and password) to the server to log in to the server.

## 27.7 SSH Implementation on the ZyWALL

Your ZyWALL supports SSH version 1.5 using RSA authentication and three encryption methods (DES, 3DES and Blowfish). The SSH server is implemented on the ZyWALL for remote SMT management and file transfer on port 22. Only one SSH connection is allowed at a time.

## 27.7.1 Requirements for Using SSH

You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to the ZyWALL over SSH.

## 27.8 Configuring SSH

Click **ADVANCED**, **REMOTE MGMT** and then the **SSH** tab to change your ZyWALL's Secure Shell settings.

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

**Figure 218** SSH

The following table describes the labels in this screen.

**Table 154** SSH

LABEL	DESCRIPTION
Server Host Key	Select the certificate whose corresponding private key is to be used to identify the ZyWALL for SSH connections. You must have certificates already configured in the <b>My Certificates</b> screen (Click <b>My Certificates</b> and see <a href="#">Chapter 20 on page 342</a> for details).
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the ZyWALL using this service.
Secure Client IP Address	A secure client is a “trusted” computer that is allowed to communicate with the ZyWALL using this service. Select <b>All</b> to allow any computer to access the ZyWALL using this service. Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the ZyWALL using this service.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.



## 27.9 Secure Telnet Using SSH Examples

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

### 27.9.1 Example 1: Microsoft Windows

This section describes how to access the ZyWALL using the Secure Shell Client program.

- 1 Launch the SSH client and specify the connection information (IP address, port number or device name) for the ZyWALL.
- 2 Configure the SSH client to accept connection using SSH version 1.
- 3 A window displays prompting you to store the host key in you computer. Click **Yes** to continue.

**Figure 219** SSH Example 1: Store Host Key



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

### 27.9.2 Example 2: Linux

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

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

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

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



**Figure 220** SSH Example 2: Test

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

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

Then enter the password to log in to the ZyWALL.

**Figure 221** SSH Example 2: Log in

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

- 3 The SMT main menu displays next.

## 27.10 Secure FTP Using SSH Example

This section shows an example on file transfer using the OpenSSH client program. The configuration and connection steps are similar for other SSH client programs. Refer to your SSH client program user's guide.

- 1 Enter “sftp -1 192.168.1.1”. This command forces your computer to connect to the ZyWALL for secure file transfer using SSH version 1. If this is the first time you are connecting to the ZyWALL using SSH, a message displays prompting you to save the host information of the ZyWALL. Type “yes” and press [ENTER].
- 2 Enter the password to login to the ZyWALL.
- 3 Use the “put” command to upload a new firmware to the ZyWALL.

**Figure 222** Secure FTP: Firmware Upload Example

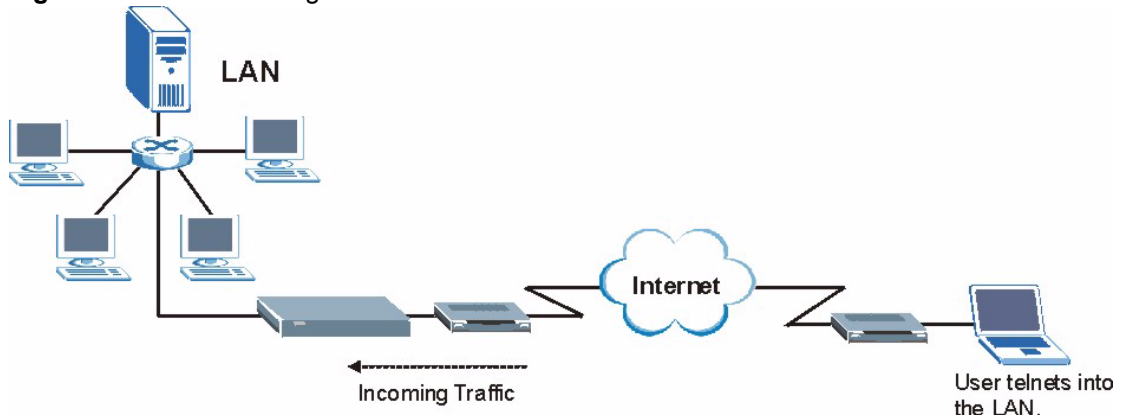
```

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

```

## 27.11 Telnet

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

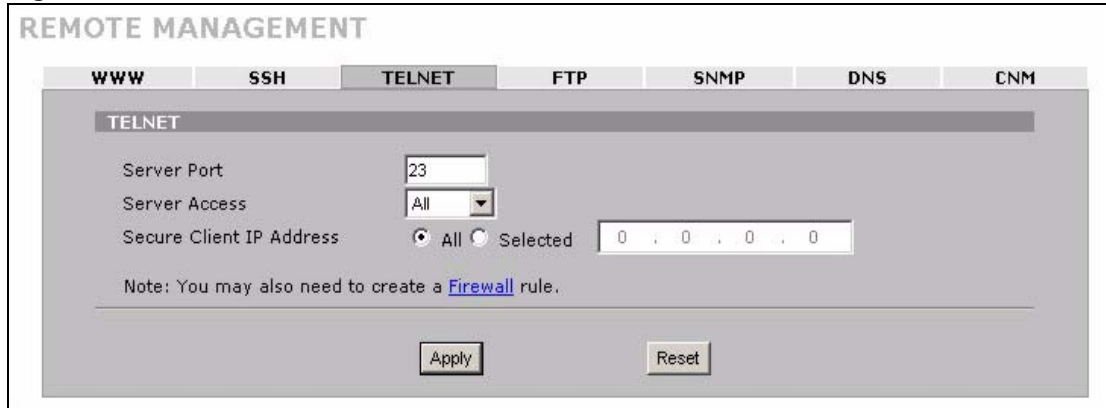
**Figure 223** Telnet Configuration on a TCP/IP Network

## 27.12 Configuring TELNET

Click **ADVANCED**, **REMOTE MGMT** and then the **TELNET** tab to configure your ZyWALL for remote Telnet access.

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

**Figure 224** Telnet



The following table describes the labels in this screen.

**Table 155** Telnet

LABEL	DESCRIPTION
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the ZyWALL using this service.
Secure Client IP Address	A secure client is a “trusted” computer that is allowed to communicate with the ZyWALL using this service. Select <b>All</b> to allow any computer to access the ZyWALL using this service. Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the ZyWALL using this service.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 27.13 FTP

You can upload and download the ZyWALL’s firmware and configuration files using FTP, please see the chapter on firmware and configuration file maintenance for details. To use this feature, your computer must have an FTP client.

To change your ZyWALL’s FTP settings, click **ADVANCED**, **REMOTE MGMT** and then the **FTP** tab. The screen appears as shown.

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

**Figure 225** FTP

The screenshot shows the 'REMOTE MANAGEMENT' configuration page for the FTP service. At the top, there are tabs for WWW, SSH, TELNET, FTP, SNMP, DNS, and CNM. The 'FTP' tab is selected. Below the tabs, there are three main configuration fields: 'Server Port' with a text box containing '21', 'Server Access' with a dropdown menu set to 'All', and 'Secure Client IP Address' with radio buttons for 'All' (selected) and 'Selected', followed by an IP address input field showing '0 . 0 . 0 . 0'. A note below these fields states: 'Note: You may also need to create a [Firewall](#) rule.' At the bottom of the configuration area, there are two buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

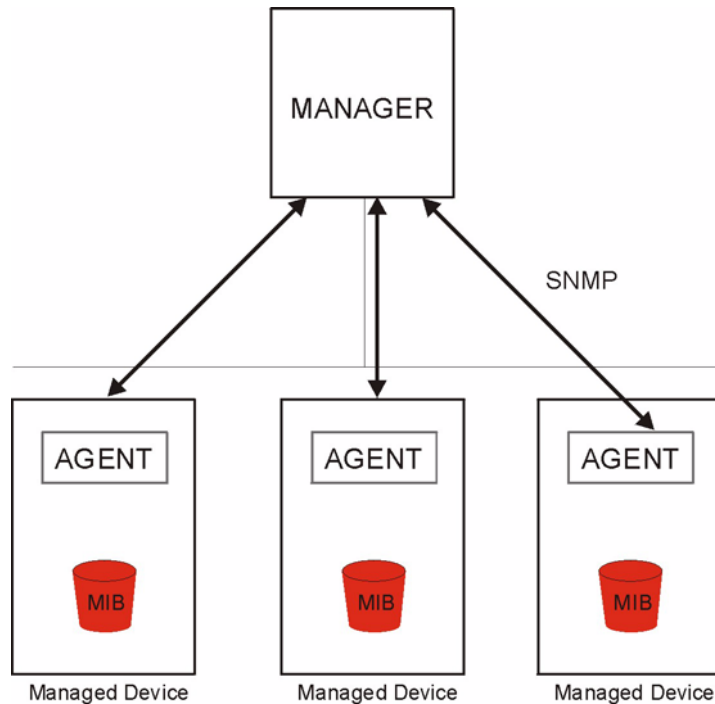
**Table 156** FTP

LABEL	DESCRIPTION
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the ZyWALL using this service.
Secure Client IP Address	A secure client is a "trusted" computer that is allowed to communicate with the ZyWALL using this service. Select <b>All</b> to allow any computer to access the ZyWALL using this service. Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the ZyWALL using this service.
Apply	Click <b>Apply</b> to save your customized settings.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 27.14 SNMP

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

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

**Figure 226** SNMP Management Model

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

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

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

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

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

## 27.14.1 Supported MIBs

The ZyWALL supports MIB II that is defined in RFC-1213 and RFC-1215. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance.

## 27.14.2 SNMP Traps

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

**Table 157** SNMP Traps

TRAP #	TRAP NAME	DESCRIPTION
0	coldStart (defined in <i>RFC-1215</i> )	A trap is sent after booting (power on).
1	warmStart (defined in <i>RFC-1215</i> )	A trap is sent after booting (software reboot).
4	authenticationFailure (defined in <i>RFC-1215</i> )	A trap is sent to the manager when receiving any SNMP get or set requirements with the wrong community (password).
6	whyReboot (defined in ZYXEL-MIB)	A trap is sent with the reason of restart before rebooting when the system is going to restart (warm start).
6a	For intentional reboot :	A trap is sent with the message "System reboot by user!" if reboot is done intentionally, (for example, download new files, CLI command "sys reboot", etc.).
6b	For fatal error :	A trap is sent with the message of the fatal code if the system reboots because of fatal errors.

## 27.14.3 REMOTE MANAGEMENT: SNMP

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

**Figure 227** SNMP

The screenshot shows the 'REMOTE MANAGEMENT' interface with the 'SNMP' tab selected. Under 'SNMP Configuration', there are four text input fields: 'Get Community' (public), 'Set Community' (public), 'Trap Community' (public), and 'Destination' (0.0.0.0). Below this is the 'SNMP' section with 'Service Port' (161), 'Service Access' (All), and 'Secure Client IP Address' (All selected). A note at the bottom states: 'Note: You may also need to create a [Firewall](#) rule.' There are 'Apply' and 'Reset' buttons at the bottom.

The following table describes the labels in this screen.

**Table 158** SNMP

LABEL	DESCRIPTION
SNMP Configuration	
Get Community	Enter the <b>Get Community</b> , which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.
Set Community	Enter the <b>Set community</b> , which is the password for incoming Set requests from the management station. The default is public and allows all requests.
Trap	
Community	Type the trap community, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests.
Destination	Type the IP address of the station to send your SNMP traps to.
SNMP	
Service Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Service Access	Select the interface(s) through which a computer may access the ZyWALL using this service.
Secure Client IP Address	A secure client is a "trusted" computer that is allowed to communicate with the ZyWALL using this service. Select <b>All</b> to allow any computer to access the ZyWALL using this service. Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the ZyWALL using this service.
Apply	Click <b>Apply</b> to save your customized settings.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 27.15 DNS

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa. Refer to [Chapter 7 on page 130](#) for more information.

Click **ADVANCED, REMOTE MGMT** and then the **DNS** tab to change your ZyWALL's DNS settings. Use this screen to set from which IP address the ZyWALL will accept DNS queries and on which interface it can send them your ZyWALL's DNS settings. This feature is not available when the ZyWALL is set to bridge mode.

**Figure 228** DNS

The screenshot shows the 'REMOTE MANAGEMENT' interface with the 'DNS' tab selected. The configuration fields are as follows:

- Service Port:** 53
- Service Access:** All
- Secure Client IP Address:** All (selected), Selected (0.0.0.0)

Note: You may also need to create a [Firewall](#) rule.

Buttons: Apply, Reset

The following table describes the labels in this screen.

**Table 159** DNS

LABEL	DESCRIPTION
Server Port	The DNS service port number is 53 and cannot be changed here.
Service Access	Select the interface(s) through which a computer may send DNS queries to the ZyWALL.
Secure Client IP Address	A secure client is a "trusted" computer that is allowed to send DNS queries to the ZyWALL. Select <b>All</b> to allow any computer to send DNS queries to the ZyWALL. Choose <b>Selected</b> to just allow the computer with the IP address that you specify to send DNS queries to the ZyWALL.
Apply	Click <b>Apply</b> to save your customized settings.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 27.16 Introducing Vantage CNM

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



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

## 27.17 Configuring CNM

Vantage CNM is disabled on the device by default. Click **ADVANCED**, **REMOTE MGMT** in the navigation panel and then click the **CNM** tab to configure your device's Vantage CNM settings.

**Figure 229** CNM

The following table describes the labels in this screen.

**Table 160** CNM

LABEL	DESCRIPTION
Registration Information	
Registration Status	<p>This read only field displays <b>Not Registered</b> when <b>Enable</b> is not selected. It displays <b>Registering</b> when the ZyWALL first connects with the Vantage CNM server and then <b>Registered</b> after it has been successfully registered with the Vantage CNM server. It will continue to display <b>Registering</b> until it successfully registers with the Vantage CNM server. It will not be able to register with the Vantage CNM server if:</p> <ul style="list-style-type: none"> <li>• The Vantage CNM server is down.</li> <li>• The Vantage CNM server IP address is incorrect.</li> <li>• The Vantage CNM server is behind a NAT router or firewall that does not forward packets through to the Vantage CNM server.</li> <li>• The encryption algorithms and/or encryption keys do not match between the ZyWALL and the Vantage CNM server.</li> </ul>

**Table 160** CNM (continued)

LABEL	DESCRIPTION
Last Registration Time	This field displays the last date (year-month-date) and time (hours-minutes-seconds) that the ZyWALL registered with the Vantage CNM server. It displays all zeroes if it has not yet registered with the Vantage CNM server.
Refresh	Click <b>Refresh</b> to update the registration status and last registration time.
Vantage CNM Setup	
Enable	Select this check box to allow Vantage CNM to manage your ZyWALL.
Vantage CNM Server Address	<p>If the Vantage server is on the same subnet as the ZyXEL device, enter the private or public IP address of the Vantage server.</p> <p>If the Vantage CNM server is on a different subnet to the ZyWALL, enter the public IP address of the Vantage server.</p> <p>If the Vantage CNM server is on a different subnet to the ZyWALL and is behind a NAT router, enter the WAN IP address of the NAT router here and configure the NAT router to forward UDP port 1864 traffic to the Vantage CNM server.</p> <p>If the Vantage CNM server is behind a firewall, you may have to create a rule on the firewall to allow UDP port 1864 traffic through to the Vantage CNM server (most (new) ZyXEL firewalls automatically allow this).</p>
Encryption Algorithm	The <b>Encryption Algorithm</b> field is used to encrypt communications between the ZyWALL and the Vantage CNM server. Choose from <b>None</b> (no encryption), <b>DES</b> or <b>3DES</b> . The <b>Encryption Key</b> field appears when you select <b>DES</b> or <b>3DES</b> . The ZyWALL must use the same encryption algorithm as the Vantage CNM server.
Encryption Key	Type eight alphanumeric characters ("0" to "9", "a" to "z" or "A" to "Z") when you choose the <b>DES</b> encryption algorithm and 24 alphanumeric characters ("0" to "9", "a" to "z" or "A" to "Z") when you choose the <b>3DES</b> encryption algorithm. The ZyWALL must use the same encryption key as the Vantage CNM server.
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.



# CHAPTER 28

## UPnP

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

### 28.1 Universal Plug and Play Overview

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

#### 28.1.1 How Do I Know If I'm Using UPnP?

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

#### 28.1.2 NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

- Dynamic port mapping
- Learning public IP addresses
- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

See [Chapter 22 on page 374](#) for further information about NAT.

#### 28.1.3 Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

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

### 28.1.4 UPnP and ZyXEL

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

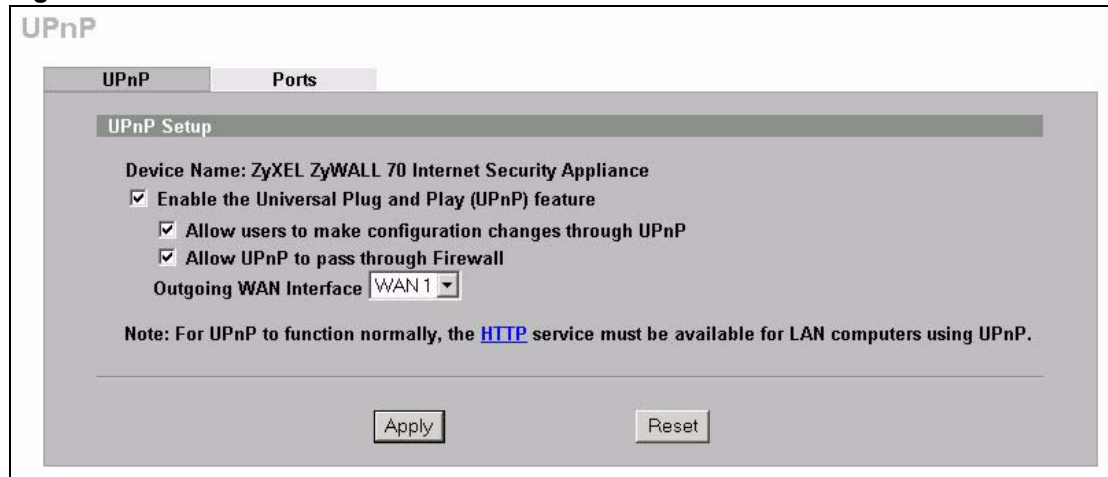
The ZyWALL only sends UPnP multicasts to the LAN.

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

## 28.2 Configuring UPnP

Click **UPnP** to display the **UPnP** screen. Not all fields are available on all models.

**Figure 230** UPnP



The following table describes the fields in this screen.

**Table 161** UPnP

LABEL	DESCRIPTION
UPnP Setup	
Device Name	This identifies the ZyXEL device in UPnP applications.
Enable the Universal Plug and Play (UPnP) feature	Select this checkbox to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the ZyWALL's IP address (although you must still enter the password to access the web configurator).

**Table 161** UPnP

LABEL	DESCRIPTION
Allow users to make configuration changes through UPnP	Select this check box to allow UPnP-enabled applications to automatically configure the ZyWALL so that they can communicate through the ZyWALL, for example by using NAT traversal. UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application.
Allow UPnP to pass through Firewall	Select this check box to allow traffic from UPnP-enabled applications to bypass the firewall. Clear this check box to have the firewall block all UPnP application packets (for example, MSN packets).
Outgoing WAN Interface	Select through which WAN port you want to send out traffic from UPnP-enabled applications. If the WAN port you select loses its connection, the ZyWALL attempts to use the other WAN port. If the other WAN port also does not work, the ZyWALL drops outgoing packets from UPnP-enabled applications.
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 28.3 Displaying UPnP Port Mapping

Click **UPnP** and then **Ports** to display the UPnP Ports screen. Use this screen to view the NAT port mapping rules that UPnP creates on the ZyWALL. Not all fields are available on all models.

**Figure 231** UPnP Ports

The screenshot shows the 'UPnP' configuration page with the 'Ports' tab active. The 'Ports Setup' section includes a checked checkbox for 'Reserve UPnP NAT rules in flash after system bootup'. Below this, it states 'WAN Interface in Use: WAN 1'. A table with the following columns is visible: '#', 'Remote Host', 'External Port', 'Protocol', 'Internal Port', 'Internal Client', 'Enabled', 'Description', and 'Lease Duration'. At the bottom of the page, there are 'Apply' and 'Refresh' buttons.

The following table describes the labels in this screen.

**Table 162** UPnP Ports

LABEL	DESCRIPTION
Reserve UPnP NAT rules in flash after system bootup	Select this check box to have the ZyWALL retain UPnP created NAT rules even after restarting. If you use UPnP and you set a port on your computer to be fixed for a specific service (for example FTP for file transfers), this option allows the ZyWALL to keep a record when your computer uses UPnP to create a NAT forwarding rule for that service.
WAN Interface in Use	This field displays through which WAN port the ZyWALL is currently sending out traffic from UPnP-enabled applications. This field displays <b>None</b> when UPnP is disabled or neither of the WAN ports has a connection.
The following read-only table displays information about the UPnP-created NAT mapping rule entries in the ZyWALL's NAT routing table.	
#	This is the index number of the UPnP-created NAT mapping rule entry.
Remote Host	This field displays the source IP address (on the WAN) of inbound IP packets. Since this is often a wildcard, the field may be blank. When the field is blank, the ZyWALL forwards all traffic sent to the <b>External Port</b> on the WAN interface to the <b>Internal Client</b> on the <b>Internal Port</b> . When this field displays an external IP address, the NAT rule has the ZyWALL forward inbound packets to the <b>Internal Client</b> from that IP address only.
External Port	This field displays the port number that the ZyWALL "listens" on (on the WAN port) for connection requests destined for the NAT rule's <b>Internal Port</b> and <b>Internal Client</b> . The ZyWALL forwards incoming packets (from the WAN) with this port number to the <b>Internal Client</b> on the <b>Internal Port</b> (on the LAN). If the field displays "0", the ZyWALL ignores the <b>Internal Port</b> value and forwards requests on all external port numbers (that are otherwise unmapped) to the <b>Internal Client</b> .
Protocol	This field displays the protocol of the NAT mapping rule (TCP or UDP).
Internal Port	This field displays the port number on the <b>Internal Client</b> to which the ZyWALL should forward incoming connection requests.
Internal Client	This field displays the DNS host name or IP address of a client on the LAN. Multiple NAT clients can use a single port simultaneously if the internal client field is set to 255.255.255.255 for UDP mappings.
Enabled	This field displays whether or not this UPnP-created NAT mapping rule is turned on. The UPnP-enabled device that connected to the ZyWALL and configured the UPnP-created NAT mapping rule on the ZyWALL determines whether or not the rule is enabled.
Description	This field displays a text explanation of the NAT mapping rule.
Lease Duration	This field displays a dynamic port-mapping rule's time to live (in seconds). It displays "0" if the port mapping is static.
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Refresh	Click <b>Refresh</b> update the screen's table.

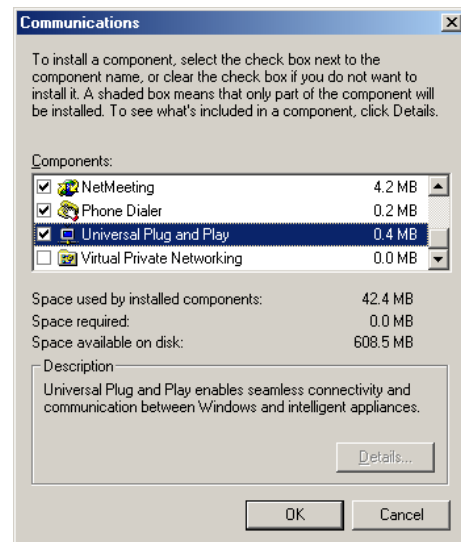
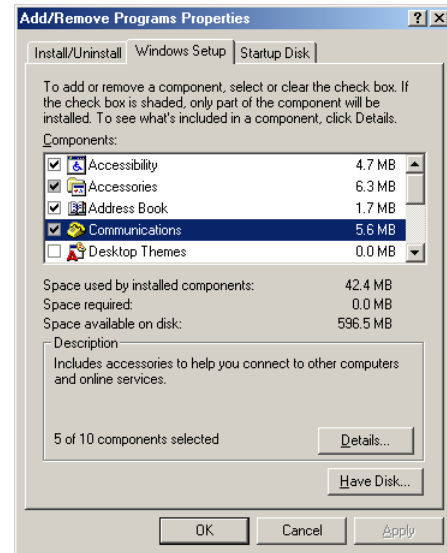
## 28.4 Installing UPnP in Windows Example

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

## 28.4.1 Installing UPnP in Windows Me

Follow the steps below to install UPnP in Windows Me.

- 1 Click **Start, Settings and Control Panel**. Double-click **Add/Remove Programs**.
- 2 Click on the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.
- 3 In the **Communications** window, select the **Universal Plug and Play** check box in the **Components** selection box.
- 4 Click **OK** to go back to the **Add/Remove Programs Properties** window and click **Next**.
- 5 Restart the computer when prompted.

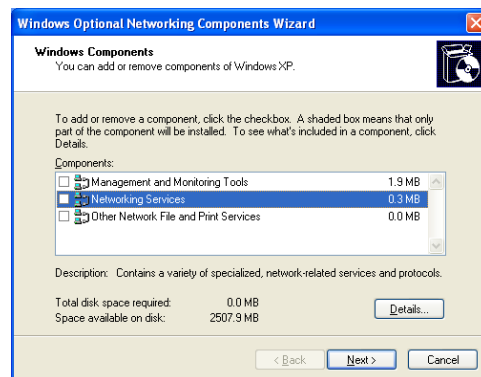
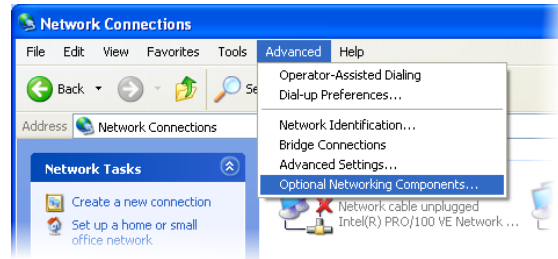




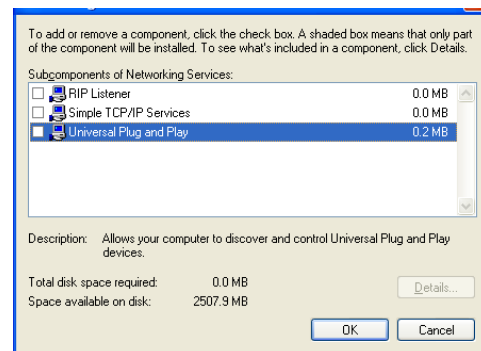
## 28.4.2 Installing UPnP in Windows XP

Follow the steps below to install UPnP in Windows XP.

- 1 Click **Start, Settings and Control Panel**.
- 2 Double-click **Network Connections**.
- 3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ...**.  
The **Windows Optional Networking Components Wizard** window displays.
- 4 Select **Networking Service** in the **Components** selection box and click **Details**.



- 5 In the **Networking Services** window, select the **Universal Plug and Play** check box.
- 6 Click **OK** to go back to the **Windows Optional Networking Component Wizard** window and click **Next**.



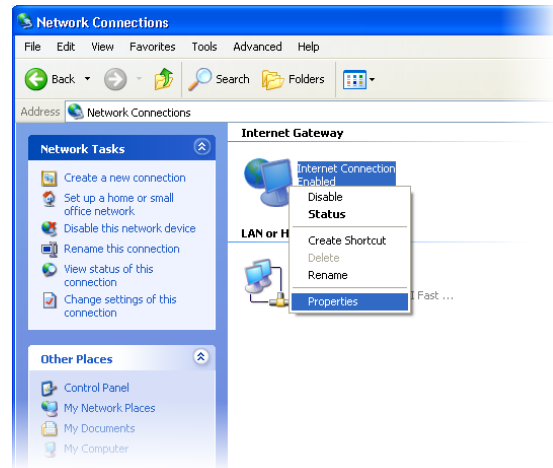
## 28.5 Using UPnP in Windows XP Example

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

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

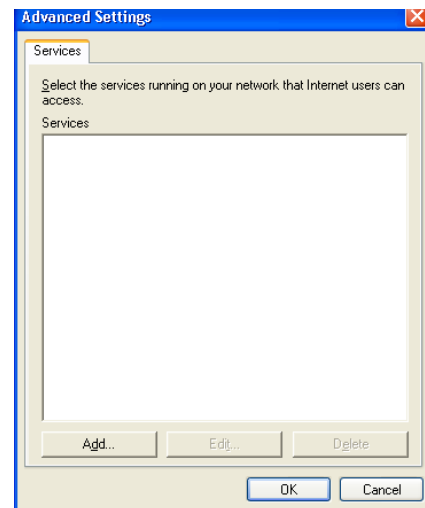
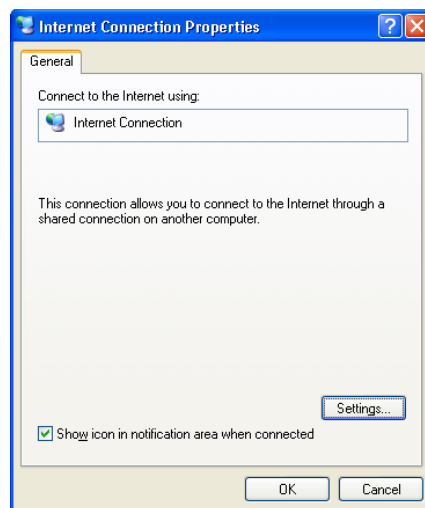
## 28.5.1 Auto-discover Your UPnP-enabled Network Device

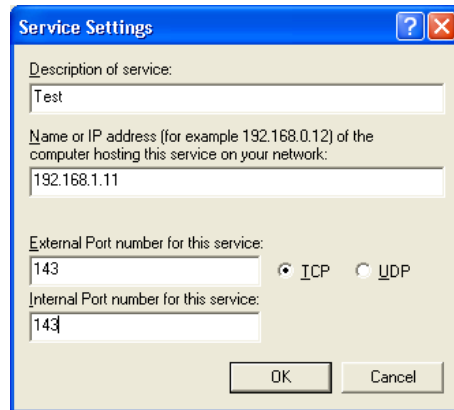
- 1 Click **Start** and **Control Panel**. Double-click **Network Connections**. An icon displays under **Internet Gateway**.
- 2 Right-click the icon and select **Properties**.



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

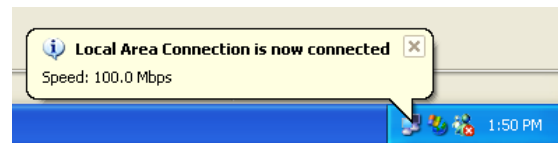
You may edit or delete the port mappings or click **Add** to manually add port mappings.



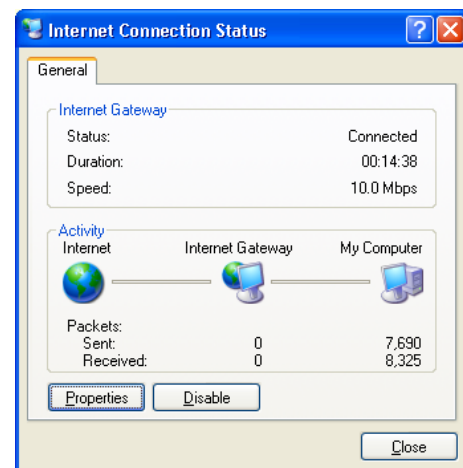


**Note:** When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

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



- 5 Double-click the icon to display your current Internet connection status.

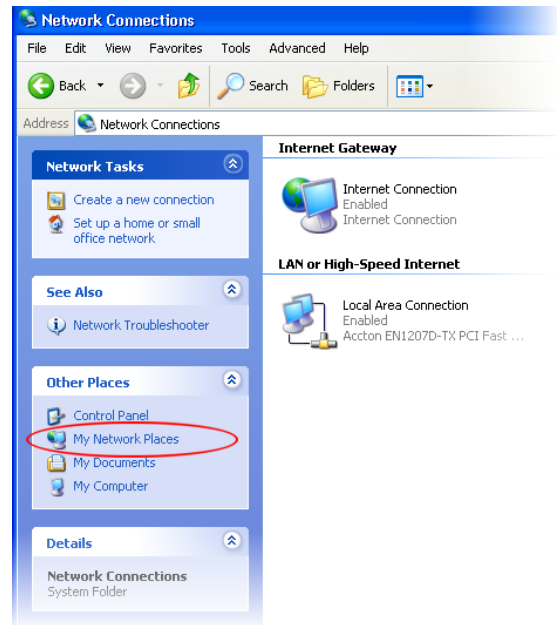


## 28.5.2 Web Configurator Easy Access

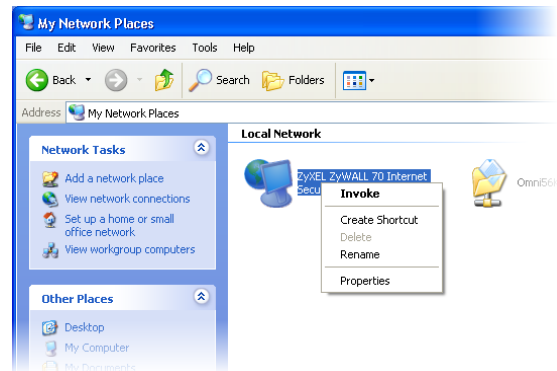
With UPnP, you can access the web-based configurator on the ZyXEL device without finding out the IP address of the ZyXEL device first. This is helpful if you do not know the IP address of the ZyXEL device.

Follow the steps below to access the web configurator.

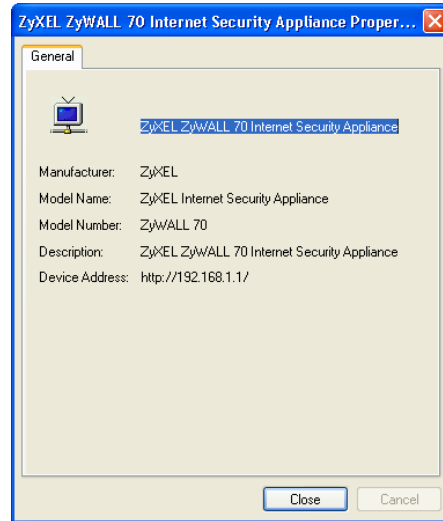
- 1 Click **Start** and then **Control Panel**.
- 2 Double-click **Network Connections**.
- 3 Select **My Network Places** under **Other Places**.



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



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



# CHAPTER 29

## ALG Screen

This chapter covers how to use the ZyWALL's ALG feature to allow certain applications to pass through the ZyWALL.

### 29.1 ALG Introduction

The ZyWALL can function as an Application Layer Gateway (ALG) to allow certain NAT un-friendly applications (such as SIP) to operate properly through the ZyWALL.

Some applications cannot operate through NAT (are NAT un-friendly) because they embed IP addresses and port numbers in their packets' data payload. The ZyWALL examines and uses IP address and port number information embedded in the data stream. When a device behind the ZyWALL uses an application for which the ZyWALL has ALG service enabled, the ZyWALL translates the device's private IP address inside the data stream to a public IP address. It also records session port numbers and dynamically creates implicit NAT port forwarding and firewall rules for the application's traffic to come in from the WAN to the LAN.

#### 29.1.1 ALG and NAT

The ZyWALL dynamically creates an implicit NAT session for the application's traffic from the WAN to the LAN.

The ALG on the ZyWALL supports all NAT mapping types, including **One to One**, **Many to One**, **Many to Many Overload** and **Many One to One**.

#### 29.1.2 ALG and the Firewall

The ZyWALL uses the dynamic port that the session uses for data transfer in creating an implicit temporary firewall rule for the session's traffic. The firewall rule only allows the session's traffic to go through in the direction that the ZyWALL determines from its inspection of the data payload of the application's packets. The firewall rule is automatically deleted after the application's traffic has gone through.

#### 29.1.3 ALG and Multiple WAN

When the ZyWALL has two WAN ports and uses the second highest priority WAN port as a back up, traffic cannot pass through when the primary WAN port connection fails. The ZyWALL does not automatically change the connection to the secondary WAN port.

If the primary WAN connection fails, the client needs to re-initialize the connection through the secondary WAN port to have the connection go through the secondary WAN port.

When the ZyWALL uses both of the WAN ports at the same time, you can configure routing policies to specify the WAN port that the connection's traffic is to use.

## 29.2 FTP

File Transfer Protocol (FTP) is an Internet file transfer service that operates on the Internet and over TCP/IP networks. 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. The FTP ALG allows TCP packets with a port 21 destination to pass through. If the FTP server is located on the LAN, you must also configure NAT port forwarding and firewall rules if you want to allow access to the server from the WAN.

## 29.3 H.323

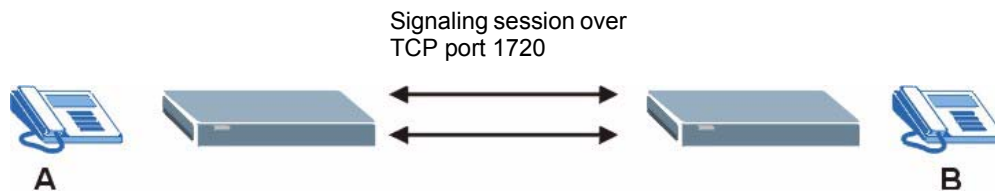
H.323 is a standard teleconferencing protocol suite that provides audio, data and video conferencing. It allows for real-time point-to-point and multipoint communication between client computers over a packet-based network that does not provide a guaranteed quality of service. NetMeeting uses H.323.

## 29.4 RTP

When you make a VoIP call using H.323 or SIP, the RTP (Real time Transport Protocol) is used to handle voice data transfer. See RFC 1889 for details on RTP.

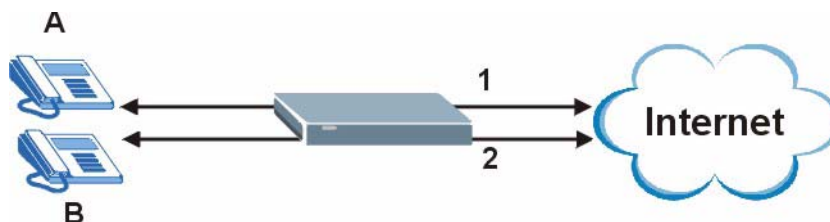
### 29.4.1 H.323 ALG Details

- The H.323 ALG supports peer-to-peer H.323 calls.
- The H.323 ALG handles H.323 calls that go through NAT or that the ZyWALL routes. You can also make other H.323 calls that do not go through NAT or routing. Examples would be calls between LAN IP addresses that are on the same subnet.
- The H.323 ALG allows calls to go out through NAT. For example, you could make a call from a private IP address on the LAN to a peer device on the WAN.
- You must configure the firewall and port forwarding to allow incoming (peer-to-peer) calls from the WAN to a private IP address on the LAN (or DMZ). The following example shows H.323 signaling and audio sessions between H.323 devices A and B.

**Figure 232** H.323 ALG Example

- With multiple WAN IP addresses on the ZyWALL, you can configure different firewall and port forwarding rules to allow incoming calls from each WAN IP address to go to a specific IP address on the LAN (or DMZ). Use policy routing to have the H.323 calls from each of those LAN or DMZ IP addresses go out through the same WAN IP address that calls come in on. The policy routing lets the ZyWALL correctly forward the return traffic for the calls initiated from the LAN IP addresses.

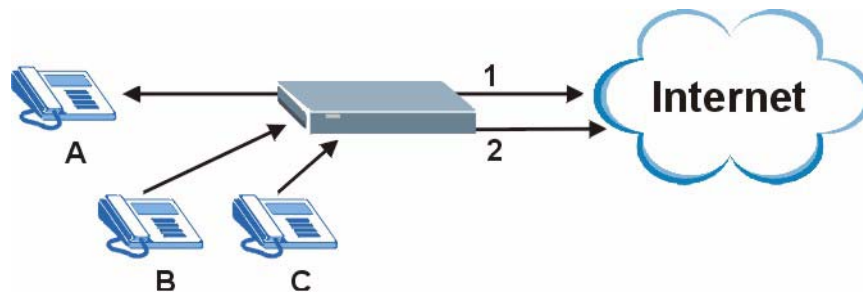
For example, you configure firewall and port forwarding rules to allow LAN IP address **A** to receive calls through public WAN IP address **1**. You configure different firewall and port forwarding rules to allow LAN IP address **B** to receive calls through public WAN IP address **2**. You configure corresponding policy routes to have calls from LAN IP address **A** go out through WAN IP address **1** and calls from LAN IP address **B** go out through WAN IP address **2**.

**Figure 233** H.323 with Multiple WAN IP Addresses

- When you configure the firewall and port forwarding to allow calls from the WAN to a specific IP address on the LAN, you can also use policy routing to have H.323 calls from other LAN or DMZ IP addresses go out through a different WAN IP address. The policy routing lets the ZyWALL correctly forward the return traffic for the calls initiated from the LAN IP addresses.

For example, you configure the firewall and port forwarding to allow LAN IP address **A** to receive calls from the Internet through WAN IP address **1**. You also use a policy route to have LAN IP address **A** make calls out through WAN IP address **1**. Configure another policy route to have H.323 calls from LAN IP addresses **B** and **C** go out through WAN IP address **2**. Even though only LAN IP address **A** can receive incoming calls from the Internet, LAN IP addresses **B** and **C** can still make calls out to the Internet.



**Figure 234** H.323 Calls from the WAN with Multiple Outgoing Calls

- The H.323 ALG operates on TCP packets with a port 1720 destination.
- The ZyWALL allows H.323 audio connections.
- The ZyWALL can also apply bandwidth management to traffic that goes through the H.323 ALG.

## 29.5 SIP

The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet. SIP is used in VoIP (Voice over IP), the sending of voice signals over the Internet Protocol.

SIP signaling is separate from the media for which it handles sessions. The media that is exchanged during the session can use a different path from that of the signaling. SIP handles telephone calls and can interface with traditional circuit-switched telephone networks.

### 29.5.1 STUN

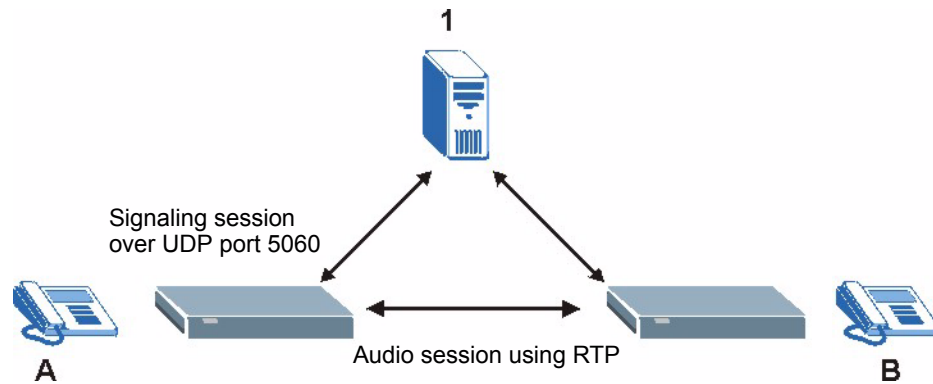
STUN (Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators) allows the VoIP device to find the presence and types of NAT routers and/or firewalls between it and the public Internet. STUN also allows the VoIP device to find the public IP address that NAT assigned, so the VoIP device can embed it in the SIP data stream. See RFC 3489 for details on STUN. You do not need to use STUN for devices behind the ZyWALL if you enable the SIP ALG.

### 29.5.2 SIP ALG Details

- SIP clients can be connected to the LAN, WLAN or DMZ. A SIP server must be on the WAN.
- You can make and receive calls between the LAN and the WAN, between the WLAN and the WAN and/or between the DMZ and the WAN. You cannot make a call between the LAN and the LAN, between the LAN and the DMZ, between the LAN and the WLAN, between the DMZ and the DMZ, and so on.
- The SIP ALG allows UDP packets with a port 5060 destination to pass through.
- The ZyWALL allows SIP audio connections.

The following example shows SIP signaling and audio sessions between SIP clients A and B and the SIP server (1).

**Figure 235** SIP ALG Example



### 29.5.3 SIP Signaling Session Timeout

Most SIP clients have an “expire” mechanism indicating the lifetime of signaling sessions. The SIP user agent sends registration packets to the SIP server periodically and keeps the session alive in the ZyWALL.

If the SIP client does not have this mechanism and makes no calls during the ZyWALL SIP timeout default (60 minutes), the ZyWALL SIP ALG drops any incoming calls after the timeout period.

### 29.5.4 SIP Audio Session Timeout

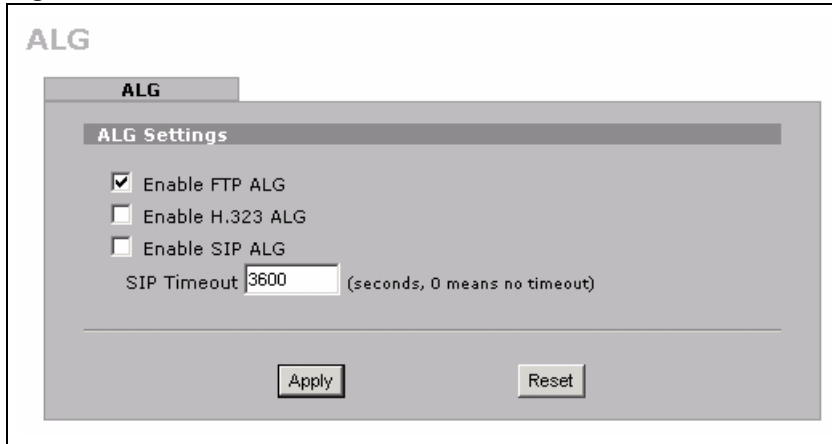
If no voice packets go through the SIP ALG before the timeout period (default 5 minutes) expires, the SIP ALG does not drop the call but blocks all voice traffic and deletes the audio session. You cannot hear anything and you will need to make a new call to continue your conversation.

## 29.6 ALG Screen

Click **ADVANCED, ALG** to open the **ALG** screen. Use the **ALG** screen to turn individual ALGs off or on and set the SIP timeout.

**Note:** If the ZyWALL provides an ALG for a service, you must enable the ALG in order to perform bandwidth management on that service's traffic.

**Figure 236** ALG



The following table describes the labels in this screen.

**Table 163** ALG

LABEL	DESCRIPTION
Enable FTP ALG	Select this check box to allow FTP sessions to pass through the ZyWALL. FTP (File Transfer Program) is a program that enables fast transfer of files, including large files that may not be possible by e-mail.
Enable H.323 ALG	Select this check box to allow H.323 sessions to pass through the ZyWALL. H.323 is a protocol used for audio communications over networks.
Enable SIP ALG	Select this check box to allow SIP sessions to pass through the ZyWALL. SIP is a signaling protocol used in VoIP (Voice over IP), the sending of voice signals over Internet Protocol.
SIP Timeout	Most SIP clients have an “expire” mechanism indicating the lifetime of signaling sessions. The SIP user agent sends registration packets to the SIP server periodically and keeps the session alive in the ZyWALL. If the SIP client does not have this mechanism and makes no calls during the ZyWALL SIP timeout (default 60 minutes), the ZyWALL SIP ALG drops any incoming calls after the timeout period. Enter the SIP signaling session timeout value.
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

# CHAPTER 30

## Logs Screens

This chapter contains information about configuring general log settings and viewing the ZyWALL's logs. Refer to [Appendix S on page 774](#) for example log message explanations.

### 30.1 Configuring View Log

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

Click **LOGS** to open the **View Log** screen. Use the **View Log** screen to see the logs for the categories that you selected in the **Log Settings** screen (see [Section 30.3 on page 475](#)). Options include logs about system maintenance, system errors, access control, allowed or blocked web sites, blocked web features (such as ActiveX controls, java and cookies), attacks (such as DoS) and IPSec.

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

**Figure 237** View Log

The screenshot shows the 'LOGS' section of the ZyWALL web interface. It includes tabs for 'View Log', 'Log Settings', and 'Reports'. Below the tabs, there is a 'Log Settings' section with a 'Display' dropdown set to 'All Logs' and buttons for 'Email Log Now', 'Refresh', and 'Clear Log'. The main part of the screen is a table of log entries.

#	Time ▲	Message	Source	Destination	Note
1	2005-07-26 01:19:16	The device has not been registered yet		203.160.254.59	myZyXEL.com
2	2005-07-26 01:19:16	Due to error code(3, 27), cert not trusted: SSL/TLS peer cer...			CERT MANAGER
3	2005-07-26 01:09:30	Time synchronization failed			
4	2005-07-26 01:09:30	Failed to sync with NTP server: ntp.cs.strath.ac.uk			
5	2005-07-26 01:09:30	Failed to sync with NTP server: ntp3.cs.wisc.edu			
6	2005-07-26 01:09:30	Failed to sync with NTP server: tock.usno.navy.mil			
17	2005-07-26 01:09:22	WAN interface gets IP:172.23.23.60			WAN1
18	2005-07-26 01:09:20	WAN connection is up.			WAN1
19	2005-07-26 01:09:18	Time set from NTP server: ntp1.sp.se, offset: -73 sec	193.10.7.250:123	172.23.23.60:1134	
20	2005-07-26 01:07:51	Successful HTTP login	192.168.1.33		User:admin
21	2005-07-26 01:05:57	Successful HTTP login	192.168.1.33		User:admin
22	2005-07-26 01:05:37	DHCP server assigns 192.168.1.33 to tw11 (00:00:E8:7C:14:80).			

The following table describes the labels in this screen.

**Table 164** View Log

LABEL	DESCRIPTION
Display	The categories that you select in the <b>Log Settings</b> page (see <a href="#">Section 30.3 on page 475</a> ) display in the drop-down list box. Select a category of logs to view; select <b>All Logs</b> to view logs from all of the log categories that you selected in the <b>Log Settings</b> page.
#	This field displays the log number.
Time	This field displays the time the log was recorded. See <a href="#">Section 31.4 on page 486</a> to configure the ZyWALL's time and date.
Message	This field states the reason for the log.
Source	This field lists the source IP address and the port number of the incoming packet.
Destination	This field lists the destination IP address and the port number of the incoming packet.
Note	This field displays additional information about the log entry.
Email Log Now	Click <b>Email Log Now</b> to send the log screen to the e-mail address specified in the <b>Log Settings</b> page (make sure that you have first filled in the <b>E-mail Log Settings</b> fields in <b>Log Settings</b> , see <a href="#">Section 30.3 on page 475</a> ).
Refresh	Click <b>Refresh</b> to renew the log screen.
Clear Log	Click <b>Clear Log</b> to delete all the logs.

## 30.2 Log Description Example

The following is an example of how a log displays in the command line interpreter and a description of the sample log. Refer to the appendices for more log message descriptions and details on using the command line interpreter to display logs.

```
# .time                source                destination
notes
message
5|06/08/2004 05:58:20 |172.21.4.187:137      |172.21.255.255:137
|ACCESS BLOCK
Firewall default policy: UDP (W to W/ZW)
```

**Table 165** Example Log Description

LABEL	DESCRIPTION
#	This is log number five.
time	The log was generated on June 8, 2004 at 5:58 and 20 seconds AM.
source	The log was generated due to a NetBIOS packet sent from IP address 172.21.4.187 port 137.
destination	The NetBIOS packet was sent to the 172.21.255.255 subnet port 137. This was a NetBIOS UDP broadcast packet meant to discover devices on the network.

**Table 165** Example Log Description

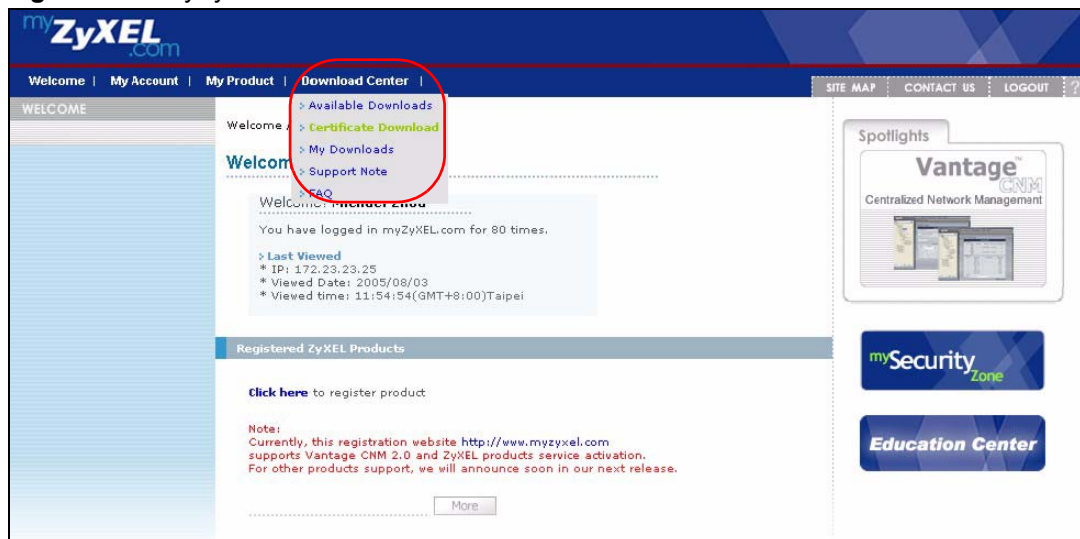
LABEL	DESCRIPTION
notes	The ZyWALL blocked the packet.
message	The ZyWALL blocked the packet in accordance with the firewall's default policy of blocking sessions that are initiated from the WAN. "UDP" means that this was a User Datagram Protocol packet. "W to W/ZW" indicates that the packet was traveling from the WAN to the WAN or the ZyWALL.

### 30.2.1 Certificate Not Trusted Log Note

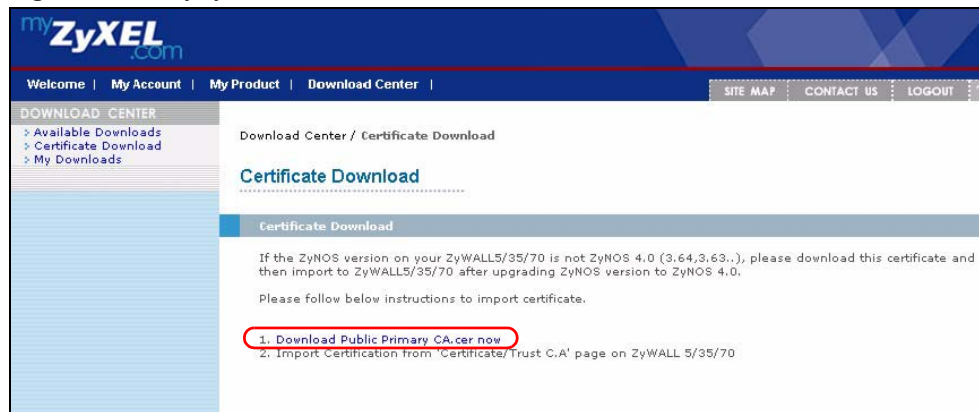
myZyXEL.com and the update server use certificate signed by VeriSign to identify themselves. If the ZyWALL does not have a CA certificate signed by VeriSign as a trusted CA, the ZyWALL will not trust the certificate from myZyXEL.com and the update server. The ZyWALL will generate a log like "Due to error code(11), cert not trusted: SSL/TLS peer certif..." for every time it attempt to establish a (HTTPS) connection with myZyXEL.com and the update server. The V4.00 default configuration file includes a trusted CA certificate signed by VeriSign. If you upgraded to ZyNOS V4.00 firmware without uploading the V4.00 default configuration file, you can download a CA certificate signed by VeriSign from myZyXEL.com and import it into the ZyWALL as a trusted CA. This will stop the ZyWALL from generating this log every time it attempts to connect with myzyxel.com and the update server.

Follow the steps below to download the certificate from myZyXEL.com.

- 1 Go to <http://www.myZyXEL.com> and log in with your account.
- 2 Click **Download Center** and then **Certificate Download**.

**Figure 238** myZyXEL.com: Download Center

- 3 Click the link in the **Certificate Download** screen.

**Figure 239** myZyXEL.com: Certificate Download

### 30.3 Configuring Log Settings

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

Use the **Log Settings** screen to configure to where the ZyWALL is to send logs; the schedule for when the ZyWALL is to send the logs and which logs and/or immediate alerts the ZyWALL is to send.

An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites or web sites with restricted web features such as cookies, active X and so on. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts display in red and logs display in black.

**Note:** Alerts are e-mailed as soon as they happen. Logs may be e-mailed as soon as the log is full (see **Log Schedule**). Selecting many alert and/or log categories (especially **Access Control**) may result in many e-mails being sent.

Figure 240 Log Settings

**LOGS**

**View Log   Log Settings   Reports**

---

**E-mail Log Settings**

Mail Server  (Outgoing SMTP Server Name or IP Address)

Mail Subject

Mail Sender  (E-Mail Address)

Send Log to  (E-Mail Address)

Send Alerts to  (E-Mail Address)

Log Schedule  (Dropdown)

Day for Sending Log  (Dropdown)

Time for Sending Log  (Hour)  (Minute)

SMTP Authentication

User Name

Password

---

**Syslog Logging**

Active

Syslog Server  (Server Name or IP Address)

Log Facility  (Dropdown)

---

**Active Log and Alert**

<p><b>Log</b></p> <p><input checked="" type="checkbox"/> System Maintenance</p> <p><input checked="" type="checkbox"/> System Errors</p> <p><input checked="" type="checkbox"/> Access Control</p> <p><input type="checkbox"/> Asymmetrical Routes</p> <p><input type="checkbox"/> Multicasts / Broadcasts</p> <p><input type="checkbox"/> TCP Reset</p> <p><input type="checkbox"/> Packet Filter</p> <p><input checked="" type="checkbox"/> ICMP</p> <p><input checked="" type="checkbox"/> Remote Management</p> <p><input checked="" type="checkbox"/> Call Record</p> <p><input checked="" type="checkbox"/> PPP</p> <p><input type="checkbox"/> UPnP</p> <p><input type="checkbox"/> Forward Web Sites</p> <p><input checked="" type="checkbox"/> Blocked Web Sites</p> <p><input checked="" type="checkbox"/> Blocked Java etc.</p> <p><input checked="" type="checkbox"/> Attacks</p> <p><input checked="" type="checkbox"/> IPSec</p> <p><input checked="" type="checkbox"/> IKE</p> <p><input checked="" type="checkbox"/> PKI</p> <p><input checked="" type="checkbox"/> SSL/TLS</p> <p><input checked="" type="checkbox"/> 802.1X</p> <p><input checked="" type="checkbox"/> Wireless</p> <p><input checked="" type="checkbox"/> IDP</p> <p><input checked="" type="checkbox"/> Anti-Virus</p> <p><input checked="" type="checkbox"/> Anti-Spam</p>	<p><b>Send Immediate Alert</b></p> <p><input type="checkbox"/> System Errors</p> <p><input type="checkbox"/> Access Control</p> <p><input type="checkbox"/> Blocked Web Sites</p> <p><input type="checkbox"/> Blocked Java etc.</p> <p><input type="checkbox"/> Attacks</p> <p><input type="checkbox"/> IPSec</p> <p><input type="checkbox"/> IKE</p> <p><input type="checkbox"/> PKI</p> <p><input type="checkbox"/> IDP</p> <p><input type="checkbox"/> Anti-Virus</p>
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

---

**Log Consolidation**

Active

Log Consolidation Period  1 ~ 600 (Seconds)



The following table describes the labels in this screen.

**Table 166** Log Settings

LABEL	DESCRIPTION
E-mail Log Settings	
Mail Server	Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages will not be sent via e-mail.
Mail Subject	Type a title that you want to be in the subject line of the log e-mail message that the ZyWALL sends.
Mail Sender	Enter the e-mail address that you want to be in the from/sender line of the log e-mail message that the ZyWALL sends. If you activate SMTP authentication, the e-mail address must be able to be authenticated by the mail server as well.
Send Log To	Logs are sent to the e-mail address specified in this field. If this field is left blank, logs will not be sent via e-mail.
Send Alerts To	Alerts are sent to the e-mail address specified in this field. If this field is left blank, alerts will not be sent via e-mail.
Log Schedule	<p>This drop-down menu is used to configure the frequency of log messages being sent as E-mail:</p> <ul style="list-style-type: none"> <li>• <b>Daily</b></li> <li>• <b>Weekly</b></li> <li>• <b>Hourly</b></li> <li>• <b>When Log is Full</b></li> <li>• <b>None.</b></li> </ul> <p>If you select <b>Weekly</b> or <b>Daily</b>, specify a time of day when the E-mail should be sent. If you select <b>Weekly</b>, then also specify which day of the week the E-mail should be sent. If you select <b>When Log is Full</b>, an alert is sent when the log fills up. If you select <b>None</b>, no log messages are sent.</p>
Day for Sending Log	Use the drop down list box to select which day of the week to send the logs.
Time for Sending Log	Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs.
SMTP Authentication	<p>SMTP (Simple Mail Transfer Protocol) is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.</p> <p>Select the check box to activate SMTP authentication. If mail server authentication is needed but this feature is disabled, you will not receive the e-mail logs.</p>
User Name	Enter the user name (up to 31 characters) (usually the user name of a mail account).
Password	Enter the password associated with the user name above.
Syslog Logging	Syslog logging sends a log to an external syslog server used to store logs.
Active	Click <b>Active</b> to enable syslog logging.
Syslog Server	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
Log Facility	Select a location from the drop down list box. The log facility allows you to log the messages to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Active Log and Alert	
Log	Select the categories of logs that you want to record. Logs include alerts.

**Table 166** Log Settings (continued)

LABEL	DESCRIPTION
Send Immediate Alert	Select the categories of alerts for which you want the ZyWALL to instantly e-mail alerts to the e-mail address specified in the <b>Send Alerts To</b> field.
Log Consolidation	
Active	Some logs (such as the Attacks logs) may be so numerous that it becomes easy to ignore other important log messages. Select this check box to merge logs with identical messages into one log. You can use the <code>sys log consolidate msglist</code> command to see what log messages will be consolidated.
Log Consolidation Period	Specify the time interval during which the ZyWALL merges logs with identical messages into one log.
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 30.4 Configuring Reports

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

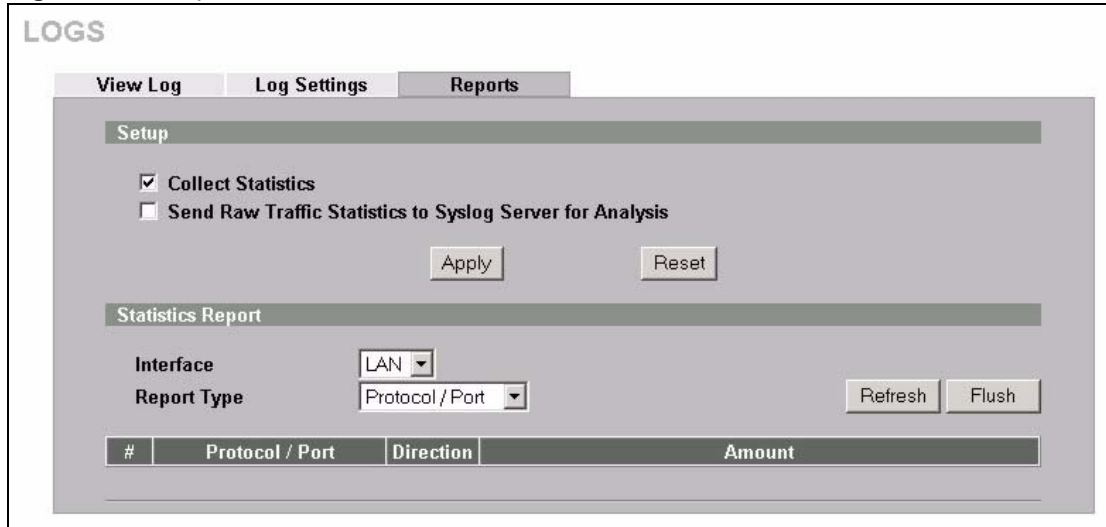
- Web sites visited the most often
- Number of times the most visited web sites were visited
- The most-used protocols or service ports
- The amount of traffic for the most used protocols or service ports
- The LAN IP addresses to and/or from which the most traffic has been sent
- How much traffic has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

**Note:** The web site hit count may not be 100% accurate because sometimes when an individual web page loads, it may contain references to other web sites that also get counted as hits.

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

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

**Figure 241** Reports



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

The following table describes the labels in this screen.

**Table 167** Reports

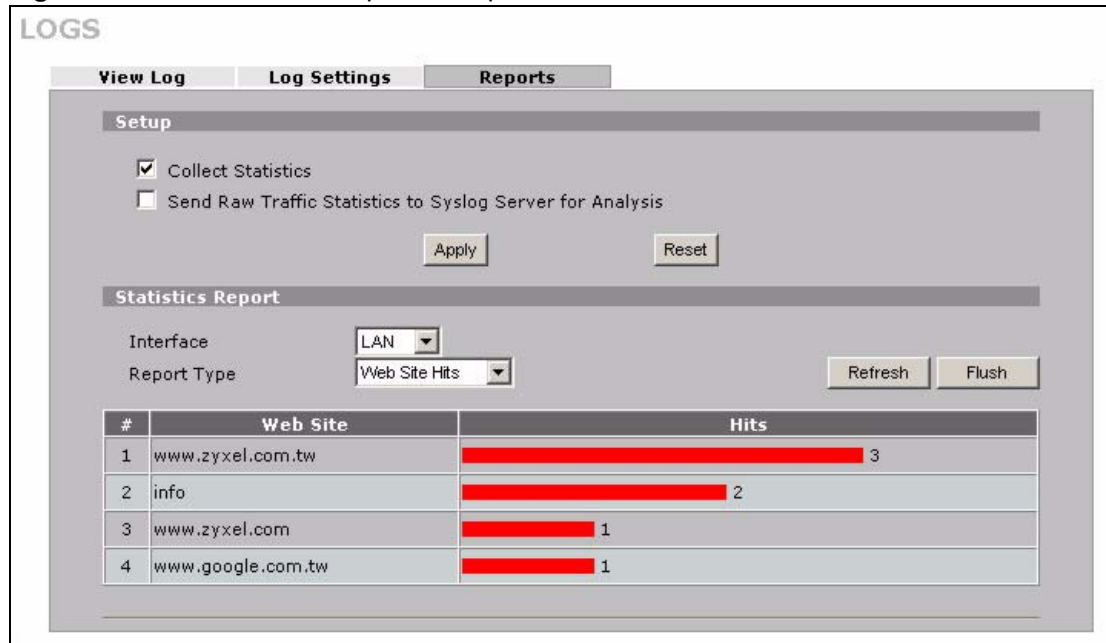
LABEL	DESCRIPTION
Collect Statistics	Select the check box and click <b>Apply</b> to have the ZyWALL record report data.
Send Raw Traffic Statistics to Syslog Server for Analysis	Select the check box and click <b>Apply</b> to have the ZyWALL send unprocessed traffic statistics to a syslog server for analysis. You must have the syslog server already configured in the <b>Log Settings</b> screen.
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.
Interface	Select on which interface ( <b>LAN</b> , <b>DMZ</b> or <b>WLAN</b> ) the logs will be collected. The logs on the DMZ, LAN or WLAN IP alias 1 and 2 are also recorded.
Report Type	Use the drop-down list box to select the type of reports to display. <b>Web Site Hits</b> displays the web sites that have been visited the most often from the LAN and how many times they have been visited. <b>Protocol/Port</b> displays the protocols or service ports that have been used the most and the amount of traffic for the most used protocols or service ports. <b>Host IP Address</b> displays the LAN, DMZ or WLAN IP addresses to and /or from which the most traffic has been sent and how much traffic has been sent to and from those IP addresses.
Refresh	Click <b>Refresh</b> to update the report display. The report also refreshes automatically when you close and reopen the screen.
Flush	Click <b>Flush</b> to discard the old report data and update the report display.

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

### 30.4.1 Viewing Web Site Hits

In the **Reports** screen, select **Web Site Hits** from the **Report Type** drop-down list box to have the ZyWALL record and display which web sites have been visited the most often and how many times they have been visited.

**Figure 242** Web Site Hits Report Example



The following table describes the label in this screen.

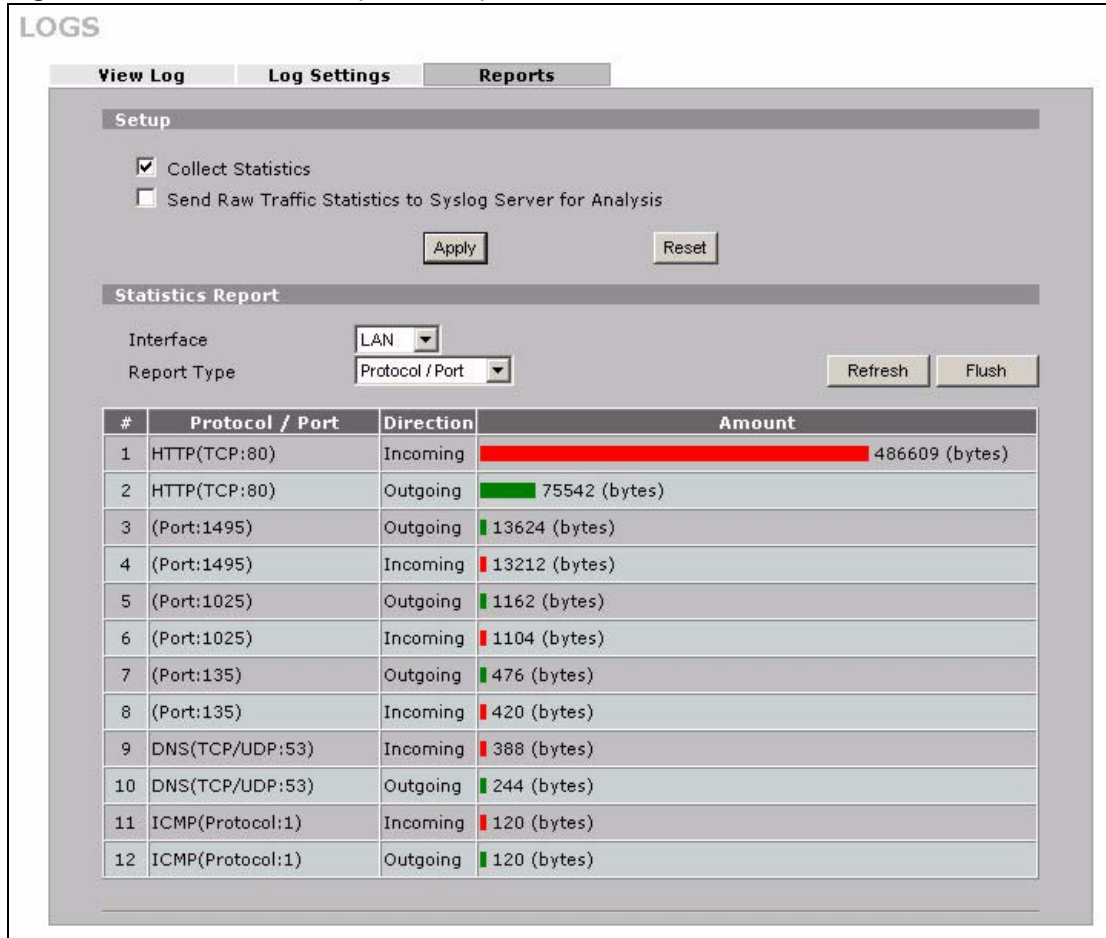
**Table 168** Web Site Hits Report

LABEL	DESCRIPTION
Web Site	This column lists the domain names of the web sites visited most often from computers on the LAN, DMZ or WLAN. The names are ranked by the number of visits to each web site and listed in descending order with the most visited web site listed first. The ZyWALL counts each page viewed in a web site as another hit on the web site.
Hits	This column lists how many times each web site has been visited. The count starts over at 0 if a web site passes the hit count limit (see <a href="#">Table 171 on page 483</a> ).

### 30.4.2 Viewing Protocol/Port

In the **Reports** screen, select **Protocol/Port** from the **Report Type** drop-down list box to have the ZyWALL record and display which protocols or service ports have been used the most and the amount of traffic for the most used protocols or service ports.

**Figure 243** Protocol/Port Report Example



The following table describes the labels in this screen.

**Table 169** Protocol/ Port Report

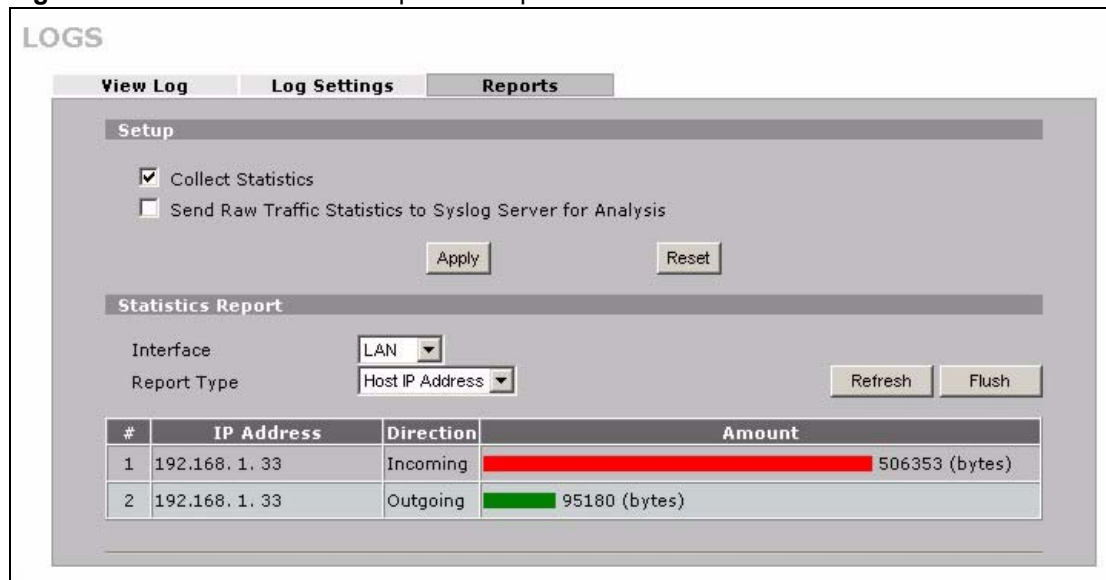
LABEL	DESCRIPTION
Protocol/Port	This column lists the protocols or service ports for which the most traffic has gone through the ZyWALL. The protocols or service ports are listed in descending order with the most used protocol or service port listed first.
Direction	This field displays <b>Incoming</b> to denote traffic that is coming in from the WAN to the LAN, DMZ or WLAN. This field displays <b>Outgoing</b> to denote traffic that is going out from the LAN, DMZ or WLAN to the WAN.
Amount	This column lists how much traffic has been sent and/or received for each protocol or service port. The measurement unit shown (bytes, Kbytes, Mbytes or Gbytes) varies with the amount of traffic for the particular protocol or service port. The count starts over at 0 if a protocol or port passes the bytes count limit (see <a href="#">Table 171 on page 483</a> ).

### 30.4.3 Viewing Host IP Address

In the **Reports** screen, select **Host IP Address** from the **Report Type** drop-down list box to have the ZyWALL record and display the LAN, DMZ or WLAN IP addresses that the most traffic has been sent to and/or from and how much traffic has been sent to and/or from those IP addresses.

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

**Figure 244** Host IP Address Report Example



The following table describes the labels in this screen.

**Table 170** Host IP Address Report

LABEL	DESCRIPTION
IP Address	This column lists the LAN, DMZ or WLAN IP addresses to and/or from which the most traffic has been sent. The LAN, DMZ or WLAN IP addresses are listed in descending order with the LAN, DMZ or WLAN IP address to and/or from which the most traffic was sent listed first.
Direction	This field displays <b>Incoming</b> to denote traffic that is coming in from the WAN to the LAN, DMZ or WLAN. This field displays <b>Outgoing</b> to denote traffic that is going out from the LAN, DMZ or WLAN to the WAN.
Amount	This column displays how much traffic has gone to and from the listed LAN, DMZ or WLAN IP addresses. The measurement unit shown (bytes, Kbytes, Mbytes or Gbytes) varies with the amount of traffic sent to and from the LAN, DMZ or WLAN IP address. The count starts over at 0 if the total traffic sent to and from a LAN, DMZ or WLAN IP passes the bytes count limit (see <a href="#">Table 171 on page 483</a> ).

### 30.4.4 Reports Specifications

The following table lists detailed specifications on the reports feature.

**Table 171** Report Specifications

LABEL	DESCRIPTION
Number of web sites/protocols or ports/IP addresses listed:	20
Hit count limit:	Up to $2^{32}$ hits can be counted per web site. The count starts over at 0 if it passes four billion.
Bytes count limit:	Up to $2^{64}$ bytes can be counted per protocol/port or LAN IP address. The count starts over at 0 if it passes $2^{64}$ bytes.

# CHAPTER 31

## Maintenance

This chapter displays information on the maintenance screens.

### 31.1 Maintenance Overview

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

### 31.2 General Setup

#### 31.2.1 General Setup and System Name

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

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

#### 31.2.2 General Setup

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

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



**Figure 245** General Setup

The following table describes the labels in this screen.

**Table 172** General Setup

LABEL	DESCRIPTION
General Setup	
System Name	Choose a descriptive name for identification purposes. It is recommended you enter your computer's "Computer name" in this field. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. The domain name entered by you is given priority over the ISP assigned domain name.
Administrator Inactivity Timer	Type how many minutes a management session (either via the web configurator or SMT) can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

### 31.3 Configuring Password

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

**Figure 246** Password Setup

The screenshot shows the 'MAINTENANCE' section with the 'Password' tab selected. The 'Password Setup' sub-section contains three text input fields labeled 'Old Password', 'New Password', and 'Retype to Confirm'. Below these fields are two buttons: 'Apply' and 'Reset'.

The following table describes the labels in this screen.

**Table 173** Password Setup

LABEL	DESCRIPTION
Old Password	Type the default password or the existing password you use to access the system in this field.
New Password	Type your new system password (up to 30 characters). Note that as you type a password, the screen displays a (*) for each character you type.
Retype to Confirm	Type the new password again for confirmation.
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 31.4 Time and Date

The ZyWALL's Real Time Chip (RTC) keeps track of the time and date. There is also a software mechanism to set the time manually or get the current time and date from an external server when you turn on your ZyWALL.

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

**Figure 247** Time and Date

The following table describes the labels in this screen.

**Table 174** Time and Date

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the ZyWALL's present time.
Current Date	This field displays the ZyWALL's present date.
Time and Date Setup	
Manual	Select this radio button to enter the time and date manually. If you configure a new time and date, Time Zone and Daylight Saving at the same time, the new time and date you entered has priority and the Time Zone and Daylight Saving settings do not affect it.
New Time (hh:mm:ss)	This field displays the last updated time from the time server or the last time configured manually. When you set <b>Time and Date Setup</b> to <b>Manual</b> , enter the new time in this field and then click <b>Apply</b> .
New Date (yyyy-mm-dd)	This field displays the last updated date from the time server or the last date configured manually. When you set <b>Time and Date Setup</b> to <b>Manual</b> , enter the new date in this field and then click <b>Apply</b> .

**Table 174** Time and Date (continued)

LABEL	DESCRIPTION
Get from Time Server	Select this radio button to have the ZyWALL get the time and date from the time server you specified below.
Time Protocol	<p>Select the time service protocol that your time server uses. 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.</p> <p>The main difference between them is the format.  <b>Daytime (RFC 867)</b> format is day/month/year/time zone of the server.  <b>Time (RFC 868)</b> format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0.  The default, <b>NTP (RFC 1305)</b>, is similar to <b>Time (RFC 868)</b>.</p>
Time Server Address	Enter the IP address or URL of your time server. Check with your ISP/network administrator if you are unsure of this information.
Synchronize Now	Click this button to have the ZyWALL get the time and date from a time server (see the <b>Time Server Address</b> field). This also saves your changes (including the time server address).
Time Zone Setup	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Enable Daylight Saving	<p>Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.</p> <p>Select this option if you use Daylight Saving Time.</p>
Start Date	<p>Configure the day and time when Daylight Saving Time starts if you selected <b>Enable Daylight Saving</b>. The <b>o'clock</b> field uses the 24 hour format. Here are a couple of examples:</p> <p>Daylight Saving Time starts in most parts of the United States on the first Sunday of April. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select <b>First, Sunday, April</b> and type 2 in the <b>o'clock</b> field.</p> <p>Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select <b>Last, Sunday, March</b>. The time you type in the <b>o'clock</b> field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).</p>
End Date	<p>Configure the day and time when Daylight Saving Time ends if you selected <b>Enable Daylight Saving</b>. The <b>o'clock</b> field uses the 24 hour format. Here are a couple of examples:</p> <p>Daylight Saving Time ends in the United States on the last Sunday of October. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select <b>Last, Sunday, October</b> and type 2 in the <b>o'clock</b> field.</p> <p>Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select <b>Last, Sunday, October</b>. The time you type in the <b>o'clock</b> field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).</p>
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 31.5 Pre-defined NTP Time Servers List

When you turn on the ZyWALL for the first time, the date and time start at 2000-01-01 00:00:00. The ZyWALL then attempts to synchronize with one of the following pre-defined list of NTP time servers.

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

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

**Table 175** Default Time Servers

ntp1.cs.wisc.edu
ntp1.gbg.netnod.se
ntp2.cs.wisc.edu
tock.usno.navy.mil
ntp3.cs.wisc.edu
ntp.cs.strath.ac.uk
ntp1.sp.se
time1.stupi.se
tick.stdtime.gov.tw
tock.stdtime.gov.tw
time.stdtime.gov.tw

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

### 31.5.1 Resetting the Time

The ZyWALL resets the time in the following instances:

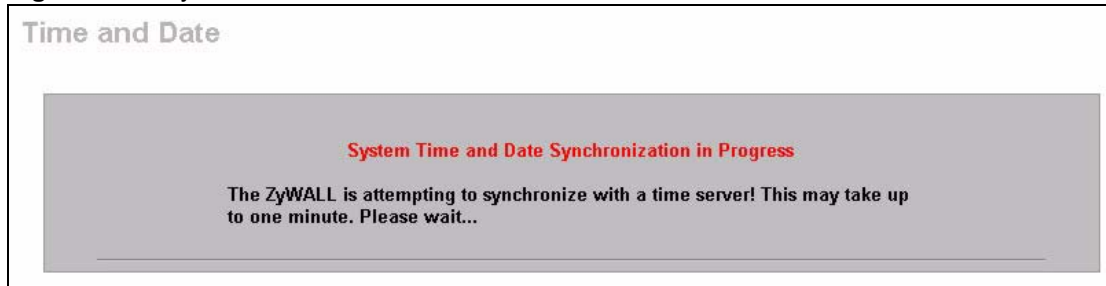
- When you click **Synchronize Now**.
- On saving your changes.
- When the ZyWALL starts up.
- 24-hour intervals after starting.

### 31.5.2 Time Server Synchronization

Click the **Synchronize Now** button to get the time and date from the predefined time server or the time server you specified in the **Time Server Address** field.

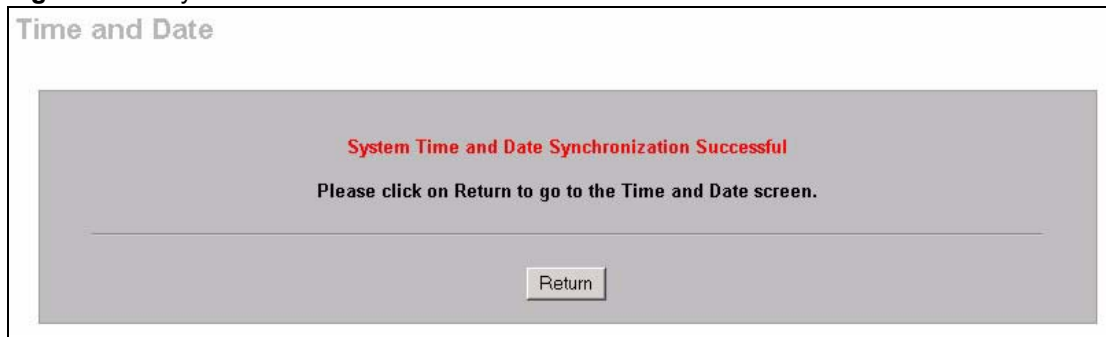
When the **System Time and Date Synchronization in Process** screen appears, wait up to one minute.

**Figure 248** Synchronization in Process



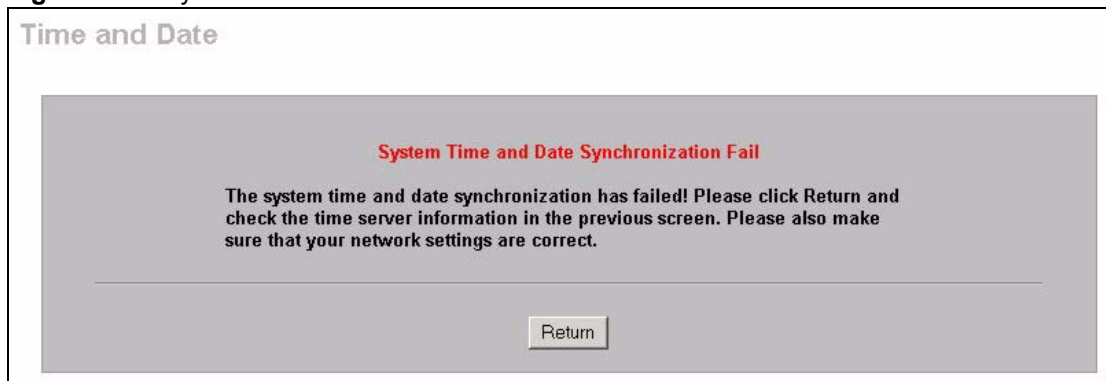
Click the **Return** button to go back to the **Time and Date** screen after the time and date is updated successfully.

**Figure 249** Synchronization is Successful



If the update was not successful, the following screen appears. Click **Return** to go back to the **Time and Date** screen.

**Figure 250** Synchronization Fail



## 31.6 Introduction To Transparent Bridging

A transparent bridge is invisible to the operation of a network in that it does not modify the frames it forwards. The bridge checks the source address of incoming frames on the port and learns MAC addresses to associate with that port. All future communications to that MAC address will only be sent on that port.

The bridge gradually builds a host MAC-address-to-port mapping table such as in the following example, during the learning process.

**Table 176** MAC-address-to-port Mapping Table

HOST MAC ADDRESS	PORT
00a0c5123456	3
00a0c5123478 (host A)	1
00a0c512349a	3
00a0c51234bc	2
00a0c51234de	4

For example, if a bridge receives a frame via port 1 from host A (MAC address 00a0c5123478), the bridge associates host A with port 1. When the bridge receives another frame on one of its ports with destination address 00a0c5123478, it forwards the frame directly through port 1 after checking the internal table.

The bridge takes one of these actions after it checks the destination address of an incoming frame with its internal table:

- If the table contains an association between the destination address and any of the bridge's ports aside from the one on which the frame was received, the frame is forwarded out the associated port.
- If no association is found, the frame is flooded to all ports except the inbound port. Broadcasts and multicasts also are flooded in this way.
- If the associated port is the same as the incoming port, then the frame is dropped (filtered).

## 31.7 Transparent Firewalls

A transparent firewall (also known as a transparent, in-line, shadow, stealth or bridging firewall) has the following advantages over “router firewalls”:

- 1** The use of a bridging firewall reduces configuration and deployment time because no networking configuration changes to your existing network (hosts, neighboring routers and the firewall itself) are needed. Just put it in-line with the network it is protecting. As it only moves frames between ports (after inspecting them), it is completely transparent.
- 2** Performance is improved as there's less processing overhead.

- 3 As a transparent bridge does not modify the frames it forwards, it is effectively “stealth” as it is invisible to attackers.

Bridging devices are most useful in complex environments that require a rapid or new firewall deployment. A transparent, bridging firewall can also be good for companies with several branch offices since the setups at these offices are often the same and it's likely that one design can be used for many of the networks. A bridging firewall could be configured at HQ, sent to the branches and then installed directly without additional configuration.

## 31.8 Configuring Device Mode (Router)

To configure and have your ZyWALL work as a router or a bridge, click **MAINTENANCE**, then the **Device Mode** tab. The following applies when the ZyWALL is in router mode.

**Figure 251** Device Mode (Router Mode)

The screenshot shows the 'MAINTENANCE' page with the 'Device Mode' tab selected. The 'Current Device Mode' section shows 'Device Mode' set to 'Router'. The 'Device Mode Setup' section includes a note: 'The ZyWALL restarts automatically after you change the device mode and click "Apply".' There are two radio buttons: 'Router' (unselected) and 'Bridge' (selected). Below the 'Bridge' radio button, there are three input fields: 'IP Address' with the value '192 . 168 . 1 . 1', 'IP Subnet Mask' with the value '255 . 255 . 255 . 0', and 'Gateway IP Address' with the value '0 . 0 . 0 . 0'. At the bottom of the form are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

**Table 177** Device Mode (Router Mode)

LABEL	DESCRIPTION
Current Device Mode	
Device Mode	This displays whether the ZyWALL is functioning as a router or a bridge.
Device Mode Setup	
Router	When the ZyWALL is in router mode, there is no need to select or clear this radio button.
IP Address	Click <b>LAN</b> , <b>WAN</b> , <b>DMZ</b> or <b>WLAN</b> to go to the <b>LAN</b> , <b>WAN</b> , <b>DMZ</b> or <b>WLAN</b> screen where you can view and/or change the corresponding settings.



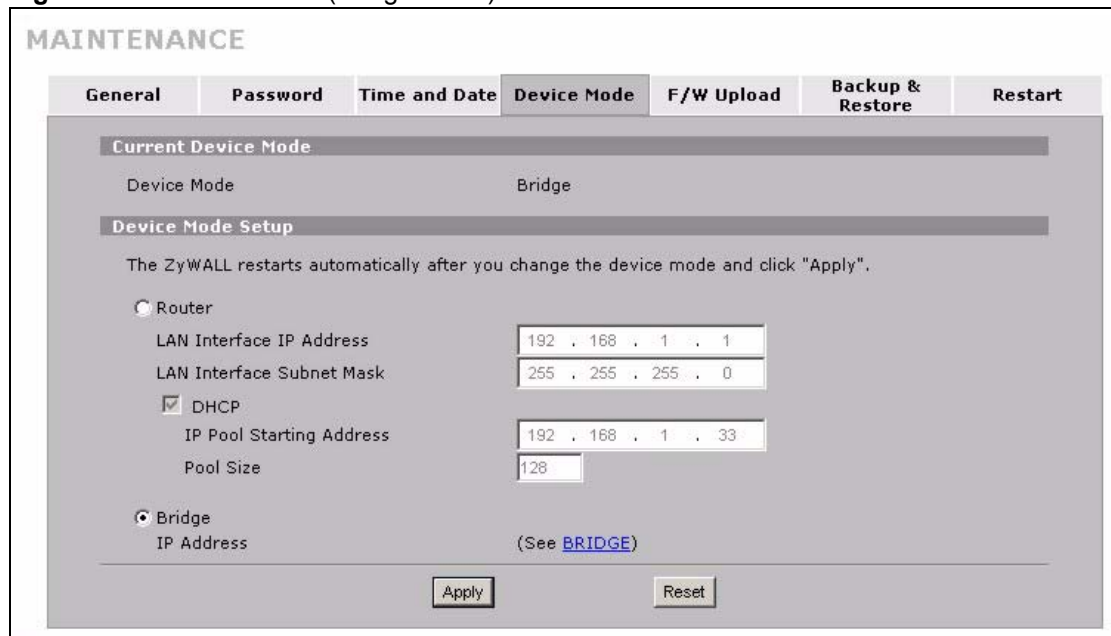
**Table 177** Device Mode (Router Mode) (continued)

LABEL	DESCRIPTION
Bridge	Select this radio button and configure the following fields, then click <b>Apply</b> to set the ZyWALL to bridge mode.
IP Address	Enter the IP address of your ZyWALL in dotted decimal notation.
IP Subnet Mask	Enter the IP subnet mask of the ZyWALL.
Gateway IP Address	Enter the gateway IP address.
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL. After you click <b>Apply</b> , please wait for one minute and use the IP address you configured in the <b>IP Address</b> field to access the ZyWALL again.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

### 31.9 Configuring Device Mode (Bridge)

To configure and have your ZyWALL work as a router or a bridge, click **MAINTENANCE**, then the **Device Mode** tab. The following applies when the ZyWALL is in bridge mode.

**Figure 252** Device Mode (Bridge Mode)



The following table describes the labels in this screen.

**Table 178** Device Mode (Bridge Mode)

LABEL	DESCRIPTION
Current Device Mode	
Device Mode	This displays whether the ZyWALL is functioning as a router or a bridge.

**Table 178** Device Mode (Bridge Mode) (continued)

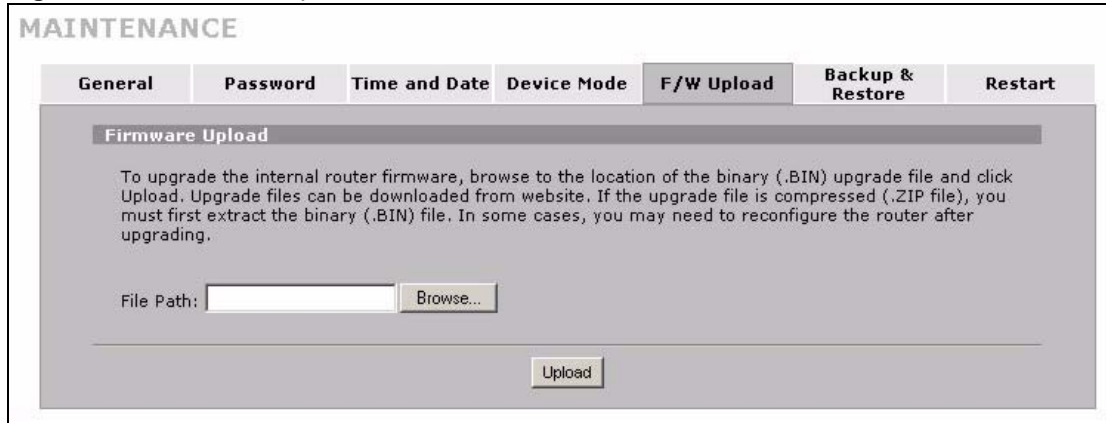
LABEL	DESCRIPTION
Device Mode Setup	
Router	Select this radio button and click <b>Apply</b> to set the ZyWALL to router mode.
LAN Interface IP Address	Enter the IP address of your ZyWALL' s LAN port in dotted decimal notation. 192.168.1.1 is the factory default.
LAN Interface Subnet Mask	Enter the IP subnet mask of the ZyWALL's LAN port.
DHCP	DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (computers) to obtain TCP/IP configuration at startup from a server. Unless you are instructed by your ISP, leave the <b>DHCP</b> check box selected. Clear it to stop the ZyWALL from acting as a DHCP server. When configured as a server, the ZyWALL provides TCP/IP configuration for the clients. If not, DHCP service is disabled and you must have another DHCP server on your LAN, or else the computers must be manually configured. When set as a server, fill in the rest of the DHCP setup fields.
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Pool Size	This field specifies the size, or count of the IP address pool.
Bridge	When the ZyWALL is in bridge mode, there is no need to select or clear this radio button.
IP Address	Click <b>Bridge</b> to go to the <b>Bridge</b> screen where you can view and/or change the bridge settings.
Apply	Click <b>Apply</b> to save your changes back to the ZyWALL. After you click <b>Apply</b> , please wait for one minute and use the IP address you configured in the <b>LAN Interface IP Address</b> field to access the ZyWALL again.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 31.10 F/W Upload Screen

Find firmware at [www.zyxel.com](http://www.zyxel.com) in a file that (usually) uses the system model name with a .bin extension, for example, "zywall.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot. See [Section 47.5 on page 621](#) for upgrading firmware using FTP/TFTP commands.

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

**Figure 253** Firmware Upload



The following table describes the labels in this screen.

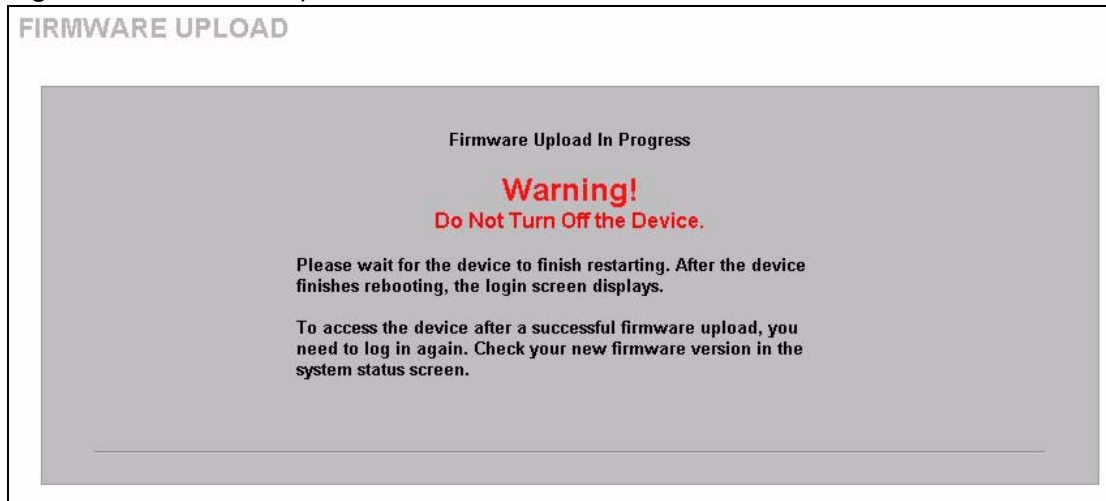
**Table 179** Firmware Upload

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

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

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

**Figure 254** Firmware Upload In Process



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

**Figure 255** Network Temporarily Disconnected

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

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

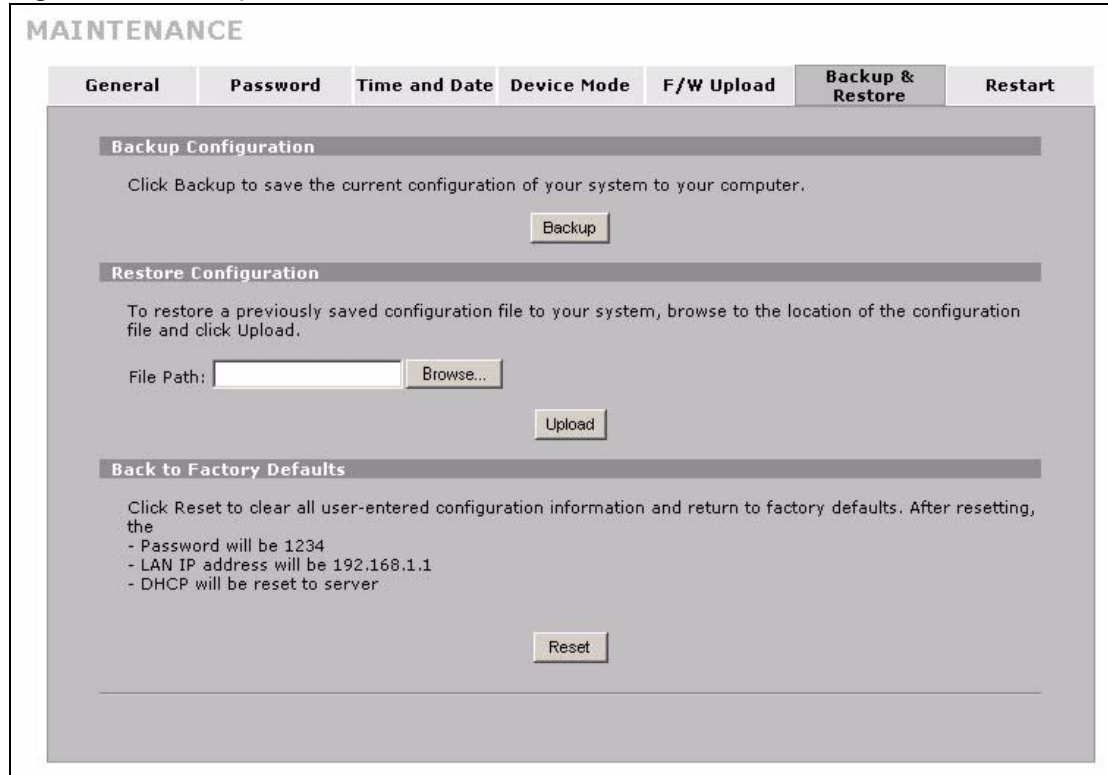
**Figure 256** Firmware Upload Error

## 31.11 Backup and Restore

See [Section 47.5 on page 621](#) for transferring configuration files using FTP/TFTP commands.

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

**Figure 257** Backup and Restore



### 31.11.1 Backup Configuration

Backup Configuration allows you to back up (save) the ZyWALL's current configuration to a file on your computer. Once your ZyWALL is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the ZyWALL's current configuration to your computer.

### 31.11.2 Restore Configuration

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

**Table 180** Restore Configuration

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

**Note:** Do not turn off the ZyWALL while configuration file upload is in progress.

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

**Figure 258** Configuration Upload Successful



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

**Figure 259** Network Temporarily Disconnected



If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.1). See your Quick Start Guide for details on how to set up your computer's IP address.

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

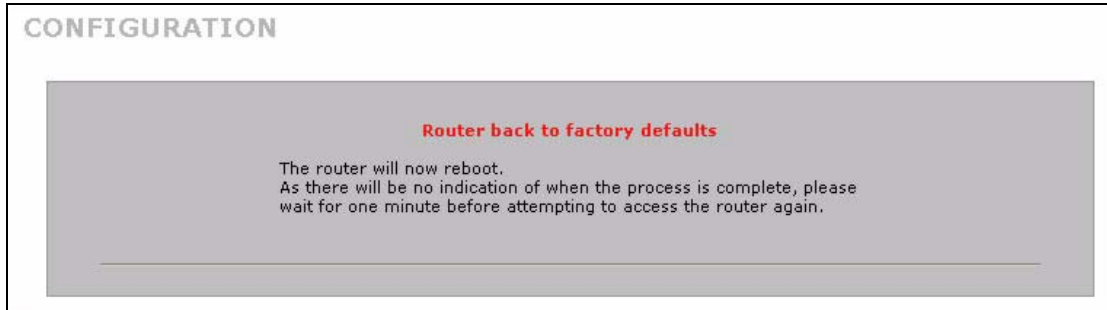
**Figure 260** Configuration Upload Error



### 31.11.3 Back to Factory Defaults

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

**Figure 261** Reset Warning Message



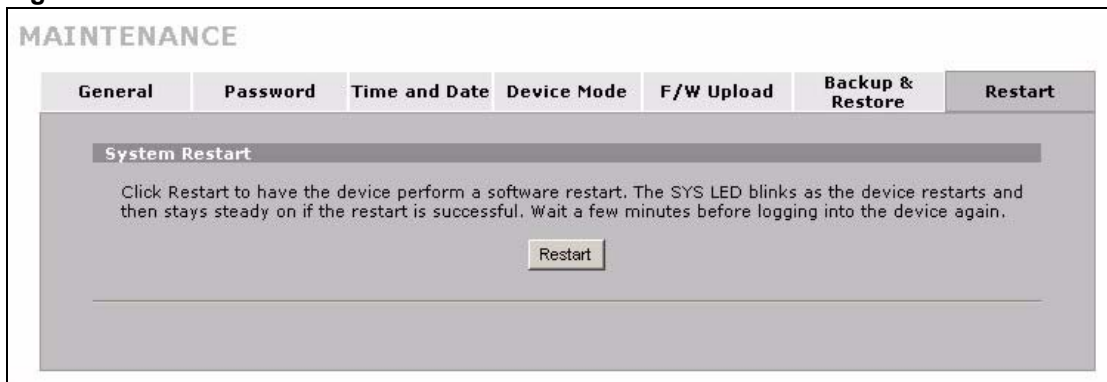
You can also press the **RESET** button on the rear panel to reset the factory defaults of your ZyWALL. Refer to [Section 2.3 on page 67](#) for more information on the **RESET** button.

### 31.12 Restart Screen

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

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

**Figure 262** Restart Screen



# CHAPTER 32

## Introducing the SMT

This chapter explains how to access the System Management Terminal and gives an overview of its menus.

### 32.1 Introduction to the SMT

The ZyWALL's SMT (System Management Terminal) is a menu-driven interface that you can access from a terminal emulator through the console port or over a telnet connection. This chapter shows you how to access the SMT (System Management Terminal) menus via console port, how to navigate the SMT and how to configure SMT menus.

### 32.2 Accessing the SMT via the Console Port

Make sure you have the physical connection properly set up as described in the Quick Start Guide.

When configuring using the console port, you need a computer equipped with communications software configured to the following parameters:

- VT100 terminal emulation.
- 9600 Baud.
- No parity, 8 data bits, 1 stop bit, flow control set to none.

#### 32.2.1 Initial Screen

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

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



**Figure 263** Initial Screen

```

Copyright (c) 1994 - 2004 ZyXEL Communications Corp.

initialize ch =0, ethernet address: 00:A0:C5:01:23:45
initialize ch =1, ethernet address: 00:A0:C5:01:23:46
initialize ch =2, ethernet address: 00:A0:C5:01:23:47
initialize ch =3, ethernet address: 00:A0:C5:01:23:48
initialize ch =4, ethernet address: 00:00:00:00:00:00
AUX port init . done
Modem init . inactive

Press ENTER to continue...

```

## 32.2.2 Entering the Password

The login screen appears after you press [ENTER], prompting you to enter the password, as shown below.

For your first login, enter the default password “1234”. As you type the password, the screen displays an “X” for each character you type.

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

**Figure 264** Password Screen

```

Enter Password : XXXX

```

## 32.3 Navigating the SMT Interface

The SMT is an interface that you use to configure your ZyWALL.

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

**Table 181** Main Menu Commands

OPERATION	KEYSTROKES	DESCRIPTION
Move down to another menu	[ENTER]	To move forward to a submenu, type in the number of the desired submenu and press [ENTER].
Move up to a previous menu	[ESC]	Press the [ESC] key to move back to the previous menu.

**Table 181** Main Menu Commands

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

### 32.3.1 Main Menu

After you enter the password, the SMT displays the **ZyWALL Main Menu**, as shown next. This guide uses the ZyWALL 70 menus as an example. The menus may vary slightly for different ZyWALL models. Not all fields or menus are available on all models.

**Figure 265** Main Menu (Router Mode)

```

Copyright (c) 1994 - 2005 ZyXEL Communications Corp.

ZyWALL 70 Main Menu

Getting Started
  1. General Setup
  2. WAN Setup
  3. LAN Setup
  4. Internet Access Setup
  5. DMZ Setup
  6. Route Setup
  7. Wireless 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
  25. IP Routing Policy Setup
  26. Schedule Setup

99. Exit

Enter Menu Selection Number:
    
```

**Figure 266** Main Menu (Bridge Mode)

```

Copyright (c) 1994 - 2005 ZyXEL Communications Corp.

ZyWALL 70 Main Menu

Getting Started
  1. General Setup

7. Wireless Setup

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

99. Exit

Enter Menu Selection Number:
    
```

The following table describes the fields in this menu.

**Table 182** Main Menu Summary

NO.	MENU TITLE	FUNCTION
1	General Setup	Use this menu to set up device mode, dynamic DNS and administrative information.
2	WAN Setup	Use this menu to clone a MAC address from a computer on your LAN and configure the backup WAN dial-up connection.

**Table 182** Main Menu Summary

NO.	MENU TITLE	FUNCTION
3	LAN Setup	Use this menu to apply LAN filters, configure LAN DHCP and TCP/IP settings.
4	Internet Access Setup	Configure your Internet access setup (Internet address, gateway, login, etc.) with this menu.
5	DMZ Setup	Use this menu to apply DMZ filters, and configure DHCP and TCP/IP settings for the DMZ port.
6	Route Setup	This menu is not available on the ZyWALL 5. Use this menu to configure your WAN route assessment, traffic redirect properties and failover parameters.
7	Wireless Setup	Use this menu to configure wireless security, WLAN DHCP and TCP/IP settings for the wireless LAN interface.
11	Remote Node Setup	Use this menu to configure detailed remote node settings (your ISP is also a remote node) as well as apply WAN filters.
12	Static Routing Setup	Configure IP static routes in this menu.
15	NAT Setup	Use this menu to configure Network Address Translation.
21	Filter and Firewall Setup	Configure filters and activate/deactivate the firewall.
22	SNMP Configuration	Use this menu to configure SNMP-related parameters.
23	System Password	Change your password in this menu (recommended).
24	System Maintenance	From displaying system status to uploading firmware, this menu provides comprehensive system maintenance.
25	IP Routing Policy Setup	This menu is not available on the ZyWALL 5. 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).

### 32.3.2 SMT Menus Overview

The following table gives you an overview of your ZyWALL's various SMT menus.

**Table 183** SMT Menus Overview

MENUS	SUB MENUS		
1 General Setup	1.1 Configure Dynamic DNS	1.1.1 DDNS Host Summary	1.1.1 DDNS Edit Host
2 WAN Setup	2.1 Advanced WAN Setup		
3 LAN Setup	3.1 LAN Port Filter Setup		
	3.2 TCP/IP and DHCP Ethernet Setup	3.2.1 IP Alias Setup	
4 Internet Access Setup			
5 DMZ Setup	5.1 DMZ Port Filter Setup		
	5.2 TCP/IP and DHCP Ethernet Setup	5.2.1 IP Alias Setup	

**Table 183** SMT Menus Overview (continued)

MENUS	SUB MENUS		
6 Route Setup (for the ZyWALL 35 and the ZyWALL 70)	6.1 Route Assessment		
	6.2 Traffic Redirect		
	6.3 Route Failover		
7 Wireless Setup	7.1 Wireless Setup	7.1.1 WLAN MAC Address Filter	
	7.2 TCP/IP and DHCP Ethernet Setup	7.2.1 IP Alias Setup	
11 Remote Node Setup	11.1 Remote Node Profile	11.1.2 Remote Node Network Layer Options	
		11.1.4 Remote Node Filter	
		11.1.5 Traffic Redirect Setup (for the ZyWALL 5 only)	
	11.2 Remote Node Profile (for the ZyWALL 35 and the ZyWALL 70)	11.2.2 Remote Node Network Layer Options	
		11.2.4 Remote Node Filter	
	11.3 Remote Node Profile (Backup ISP)	11.3.1 Remote Node PPP Options	
		11.3.2 Remote Node Network Layer Options	
		11.3.3 Remote Node Script	
		11.3.4 Remote Node Filter	
	12 Static Routing Setup	12.1 Edit Static Route Setup	
15 NAT Setup	15.1 Address Mapping Sets	15.1.x Address Mapping Rules	15.1.x.x Address Mapping Rule
	15.2 NAT Server Sets	15.2.x NAT Server Setup	15.2.x.x - NAT Server Configuration
	15.3 Trigger Ports	15.3.x Trigger Port Setup	
21 Filter and Firewall Setup	21.1 Filter Set Configuration	21.1.x Filter Rules Summary	21.1.x.x Generic Filter Rule
			21.1.x.x TCP/IP Filter Rule
	21.2 Firewall Setup		
23 System Password			

**Table 183** SMT Menus Overview (continued)

MENUS	SUB MENUS		
24 System Maintenance	24.1 System Status		
	24.2 System Information and Console Port Speed	24.2.1 System Information	
		24.2.2 Console Port Speed	
	24.3 Log and Trace	24.3.1 View Error Log	
		24.3.2 Syslog Logging	
		24.3.4 Call-Triggering Packet	
	24.4 Diagnostic		
	24.5 Backup Configuration		
	24.6 Restore Configuration		
	24.7 Upload Firmware	24.7.1 Upload System Firmware	
		24.7.2 Upload System Configuration File	
	24.8 Command Interpreter Mode		
	24.9 Call Control	24.9.1 Budget Management	
24.9.2 Call History			
24.10 Time and Date Setting			
24.11 Remote Management Setup			
25 IP Routing Policy Summary (for the ZyWALL 35 and the ZyWALL 70)	25.1 IP Routing Policy Setup	25.1.1 IP Routing Policy Setup	
26 Schedule Setup	26.1 Schedule Set Setup		

## 32.4 Changing the System Password

Change the system password by following the steps shown next.

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

**Figure 267** Menu 23: System Password

```
Menu 23 - System Password

Old Password= ?
New Password= ?
Retype to confirm= ?

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

- 2** Type your existing password and press [ENTER].
- 3** Type your new system password and press [ENTER].
- 4** Re-type your new system password for confirmation and press [ENTER].

Note that as you type a password, the screen displays an “x” for each character you type.

## 32.5 Resetting the ZyWALL

See [Section 2.3 on page 67](#) for directions on resetting the ZyWALL.

# CHAPTER 33

## SMT Menu 1 - General Setup

**Menu 1 - General Setup** contains administrative and system-related information.

### 33.1 Introduction to General Setup

**Menu 1 - General Setup** contains administrative and system-related information.

### 33.2 Configuring General Setup

- 1 Enter 1 in the main menu to open **Menu 1 - General Setup**.
- 2 The **Menu 1 - General Setup** screen appears, as shown next. Fill in the required fields.

**Figure 268** Menu 1: General Setup (Router Mode)

```

Menu 1 - General Setup

System Name=
Domain Name=

Device Mode= Router Mode

Edit Dynamic DNS= No

Press ENTER to Confirm or ESC to Cancel:

```

The following table describes the fields in this menu.

**Table 184** Menu 1: General Setup (Router Mode)

FIELD	DESCRIPTION
System Name	Choose a descriptive name for identification purposes. It is recommended you enter your computer's "Computer name" in this field. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. You can go to menu 24.8 and type "sys domain name" to see the current domain name used by your router. The domain name entered by you is given priority over the ISP assigned domain name. If you want to clear this field just press [SPACE BAR] and then [ENTER].
Device Mode	Press [SPACE BAR] and then [ENTER] to select <b>Router Mode</b> .



**Table 184** Menu 1: General Setup (Router Mode) (continued)

FIELD	DESCRIPTION
Edit Dynamic DNS	Press [SPACE BAR] and then [ENTER] 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.	

**Figure 269** Menu 1: General Setup (Bridge Mode)

```

Menu 1 - General Setup

System Name=
Domain Name=

Device Mode= Bridge Mode

IP Address= 192.168.1.1
Network Mask= 255.255.255.0
Gateway= 0.0.0.0
First System DNS Server
    IP Address= 0.0.0.0
Second System DNS Server
    IP Address= 0.0.0.0
Third System DNS Server
    IP Address= 0.0.0.0

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

The following table describes the fields not previously discussed (see [Table 184 on page 508](#)).

**Table 185** Menu 1: General Setup (Bridge Mode)

FIELD	DESCRIPTION
Device Mode	Press [SPACE BAR] and then [ENTER] to select <b>Bridge Mode</b> .
IP Address	Enter the IP address of your ZyWALL in dotted decimal notation.
Network Mask	Enter the subnet mask of your ZyWALL.
Gateway	Enter the gateway IP address.
First System DNS Server Second System DNS Server Third System DNS Server	Enter the DNS server's IP address(es) in the <b>IP Address</b> field(s) if you have the IP address(es) of the DNS server(s).

## 33.2.1 Configuring Dynamic DNS

To configure Dynamic DNS, set the ZyWALL to router mode in menu 1 or in the **MAINTENANCE Device Mode** screen and go to **Menu 1 - General Setup** and press [SPACE BAR] to select **Yes** in the **Edit Dynamic DNS** field. Press [ENTER] to display **Menu 1.1 - Configure Dynamic DNS** (shown next).

**Figure 270** Menu 1.1: Configure Dynamic DNS

```

Menu 1.1 - Configure Dynamic DNS

Service Provider= WWW.DynDNS.ORG
Active= No
Username=
Password= *****
Edit Host= No

Press ENTER to Confirm or ESC to Cancel:

```

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

**Table 186** Menu 1.1: Configure Dynamic DNS

FIELD	DESCRIPTION
Service Provider	This is the name of your Dynamic DNS service provider.
Active	Press [SPACE BAR] to select <b>Yes</b> and then press [ENTER] to make dynamic DNS active.
Username	Enter your user name.
Password	Enter the password assigned to you.
Edit Host	Press [SPACE BAR] and then [ENTER] to select <b>Yes</b> if you want to configure a DDNS host.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.	

### 33.2.1.1 Editing DDNS Host

To configure a DDNS host, follow the procedure below.

- 1 Configure your ZyWALL as a router in menu 1 or the **MAINTENANCE Device Mode** screen.
- 2 Enter 1 in the main menu to open **Menu 1 - General Setup**.
- 3 Press [SPACE BAR] to select **Yes** in the **Edit Dynamic DNS** field. Press [ENTER] to display **Menu 1.1 - Configure Dynamic DNS**.
- 4 Press [SPACE BAR] and then [ENTER] to select **Yes** in the **Edit Host** field. Press [ENTER] to display **Menu 1.1.1 - DDNS Host Summary**.

**Figure 271** Menu 1.1.1: DDNS Host Summary

```

Menu 1.1.1 DDNS Host Summary

#          Summary
-----
01  Hostname=ZyWALL,
    Type=Dynamic, WC=Yes, Offline=No, Policy=DDNS Server
    Detect, WAN1, HA=Yes
02  _____
03  _____
04  _____
05  _____

Select Command= None          Select Rule= N/A
Press ENTER to Confirm or ESC to Cancel:
    
```

The following table describes the fields in this screen.

**Table 187** Menu 1.1.1: DDNS Host Summary

FIELD	DESCRIPTION
#	This is the DDNS host index number.
Summary	This displays the details about the DDNS host.
Select Command	Press [SPACE BAR] to choose from <b>None</b> , <b>Edit</b> , <b>Delete</b> , <b>Next Page</b> or <b>Previous Page</b> and then press [ENTER]. You must select a DDNS host in the next field when you choose the <b>Edit</b> or <b>Delete</b> commands. Select <b>None</b> and then press [ENTER] to go to the "Press ENTER to Confirm..." prompt. Use <b>Edit</b> to create or edit a rule. Use <b>Delete</b> to remove a rule. To edit or delete a DDNS host, first make sure you are on the correct page. When a rule is deleted, subsequent rules do not move up in the page list. Select <b>Next Page</b> or <b>Previous Page</b> to view the next or previous page of DDNS hosts (respectively).
Select Rule	Type the DDNS host index number you wish to edit or delete and then press [ENTER].
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.	

- 5 Select **Edit** in the **Select Command** field; type the index number of the DDNS host you want to configure in the **Select Rule** field and press [ENTER] to open **Menu 1.1.1 - DDNS Edit Host** (see the next figure).

**Figure 272** Menu 1.1.1: DDNS Edit Host

```

Menu 1.1.1 - DDNS Edit Host

Hostname= ZyWALL
DDNS Type= DynamicDNS
Enable Wildcard Option= Yes
Enable Off Line Option= N/A
Bind WAN= 1
HA= Yes
IP Address Update Policy:
  Let DDNS Server Auto Detect= Yes
  Use User-Defined= N/A
  Use WAN IP Address= N/A

Press ENTER to Confirm or ESC to Cancel:

```

The following table describes the fields in this screen.

**Table 188** Menu 1.1.1: DDNS Edit Host

FIELD	DESCRIPTION
Host Name	Enter your host name in this field.
DDNS Type	Press [SPACE BAR] and then [ENTER] to select <b>DynamicDNS</b> if you have the Dynamic DNS service. Select <b>StaticDNS</b> if you have the Static DNS service. Select <b>CustomDNS</b> if you have the Custom DNS service.
Enable Wildcard Option	Your ZyWALL supports DYNDNS Wildcard. Press [SPACE BAR] and then [ENTER] to select <b>Yes</b> or <b>No</b> . This field is <b>N/A</b> when you choose DDNS client as your service provider.
Enable Off Line Option	This field is only available when <b>CustomDNS</b> is selected in the <b>DDNS Type</b> field. Press [SPACE BAR] and then [ENTER] to select <b>Yes</b> . When <b>Yes</b> is selected, <a href="http://www.dyndns.org/">http://www.dyndns.org/</a> traffic is redirected to a URL that you have previously specified (see <a href="http://www.dyndns.org/">www.dyndns.org</a> for details).
Bind WAN	Enter the WAN port to use for updating the IP address of the domain name.
HA	Press [SPACE BAR] and then [ENTER] to select <b>Yes</b> to enable the high availability (HA) feature. If the WAN port specified in the <b>Bind WAN</b> field does not have a connection, the ZyWALL will attempt to use the IP address of another WAN port to update the domain name. When the WAN ports are in the active/passive operating mode, the ZyWALL will update the domain name with the IP address of whichever WAN port has a connection, regardless of the setting in the <b>Bind WAN</b> field. Clear this check box and the ZyWALL will not update the domain name with an IP address if the WAN port specified in the <b>Bind WAN</b> field does not have a connection.  <b>Note:</b> If you enable high availability, DDNS can also function when the ZyWALL uses the dial backup port. DDNS does not function when the ZyWALL uses traffic redirect.  Refer to <a href="#">Section 26.10.2 on page 428</a> for detailed information.

**Table 188** Menu 1.1.1: DDNS Edit Host (continued)

FIELD	DESCRIPTION
IP Address Update Policy:	<p>You can select <b>Yes</b> in either the <b>Let DDNS Server Auto Detect</b> field (recommended) or the <b>Use User-Defined</b> field, but not both.</p> <p>With the <b>Let DDNS Server Auto Detect</b> and <b>Use User-Defined</b> fields both set to <b>No</b>, the DDNS server automatically updates the IP address of the host name(s) with the ZyWALL's WAN IP address.</p> <p>DDNS does not work with a private IP address. When both fields are set to <b>No</b>, the ZyWALL must have a public WAN IP address in order for DDNS to work.</p>
Let DDNS Server Auto Detect	<p>Only select this option when there are one or more <b>NAT</b> routers between the ZyWALL and the DDNS server. Press [SPACE BAR] to select <b>Yes</b> and then press [ENTER] to have the DDNS server automatically detect and use the IP address of the NAT router that has a public IP address.</p> <p><b>Note:</b> The DDNS server may not be able to detect the proper IP address if there is an HTTP proxy server between the ZyWALL and the DDNS server.</p>
Use User-Defined	<p>Press [SPACE BAR] to select <b>Yes</b> and then press [ENTER] to update the IP address of the host name(s) to the IP address specified below.</p> <p>Only select <b>Yes</b> if the ZyWALL uses or is behind a static public IP address.</p>
Use WAN IP Address	<p>Enter the static public IP address if you select <b>Yes</b> in the <b>Use User-Defined</b> field.</p>
<p>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.</p>	

The IP address updates when you reconfigure menu 1 or perform DHCP client renewal.

# CHAPTER 34

## WAN and Dial Backup Setup

This chapter describes how to configure the WAN using menu 2 and dial-backup using menus 2.1 and 11.1.

### 34.1 Introduction to WAN and Dial Backup Setup

This chapter explains how to configure settings for your WAN port and how to configure the ZyWALL for a dial backup connection.

### 34.2 WAN Setup

From the main menu, enter 2 to open menu 2.

**Figure 273** MAC Address Cloning in WAN Setup

```
Menu 2 - WAN Setup

WAN 1 MAC Address:
Assigned By= Factory default
IP Address= N/A
WAN 2 MAC Address:
Assigned By= Factory default
IP Address= N/A

Dial-Backup:
Active= No
Port Speed= 115200
AT Command String:
Init= at&fs0=0
Edit Advanced Setup= No

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

The following table describes the fields in this screen.

**Table 189** MAC Address Cloning in WAN Setup

FIELD	DESCRIPTION
(WAN 1/2) MAC Address	
Assigned By	Press [SPACE BAR] and then [ENTER] to choose one of two methods to assign a MAC Address. Choose <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 computer whose IP you give in the following field.
IP Address	This field is applicable only if you choose the <b>IP address attached on LAN</b> method in the <b>Assigned By</b> field. Enter the IP address of the computer on the LAN whose MAC you are cloning.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.	

## 34.3 Dial Backup

The Dial Backup port can be used in reserve, as a traditional dial-up connection should the broadband connection to the WAN port fail. To set up the auxiliary port (Dial Backup) for use in the event that the regular WAN connection is dropped, first make sure you have set up the switch and port connection (see the *Quick Start Guide*), then configure

- 1 Menu 2 - WAN Setup,
- 2 Menu 2.1 - Advanced WAN Setup and
- 3 Menu 11.1 - Remote Node Profile (Backup ISP) as shown next

Refer also to the section about traffic redirect for information on an alternate backup WAN connection.

## 34.4 Configuring Dial Backup in Menu 2

From the main menu, enter 2 to open menu 2.

**Figure 274** Menu 2: Dial Backup Setup

```

Menu 2 - WAN Setup

WAN 1 MAC Address:
  Assigned By= Factory default
  IP Address= N/A
WAN 2 MAC Address:
  Assigned By= Factory default
  IP Address= N/A

Dial-Backup:
  Active= No
  Port Speed= 115200
  AT Command String:
    Init= at&fs0=0
  Edit Advanced Setup= Yes

Press ENTER to Confirm or ESC to Cancel:

```

The following table describes the fields in this menu.

**Table 190** Menu 2: Dial Backup Setup

FIELD	DESCRIPTION
Dial-Backup:	
Active	Use this field to turn the dial-backup feature on ( <b>Yes</b> ) or off ( <b>No</b> ).
Port Speed	Press [SPACE BAR] and then press [ENTER] to select the speed of the connection between the Dial Backup port and the external device. Available speeds are: <b>9600, 19200, 38400, 57600, 115200 or 230400</b> bps.
AT Command String:	
Init	Enter the AT command string to initialize the WAN device. Consult the manual of your WAN device connected to your Dial Backup port for specific AT commands.
Edit Advanced Setup	To edit the advanced setup for the Dial Backup port, move the cursor to this field; press the [SPACE BAR] to select <b>Yes</b> and then press [ENTER] to go to <b>Menu 2.1 - Advanced Setup</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.	

## 34.5 Advanced WAN Setup

**Note:** Consult the manual of your WAN device connected to your Dial Backup port for specific AT commands.



To edit the advanced setup for the Dial Backup port, move the cursor to the **Edit Advanced Setup** field in **Menu 2 - WAN Setup**, press the [SPACE BAR] to select **Yes** and then press [ENTER].

**Figure 275** Menu 2.1: Advanced WAN Setup

```

Menu 2.1 - Advanced WAN Setup

AT Command Strings:
Dial= atdt
Drop= ~~~+++~~ath
Answer= ata

Drop DTR When Hang Up= Yes

AT Response Strings:
CLID= NMBR =
Called Id=
Speed= CONNECT

Call Control:
Dial Timeout(sec)= 60
Retry Count= 0
Retry Interval(sec)= N/A
Drop Timeout(sec)= 20
Call Back Delay(sec)= 15

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

The following table describes fields in this menu.

**Table 191** Advanced WAN Port Setup: AT Commands Fields

FIELD	DESCRIPTION
AT Command Strings:	
Dial	Enter the AT Command string to make a call.
Drop	Enter the AT Command string to drop a call. “~” represents a one second wait, e.g., “~~~+++~~ath” can be used if your modem has a slow response time.
Answer	Enter the AT Command string to answer a call.
Drop DTR When Hang Up	Press the [SPACE BAR] to choose either <b>Yes</b> or <b>No</b> . When <b>Yes</b> is selected (the default), the DTR (Data Terminal Ready) signal is dropped after the “AT Command String: Drop” is sent out.
AT Response Strings:	
CLID (Calling Line Identification)	Enter the keyword that precedes the CLID (Calling Line Identification) in the AT response string. This lets the ZyWALL capture the CLID in the AT response string that comes from the WAN device. CLID is required for CLID authentication.
Called Id	Enter the keyword preceding the dialed number.
Speed	Enter the keyword preceding the connection speed.

**Table 192** Advanced WAN Port Setup: Call Control Parameters

FIELD	DESCRIPTION
Call Control	
Dial Timeout (sec)	Enter a number of seconds for the ZyWALL to keep trying to set up an outgoing call before timing out (stopping). The ZyWALL times out and stops if it cannot set up an outgoing call within the timeout value.
Retry Count	Enter a number of times for the ZyWALL to retry a busy or no-answer phone number before blacklisting the number.
Retry Interval (sec)	Enter a number of seconds for the ZyWALL to wait before trying another call after a call has failed. This applies before a phone number is blacklisted.
Drop Timeout (sec)	Enter a number of seconds for the ZyWALL to wait before dropping the DTR signal if it does not receive a positive disconnect confirmation.
Call Back Delay (sec)	Enter a number of seconds for the ZyWALL to wait between dropping a callback request call and dialing the co-responding callback call.

## 34.6 Remote Node Profile (Backup ISP)

On a ZyWALL with multiple WAN ports, enter **3** in **Menu 11 - Remote Node Setup** to open **Menu 11.3 - Remote Node Profile (Backup ISP)** (shown below) and configure the setup for your Dial Backup port connection.

On a ZyWALL with a single WAN port, enter **2** in **Menu 11 - Remote Node Setup** to open **Menu 11.2 - Remote Node Profile (Backup ISP)** and configure the setup for your Dial Backup port connection.

**Figure 276** Menu 11.3: Remote Node Profile (Backup ISP)

```

Menu 11.3 - Remote Node Profile (Backup ISP)

Rem Node Name=                               Edit PPP Options= No
Active= No                                    Edit IP= No
                                              Edit Script Options= No

Outgoing:                                     Telco Option:
  My Login= ChangeMe                          Allocated Budget (min)= 0
  My Password= *****                       Period(hr)= 0
  Retype to Confirm= *****                 Schedules=
  Authen= CHAP/PAP                            Always On= No
  Pri Phone #= 0
  Sec Phone #=

                                              Session Options:
                                              Edit Filter Sets= No
                                              Idle Timeout(sec)= 100

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

The following table describes the fields in this menu.

**Table 193** Menu 11.3: Remote Node Profile (Backup ISP)

FIELD	DESCRIPTION
Rem Node Name	Enter a descriptive name for the remote node. This field can be up to eight characters.
Active	Press [SPACE BAR] and then [ENTER] to select <b>Yes</b> to enable the remote node or <b>No</b> to disable the remote node.
Outgoing	
My Login	Enter the login name assigned by your ISP for this remote node.
My Password	Enter the password assigned by your ISP for this remote node.
Retype to Confirm	Enter your password again to make sure that you have entered is correctly.
Authen	This field sets the authentication protocol used for outgoing calls. Options for this field are: <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.
Pri Phone # Sec Phone #	Enter the first (primary) phone number from the ISP for this remote node. If the Primary Phone number is busy or does not answer, your ZyWALL dials the Secondary Phone number if available. Some areas require dialing the pound sign # before the phone number for local calls. Include a # symbol at the beginning of the phone numbers as required.
Edit PPP Options	Move the cursor to this field and use the space bar to select [Yes] and press [Enter] to edit the PPP options for this remote node. This brings you to <b>Menu 11.3.1 - Remote Node PPP Options</b> (see <a href="#">Section 34.7 on page 520</a> ).

**Table 193** Menu 11.3: Remote Node Profile (Backup ISP) (continued)

FIELD	DESCRIPTION
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 11.3.2 - Remote Node Network Layer Options</b> . See <a href="#">Section 34.8 on page 521</a> for more information.
Edit Script Options	Press [SPACE BAR] to select <b>Yes</b> and press [ENTER] to edit the AT script for the dial backup remote node ( <b>Menu 11.3.3 - Remote Node Script</b> ). See <a href="#">Section 34.9 on page 523</a> for more information.
Telco Option	
Allocated Budget	Enter the maximum number of minutes that this remote node may be called within the time period configured in the <b>Period</b> field. The default for this field is 0 meaning there is no budget control and no time limit for accessing this remote node.
Period(hr)	Enter the time period (in hours) for how often the budget should be reset. For example, to allow calls to this remote node for a maximum of 10 minutes every hour, set the <b>Allocated Budget</b> to 10 (minutes) and the <b>Period</b> to 1 (hour).
Schedules	You can apply up to four schedule sets here. For more details please refer to <a href="#">Chapter 51 on page 648</a> .
Always On	Press [SPACE BAR] to select <b>Yes</b> to set this connection to be on all the time, regardless of whether or not there is any traffic. Select <b>No</b> to have this connection act as a dial-up connection.
Session Options	
Edit Filter sets	This field leads to another "hidden" menu. Use [SPACE BAR] to select <b>Yes</b> and press [ENTER] to open menu 11.3.4 to edit the filter sets. See <a href="#">Section 34.10 on page 525</a> for more details.
Idle Timeout	Enter the number of seconds of idle time (when there is no traffic from the ZyWALL to the remote node) that can elapse before the ZyWALL automatically disconnects the PPP connection. This option only applies when the ZyWALL initiates the call.
Once you have configured this menu, press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.	

## 34.7 Editing PPP Options

The ZyWALL's dial back-up feature uses PPP. To edit the remote node PPP Options, move the cursor to the **Edit PPP Options** field in **Menu 11.3 - Remote Node Profile (Backup ISP)**, and use the space bar to select **Yes**. Press [Enter] to open **Menu 11.3.1 - Remote Node PPP Options** as shown next.

**Figure 277** Menu 11.3.1: Remote Node PPP Options

```
Menu 11.3.1 - Remote Node PPP Options

Encapsulation= Standard PPP
Compression= No

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

This table describes the Remote Node PPP Options Menu, and contains instructions on how to configure the PPP options fields.

**Table 194** Menu 11.3.1: Remote Node PPP Options

FIELD	DESCRIPTION
Encapsulation	Press [SPACE BAR] and then [ENTER] to select <b>CISCO PPP</b> if your Dial Backup WAN device uses Cisco PPP encapsulation, otherwise select <b>Standard PPP</b> .
Compression	Press [SPACE BAR] and then [ENTER] to select <b>Yes</b> to enable or <b>No</b> to disable Stac compression.
Once you have configured this menu, press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.	

## 34.8 Editing TCP/IP Options

Move the cursor to the **Edit IP** field in menu 11.3, then press [SPACE BAR] to select **Yes**. Press [ENTER] to open **Menu 11.3.2 - Remote Node Network Layer Options**. Not all fields are available on all models.

**Figure 278** Menu 11.3.2: Remote Node Network Layer Options

```

Menu 11.3.2 - Remote Node Network Layer Options

IP Address Assignment= Static
Rem IP Addr= 0.0.0.0
Rem Subnet Mask= 0.0.0.0
My WAN Addr= 0.0.0.0

Network Address Translation= SUA Only
NAT Lookup Set= 255
Metric= 15
Private= No
RIP Direction= None
  Version= N/A
Multicast= None

Enter here to CONFIRM or ESC to CANCEL:

```

The following table describes the fields in this menu.

**Table 195** Menu 11.3.2: Remote Node Network Layer Options

FIELD	DESCRIPTION
IP Address Assignment	If your ISP did not assign you a fixed IP address, press [SPACE BAR] and then [ENTER] to select <b>Dynamic</b> , otherwise select <b>Static</b> and enter the IP address and subnet mask in the following fields.
Rem IP Address	Enter the (fixed) IP address assigned to you by your ISP (static IP address assignment is selected in the previous field).
Rem Subnet Mask	Enter the subnet mask associated with your static IP.
My WAN Addr	Leave the field set to 0.0.0.0 to have the ISP or other remote router dynamically (automatically) assign your WAN IP address if you do not know it. Enter your WAN IP address here if you know it (static). This is the address assigned to your local ZyWALL, not the remote router.
Network Address Translation	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet). Press [SPACE BAR] and then [ENTER] to select either <b>Full Feature</b> , <b>None</b> or <b>SUA Only</b> . Choose <b>None</b> to disable NAT. Choose <b>SUA Only</b> if you have a single public IP address. SUA (Single User Account) is a subset of NAT that supports two types of mapping: <b>Many-to-One</b> and <b>Server</b> . Choose <b>Full Feature</b> if you have multiple public IP addresses. <b>Full Feature</b> mapping types include: <b>One-to-One</b> , <b>Many-to-One</b> (SUA/PAT), <b>Many-to-Many Overload</b> , <b>Many- One-to-One</b> and <b>Server</b> . When you select <b>Full Feature</b> you must configure at least one address mapping set. See <a href="#">Chapter 22 on page 374</a> for a full discussion on this feature.

**Table 195** Menu 11.3.2: Remote Node Network Layer Options

FIELD	DESCRIPTION
NAT Lookup Set	If you select <b>SUA Only</b> in the <b>Network Address Translation</b> field, it displays <b>255</b> and indicates the SMT will use the pre-configured <b>Set 255</b> (read only) in menu 15.1. If you select <b>Full Feature</b> or <b>None</b> in the <b>Network Address Translation</b> field, it displays <b>1</b> , <b>2</b> or <b>3</b> and indicates the SMT will use the pre-configured <b>Set 1</b> in menu 15.1 for the first WAN port, <b>Set 2</b> in menu 15.1 for the second WAN port and <b>Set 3</b> for the Backup port. Refer to <a href="#">Section 42.2 on page 564</a> for more information.
Metric	Enter a number from 1 to 15 to set this route's priority among the ZyWALL's routes. The smaller the number, the higher priority the route has.
Private	This parameter determines if the ZyWALL will include the route to this remote node in its RIP broadcasts. If set to <b>Yes</b> , this route is kept private and not included in RIP broadcasts. If <b>No</b> , the route to this remote node will be propagated to other hosts through RIP broadcasts.
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the <b>RIP Direction</b> from <b>Both</b> , <b>None</b> , <b>In Only</b> , <b>Out Only</b> and <b>None</b> .
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version from <b>RIP-1</b> , <b>RIP-2B</b> and <b>RIP-2M</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 <a href="#">Chapter 5 on page 110</a> for more information on this feature.
Once you have completed filling in <b>Menu 11.3.2 Remote Node Network Layer Options</b> , press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration and return to menu 11.3, or press [ESC] at any time to cancel.	

## 34.9 Editing Login Script

For some remote gateways, text login is required before PPP negotiation is started. The ZyWALL provides a script facility for this purpose. The script has six programmable sets; each set is composed of an 'Expect' string and a 'Send' string. After matching a message from the server to the 'Expect' field, the ZyWALL returns the set's 'Send' string to the server.

For instance, a typical login sequence starts with the server printing a banner, a login prompt for you to enter the user name and a password prompt to enter the password:

```
Welcome to Acme, Inc.
Login: myLogin
Password:
```

To handle the first prompt, you specify "ogin: " as the 'Expect' string and "myLogin" as the 'Send' string in set 1. The reason for leaving out the leading "L" is to avoid having to know exactly whether it is upper or lower case. Similarly, you specify "word: " as the 'Expect' string and your password as the 'Send' string for the second prompt in set 2.

You can use two variables, \$USERNAME and \$PASSWORD (all UPPER case), to represent the actual user name and password in the script, so they will not show in the clear. They are replaced with the outgoing login name and password in the remote node when the ZyWALL sees them in a 'Send' string. Please note that both variables must be entered exactly as shown. No other characters may appear before or after, either, i.e., they must be used alone in response to login and password prompts.

Please note that the ordering of the sets is significant, i.e., starting from set 1, the ZyWALL will wait until the 'Expect' string is matched before it proceeds to set 2, and so on for the rest of the script. When both the 'Expect' and the 'Send' fields of the current set are empty, the ZyWALL will terminate the script processing and start PPP negotiation. This implies two things: first, the sets must be contiguous; the sets after an empty one are ignored. Second, the last set should match the final message sent by the server. For instance, if the server prints:

```
login successful.
Starting PPP...
```

after you enter the password, then you should create a third set to match the final "PPP . . ." but without a "Send" string. Otherwise, the ZyWALL will start PPP prematurely right after sending your password to the server.

If there are errors in the script and it gets stuck at a set for longer than the "Dial Timeout" in menu 2 (default 60 seconds), the ZyWALL will timeout and drop the line. To debug a script, go to Menu 24.4 to initiate a manual call and watch the trace display to see if the sequence of messages and prompts from the server differs from what you expect.

**Figure 279** Menu 11.3.3: Remote Node Script

```

Menu 11.3.3 - Remote Node Script

Active= No

Set 1:
  Expect=
  Send=
Set 2:
  Expect=
  Send=
Set 3:
  Expect=
  Send=
Set 4:
  Expect=
  Send=
Set 5:
  Expect=
  Send=
Set 6:
  Expect=
  Send=

Enter here to CONFIRM or ESC to CANCEL:

```



The following table describes the fields in this menu.

**Table 196** Menu 11.3.3: Remote Node Script

FIELD	DESCRIPTION
Active	Press [SPACE BAR] and then [ENTER] to select either <b>Yes</b> to enable the AT strings or <b>No</b> to disable them.
Set 1-6: Expect	Enter an Expect string to match. After matching the Expect string, the ZyWALL returns the string in the <b>Send</b> field.
Set 1-6: Send	Enter a string to send out after the Expect string is matched.

## 34.10 Remote Node Filter

Move the cursor to the field **Edit Filter Sets** in menu 11.3, and then press [SPACE BAR] to set the value to **Yes**. Press [ENTER] to open **Menu 11.3.4 - Remote Node Filter**.

Use menu 11.3.4 to specify the filter set(s) to apply to the incoming and outgoing traffic between this remote node and the ZyWALL to prevent certain packets from triggering calls. You can specify up to four filter sets separated by commas, for example, 1, 5, 9, 12, in each filter field. Note that spaces are accepted in this field. Please refer to [Chapter 44 on page 584](#) for more information on defining the filters.

**Figure 280** Menu 11.3.4: Remote Node Filter

```

Menu 11.3.4 - Remote Node Filter

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

Enter here to CONFIRM or ESC to CANCEL:

```

# CHAPTER 35

## LAN Setup

This chapter describes how to configure the LAN using **Menu 3 - LAN Setup**.

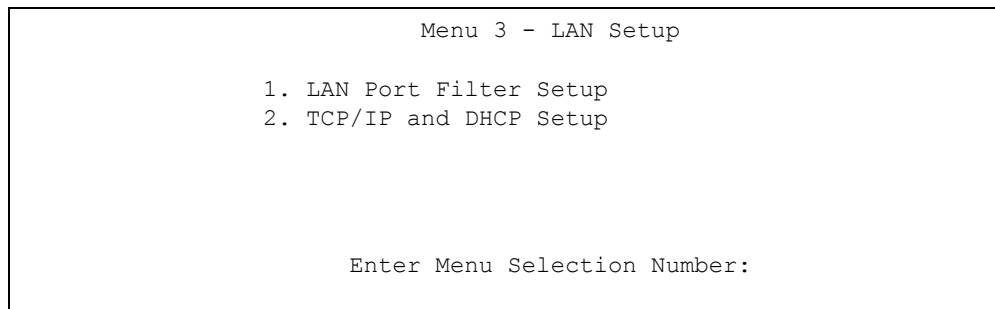
### 35.1 Introduction to LAN Setup

This chapter describes how to configure the ZyWALL for LAN and wireless LAN connections.

### 35.2 Accessing the LAN Menus

From the main menu, enter 3 to open **Menu 3 - LAN Setup**.

**Figure 281** Menu 3: LAN Setup



```
Menu 3 - LAN Setup

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

Enter Menu Selection Number:
```

### 35.3 LAN Port Filter Setup

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

**Figure 282** Menu 3.1: LAN Port Filter Setup

```
Menu 3.1 - LAN Port Filter Setup

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

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

## 35.4 TCP/IP and DHCP Ethernet Setup Menu

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

**Figure 283** Menu 3: TCP/IP and DHCP Setup

```
Menu 3 - LAN Setup

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

Enter Menu Selection Number:
```

From menu 3, select the submenu option **TCP/IP and DHCP Setup** and press [ENTER]. The screen now displays **Menu 3.2 - TCP/IP and DHCP Ethernet Setup**, as shown next. Not all fields are available on all models.

**Figure 284** Menu 3.2: TCP/IP and DHCP Ethernet Setup

```

Menu 3.2 - TCP/IP and DHCP Ethernet Setup

DHCP= Server                    TCP/IP Setup:
Client IP Pool:
  Starting Address= 192.168.1.33  IP Address= 192.168.1.1
  Size of Client IP Pool= 128    IP Subnet Mask= 255.255.255.0
                                   RIP Direction= Both
                                   Version= RIP-1
                                   Multicast= None
                                   Edit IP Alias= No

DHCP Server Address= N/A

Press ENTER to Confirm or ESC to Cancel:

```

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

**Table 197** Menu 3.2: DHCP Ethernet Setup Fields

FIELD	DESCRIPTION
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 items need to be set:
Client IP Pool:	
Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Size of Client IP Pool	This field specifies the size, or count of the IP address pool.

**Table 197** Menu 3.2: DHCP Ethernet Setup Fields

FIELD	DESCRIPTION
First DNS Server Second DNS Server Third DNS Server	<p>The ZyWALL passes a DNS (Domain Name System) server IP address (in the order you specify here) to the DHCP clients.</p> <p>Select <b>From ISP</b> if your ISP dynamically assigns DNS server information (and the ZyWALL's WAN IP address). The <b>IP Address</b> field below displays the (read-only) DNS server IP address that the ISP assigns.</p> <p>Select <b>User-Defined</b> if you have the IP address of a DNS server. Enter the DNS server's IP address in the <b>IP Address</b> field below. If you chose <b>User-Defined</b>, but leave the IP address set to 0.0.0.0, <b>User-Defined</b> changes to <b>None</b> after you save your changes. If you set a second choice to <b>User-Defined</b>, and enter the same IP address, the second <b>User-Defined</b> changes to <b>None</b> after you save your changes.</p> <p>Select <b>DNS Relay</b> to have the ZyWALL act as a DNS proxy. The ZyWALL's LAN IP address displays in the <b>IP Address</b> field below (read-only). The ZyWALL tells the DHCP clients on the LAN that the ZyWALL itself is the DNS server. When a computer on the LAN sends a DNS query to the ZyWALL, the ZyWALL forwards the query to the ZyWALL's system DNS server (configured in menu 1) and relays the response back to the computer. You can only select <b>DNS Relay</b> for one of the three servers; if you select <b>DNS Relay</b> for a second or third DNS server, that choice changes to <b>None</b> after you save your changes.</p> <p>Select <b>None</b> if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it.</p>
DHCP Server Address	If <b>Relay</b> is selected in the <b>DHCP</b> field above, then type the IP address of the actual, remote DHCP server here.

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

**Note:** LAN and DMZ IP addresses must be on separate subnets.

**Table 198** Menu 3.2: LAN TCP/IP Setup Fields

FIELD	DESCRIPTION
TCP/IP Setup:	
IP Address	Enter the IP address of your ZyWALL in dotted decimal notation
IP Subnet Mask	Your ZyWALL will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyWALL.
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP direction. Options are: <b>Both</b> , <b>In Only</b> , <b>Out Only</b> or <b>None</b> .
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version. Options are: <b>RIP-1</b> , <b>RIP-2B</b> or <b>RIP-2M</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] and then [ENTER] to enable IP Multicasting or select <b>None</b> (default) to disable it.
Edit IP Alias	The ZyWALL supports three logical LAN interfaces via its single physical Ethernet interface with the ZyWALL itself as the gateway for each LAN network. Press [SPACE BAR] to select <b>Yes</b> and then press [ENTER] to display menu 3.2.1
When you have completed this menu, press [ENTER] at the prompt [Press ENTER to Confirm...] to save your configuration, or press [ESC] at any time to cancel.	

### 35.4.1 IP Alias Setup

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

You must use menu 3.2 to configure the first network. Move the cursor to the **Edit IP Alias** field, press [SPACE BAR] to choose **Yes** and press [ENTER] to configure the second and third network.

Press [ENTER] to open **Menu 3.2.1 - IP Alias Setup**, as shown next.

**Figure 285** Menu 3.2.1: IP Alias Setup

```

Menu 3.2.1 - IP Alias Setup

IP Alias 1= Yes
  IP Address= 192.168.2.1
  IP Subnet Mask= 255.255.255.0
  RIP Direction= None
    Version= RIP-1
  Incoming protocol filters=
  Outgoing protocol filters=
IP Alias 2= No
  IP Address= N/A
  IP Subnet Mask= N/A
  RIP Direction= N/A
    Version= N/A
  Incoming protocol filters= N/A
  Outgoing protocol filters= N/A

Enter here to CONFIRM or ESC to CANCEL:

```

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

**Table 199** Menu 3.2.1: IP Alias Setup

FIELD	DESCRIPTION
IP Alias 1, 2	Choose <b>Yes</b> to configure the LAN network for the ZyWALL.
IP Address	Enter the IP address of your ZyWALL in dotted decimal notation.
IP Subnet Mask	Your ZyWALL will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the ZyWALL.
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP direction. Options are <b>Both</b> , <b>In Only</b> , <b>Out Only</b> or <b>None</b> .
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version. Options are <b>RIP-1</b> , <b>RIP-2B</b> or <b>RIP-2M</b> .
Incoming Protocol Filters	Enter the filter set(s) you wish to apply to the incoming traffic between this node and the ZyWALL.

**Table 199** Menu 3.2.1: IP Alias Setup (continued)

FIELD	DESCRIPTION
Outgoing Protocol Filters	Enter the filter set(s) you wish to apply to the outgoing traffic between this node and the ZyWALL.
When you have completed this menu, press [ENTER] at the prompt [Press ENTER to Confirm...] to save your configuration, or press [ESC] at any time to cancel.	

# CHAPTER 36

## Internet Access

This chapter shows you how to configure your ZyWALL for Internet access.

### 36.1 Introduction to Internet Access Setup

Use information from your ISP along with the instructions in this chapter to set up your ZyWALL to access the Internet. There are three different menu 4 screens depending on whether you chose **Ethernet**, **PPTP** or **PPPoE** Encapsulation. Contact your ISP to determine what encapsulation type you should use.

**Note:** This menu configures **WAN 1** on a ZyWALL with multiple WAN ports. Configure the WAN 2 port in **Menu 11.2 - Remote Node Profile** or in the **WAN WAN 2** screen via the web configurator.

### 36.2 Ethernet Encapsulation

If you choose **Ethernet** in menu 4 you will see the next menu.

**Figure 286** Menu 4: Internet Access Setup (Ethernet)

```
Menu 4 - Internet Access Setup

ISP's Name= WAN_1
Encapsulation= Ethernet
  Service Type= Standard
  My Login= N/A
  My Password= N/A
  Retype to Confirm= N/A
  Login Server= N/A
  Relogin Every (min)= N/A
IP Address Assignment= Dynamic
  IP Address= N/A
  IP Subnet Mask= N/A
  Gateway IP Address= N/A
Network Address Translation= SUA Only

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



The following table describes the fields in this menu.

**Table 200** Menu 4: Internet Access Setup (Ethernet)

FIELD	DESCRIPTION
ISP's Name	This is the descriptive name of your ISP for identification purposes.
Encapsulation	Press [SPACE BAR] and then press [ENTER] to choose <b>Ethernet</b> . The encapsulation method influences your choices for the <b>IP Address</b> field.
Service Type	Press [SPACE BAR] and then [ENTER] to select <b>Standard</b> , <b>RR-Toshiba</b> (RoadRunner Toshiba authentication method), <b>RR-Manager</b> (RoadRunner Manager authentication method), <b>RR-Telstra</b> or <b>Telia Login</b> . Choose a RoadRunner flavor if your ISP is Time Warner's RoadRunner; otherwise choose <b>Standard</b> .
<b>Note:</b> DSL users must choose the <b>Standard</b> option only. The <b>My Login</b> , <b>My Password</b> and <b>Login Server</b> fields are not applicable in this case.	
My Login	Enter the login name given to you by your ISP.
My Password	Type your password again for confirmation.
Retype to Confirm	Enter your password again to make sure that you have entered is correctly.
Login Server	The ZyWALL will find the RoadRunner Server IP if this field is left blank. If it does not, then you must enter the authentication server IP address.
Relogin Every (min)	This field is available when you select <b>Telia Login</b> in the <b>Service Type</b> field. The Telia server logs the ZyWALL out if the ZyWALL does not log in periodically. Type the number of minutes from 1 to 59 (30 recommended) for the ZyWALL to wait between logins.
IP Address Assignment	If your ISP did not assign you a fixed IP address, press [SPACE BAR] and then [ENTER] to select <b>Dynamic</b> , otherwise select <b>Static</b> and enter the IP address and subnet mask in the following fields.
IP Address	Enter the (fixed) IP address assigned to you by your ISP (static IP address assignment is selected in the previous field).
IP Subnet Mask	Enter the subnet mask associated with your static IP.
Gateway IP Address	Enter the gateway IP address associated with your static IP.
Network Address Translation	<p>Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet).</p> <p>Choose <b>None</b> to disable NAT.</p> <p>Choose <b>SUA Only</b> if you have a single public IP address. SUA (Single User Account) is a subset of NAT that supports two types of mapping: <b>Many-to-One</b> and <b>Server</b>.</p> <p>Choose <b>Full Feature</b> if you have multiple public IP addresses. <b>Full Feature</b> mapping types include: <b>One-to-One</b>, <b>Many-to-One</b> (SUA/PAT), <b>Many-to-Many Overload</b>, <b>Many- One-to-One</b> and <b>Server</b>. When you select <b>Full Feature</b> you must configure at least one address mapping set!</p> <p>Please see <a href="#">Chapter 22 on page 374</a> for a more detailed discussion on the Network Address Translation feature.</p>
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.	

## 36.3 Configuring the PPTP Client

**Note:** The ZyWALL supports only one PPTP server connection at any given time.

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

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

**Figure 287** Internet Access Setup (PPTP)

```

Menu 4 - Internet Access Setup

ISP's Name= WAN_1
Encapsulation= PPTP
Service Type= N/A
My Login=
My Password= *****
Retype to Confirm= *****
Idle Timeout= 100

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

Press ENTER to Confirm or ESC to Cancel:

```

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

**Table 201** New Fields in Menu 4 (PPTP) Screen

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

## 36.4 Configuring the PPPoE Client

If you enable PPPoE in menu 4, you will see the next screen. For more information on PPPoE, please see [Appendix F on page 702](#).

**Figure 288** Internet Access Setup (PPPoE)

```

Menu 4 - Internet Access Setup

ISP's Name= WAN_1
Encapsulation= PPPoE
Service Type= N/A
My Login=
My Password= *****
Retype to Confirm= *****
Idle Timeout= 100

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

Press ENTER to Confirm or ESC to Cancel:

```

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

**Table 202** New Fields in Menu 4 (PPPoE) screen

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

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

## 36.5 Basic Setup Complete

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

**Note:** When the firewall is activated, the default policy allows all communications to the Internet that originate from the LAN, and blocks all traffic to the LAN that originates from the Internet.

You may deactivate the firewall in menu 21.2 or via the ZyWALL embedded web configurator. You may also define additional firewall rules or modify existing ones but please exercise extreme caution in doing so. See the chapters on firewall for more information on the firewall.

# CHAPTER 37

## DMZ Setup

This chapter describes how to configure the ZyWALL's DMZ using **Menu 5 - DMZ Setup**.

### 37.1 Configuring DMZ Setup

From the main menu, enter 5 to open **Menu 5 – DMZ Setup**.

**Figure 289** Menu 5: DMZ Setup

```
Menu 5 - DMZ Setup

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

Enter Menu Selection Number:
```

### 37.2 DMZ Port Filter Setup

This menu allows you to specify the filter sets that you wish to apply to your public server(s) traffic.

**Figure 290** Menu 5.1: DMZ Port Filter Setup

```
Menu 5.1 - DMZ Port Filter Setup

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

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

### 37.3 TCP/IP Setup

For more detailed information about RIP setup, IP Multicast and IP alias, please refer to [Chapter 5 on page 110](#).

### 37.3.1 IP Address

From the main menu, enter 5 to open **Menu 5 - DMZ Setup** to configure TCP/IP (RFC 1155).

**Figure 291** Menu 5: DMZ Setup

```
Menu 5 - DMZ Setup

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

Enter Menu Selection Number:
```

From menu 5, select the submenu option **2. TCP/IP and DHCP Setup** and press [ENTER]. The screen now displays **Menu 5.2 - TCP/IP and DHCP Ethernet Setup**, as shown next.

**Figure 292** Menu 5.2: TCP/IP and DHCP Ethernet Setup

```
Menu 5.2 - TCP/IP and DHCP Ethernet Setup

DHCP= None
Client IP Pool:
  Starting Address= N/A
  Size of Client IP Pool= N/A

DHCP Server Address= N/A

TCP/IP Setup:
IP Address= 10.10.2.1
IP Subnet Mask= 255.255.255.0
RIP Direction= None
  Version= N/A
Multicast= IGMP-v2
Edit IP Alias= No

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

The DHCP and TCP/IP setup fields are the same as the ones in **Menu 3.2 - TCP/IP and DHCP Ethernet Setup**. Each public server will need a unique IP address. Refer to [Section 35.4 on page 527](#) for information on how to configure these fields.

**Note:** DMZ, WLAN and LAN IP addresses must be on separate subnets. You must also configure NAT for the DMZ port (see [Chapter 42 on page 562](#)) in menus 15.1 and 15.2.

### 37.3.2 IP Alias Setup

You must use menu 5.2 to configure the first network. Move the cursor to the **Edit IP Alias** field, press [SPACE BAR] to choose **Yes** and press [ENTER] to configure the second and third network.

Pressing [ENTER] opens **Menu 5.2.1 - IP Alias Setup**, as shown next.

**Figure 293** Menu 5.2.1: IP Alias Setup

```
Menu 5.2.1 - IP Alias Setup

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

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

Refer to [Table 199 on page 530](#) for instructions on configuring IP alias parameters.



# CHAPTER 38

## Route Setup

This chapter describes how to configure the ZyWALL's traffic redirect. This chapter applies to the ZyWALL 35 and ZyWALL 70.

### 38.1 Configuring Route Setup

From the main menu, enter 6 to open **Menu 6 - Route Setup**.

**Figure 294** Menu 6: Route Setup

```
Menu 6 - Route Setup

1. Route Assessment
2. Traffic Redirect
3. Route Failover

Enter Menu Selection Number:
```

### 38.2 Route Assessment

This menu allows you to configure traffic redirect properties.

**Figure 295** Menu 6.1: Route Assessment

```
Menu 6.1 - Route Assessment

Probing WAN 1 Check Point= Yes
  Use Default Gateway as Check Point= Yes
  Check Point= N/A
Probing WAN 2 Check Point= Yes
  Use Default Gateway as Check Point= Yes
  Check Point= N/A
Probing Traffic Redirection Check Point= No
  Use Default Gateway as Check Point= N/A
  Check Point= N/A

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



The following table describes the fields in this menu.

**Table 203** Menu 6.1: Route Assessment

FIELD	DESCRIPTION
Probing WAN 1/2 Check Point	Press [SPACE BAR] and then press [ENTER] to choose <b>Yes</b> to test your ZyWALL's WAN accessibility.  If you do not select <b>No</b> in the <b>Use Default Gateway as Check Point</b> field and enter a domain name or IP address of a reliable nearby computer (for example, your ISP's DNS server address) in the <b>Check Point</b> field, the ZyWALL will use the default gateway IP address.
Probing Traffic Redirection Check Point	Press [SPACE BAR] and then press [ENTER] to choose <b>Yes</b> to test your ZyWALL's traffic redirect connection.  If you do not select <b>No</b> in the <b>Use Default Gateway as Check Point</b> field and enter a domain name or IP address of a reliable nearby computer (for example, your ISP's DNS server address) in the <b>Check Point</b> field, the ZyWALL will use the default gateway IP address.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.	

### 38.3 Traffic Redirect

To configure the parameters for traffic redirect, enter **2** in **Menu 6 - Route Setup** to open **Menu 6.2 - Traffic Redirect** as shown next.

**Figure 296** Menu 6.2: Traffic Redirect

```

Menu 6.2 - Traffic Redirect

Active= No
Configuration:
Backup Gateway IP Address= 0.0.0.0
Metric= 14

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

The following table describes the fields in this menu.

**Table 204** Menu 6.2: Traffic Redirect

FIELD	DESCRIPTION
Active	Press [SPACE BAR] and select Yes (to enable) or No (to disable) traffic redirect setup. The default is No.
Backup Gateway IP Address	Enter the IP address of your backup gateway in dotted decimal notation. The ZyWALL automatically forwards traffic to this IP address if the ZyWALL's Internet connection terminates.

**Table 204** Menu 6.2: Traffic Redirect

FIELD	DESCRIPTION
Metric	This field sets this route's priority among the routes the ZyWALL uses. Enter a number from 1 to 15 to set this route's priority among the ZyWALL's routes (see <a href="#">Section 7.5 on page 134</a> ) The smaller the number, the higher priority the route has.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.	

## 38.4 Route Failover

This menu allows you to configure how the ZyWALL uses the route assessment ping check function.

**Figure 297** Menu 6.3: Route Failover

Menu 6.3 - Route Failover
Period= 5 Timeout=: 3 Fail Tolerance= 3
Press ENTER to Confirm or ESC to Cancel:

The following table describes the fields in this menu.

**Table 205** Menu 6.3: Route Failover

FIELD	DESCRIPTION
Period	Type the number of seconds for the ZyWALL to wait between checks to see if it can connect to the WAN IP address (in the <b>Check Point</b> field of menu 6.1) or the default gateway. Allow more time if your destination IP address handles lots of traffic.
Timeout	Type the number of seconds for your ZyWALL to wait for a ping response from the IP address in the <b>Check Point</b> field of menu 6.1 before it times out. The WAN connection is considered "down" after the ZyWALL times out the number of times specified in the <b>Fail Tolerance</b> field. Use a higher value in this field if your network is busy or congested.
Fail Tolerance	Type the number of times your ZyWALL may attempt and fail to connect to the Internet before traffic is forwarded to the backup gateway.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.	



# CHAPTER 39

## Wireless Setup

Use menu 7 to set up your ZyWALL as the wireless access point.

### 39.1 Wireless LAN Setup

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

From the main menu, enter 7 to open **Menu 7 - WLAN Setup** to configure the Wireless LAN setup. To edit the wireless LAN configuration, enter 1 to open **Menu 7.1 - Wireless Setup** as shown next.

**Figure 298** Menu 7.1: Wireless Setup

```
Menu 7.1 - Wireless Setup

Enable Wireless LAN= No
Bridge Channel= WLAN
ESSID= ZyXEL
Hide ESSID= No
Channel ID= CH06 2437MHz
RTS Threshold= 2432
Frag. Threshold= 2432
WEP= Disable
  Default Key= N/A
  Key1= N/A
  Key2= N/A
  Key3= N/A
  Key4= N/A
Edit MAC Address Filter= No

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

**Note:** The settings of all client stations on the wireless LAN must match those of the ZyWALL.

Follow the instructions in the next table on how to configure the wireless LAN parameters.

**Table 206** Menu 7.1: Wireless Setup

FIELD	DESCRIPTION
Enable Wireless LAN	Press [SPACE BAR] to select <b>Yes</b> to turn on the wireless LAN. The wireless LAN is off by default. Configure wireless LAN security features such as Mac filters and 802.1X before you turn on the wireless LAN.
Bridge Channel	Select <b>LAN</b> to use the wireless card as part of the LAN. Select <b>DMZ</b> to use the wireless card as part of the DMZ. Select <b>WLAN</b> to use the wireless card as part of the WLAN. The ZyWALL restarts after you change the wireless card setting.  <b>Note:</b> If you set the wireless card to be part of the LAN or DMZ, you can still use wireless access, but not the WLAN interface in the firewall. The firewall will treat the wireless card as part of the LAN or DMZ respectively.
ESSID	(Extended Service Set IDentification) The ESSID identifies the AP to which the wireless stations associate. Wireless stations associating to the Access Point must have the same ESSID. Enter a descriptive name (up to 32 characters) for the wireless LAN.
Hide ESSID	Press [SPACE BAR] to select <b>Yes</b> to hide the ESSID in the outgoing beacon frame so a station cannot obtain the ESSID through passive scanning.
Channel ID	This allows you to set the operating frequency/channel depending on your particular region. Use the [SPACE BAR] to select a channel.
RTS Threshold	(Request To Send) The threshold (number of bytes) for enabling RTS/CTS handshake. Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this attribute to be larger than the maximum MSDU (MAC service data unit) size turns off the RTS/CTS handshake. Setting this attribute to zero turns on the RTS/CTS handshake. Enter a value between <b>0</b> and <b>2432</b> .
Frag. Threshold	The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter a value between <b>256</b> and <b>2432</b> .
WEP	Select <b>Disable</b> to allow wireless stations to communicate with the access points without any data encryption. Select <b>64-bit WEP</b> or <b>128-bit WEP</b> to enable data encryption.
Default Key	Enter the key number (1 to 4) in this field. Only one key can be enabled at any one time. This key must be the same on the ZyWALL and the wireless stations to communicate.
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the ZyWALL and the wireless stations must use the same WEP key for data transmission. If you chose <b>64-bit WEP</b> in the <b>WEP Encryption</b> field, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose <b>128-bit WEP</b> in the <b>WEP Encryption</b> field, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F").  <b>Note:</b> Enter "0x" before the key to denote a hexadecimal key. Don't enter "0x" before the key to denote an ASCII key.
Edit MAC Address Filter	Press [SPACE BAR] to select <b>Yes</b> and then press [ENTER] to display menu 7.1.1.
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.	

### 39.1.1 MAC Address Filter Setup

Your ZyWALL checks the MAC address of the wireless station device against a list of allowed or denied MAC addresses. However, intruders could fake allowed MAC addresses so MAC-based authentication is less secure than EAP authentication.

Follow the steps below to create the MAC address table on your ZyWALL.

- 1 From the main menu, enter 7 to open **Menu 7 - WLAN Setup**.
- 2 Enter 1 to display **Menu 7.1 - Wireless Setup**.
- 3 In the **Edit MAC Address Filter** field, press [SPACE BAR] to select **Yes** and press [ENTER]. **Menu 7.1.1 - WLAN MAC Address Filter** displays as shown next.

**Figure 299** Menu 7.1.1: WLAN MAC Address Filter

```

Menu 7.1.1 - WLAN MAC Address Filter

Active= No
Filter Action= Allowed Association
MAC Address Filter
Address 1= 00:00:00:00:00:00
Address 2= 00:00:00:00:00:00
Address 3= 00:00:00:00:00:00
Address 4= 00:00:00:00:00:00
Address 5= 00:00:00:00:00:00
Address 6= 00:00:00:00:00:00
Address 7= 00:00:00:00:00:00
Address 8= 00:00:00:00:00:00
Address 9= 00:00:00:00:00:00
Address 10= 00:00:00:00:00:00
Address 11= 00:00:00:00:00:00
Address 12= 00:00:00:00:00:00

Enter here to CONFIRM or ESC to CANCEL:

```

The following table describes the fields in this menu.

**Table 207** Menu 7.1.1: WLAN MAC Address Filter

FIELD	DESCRIPTION
Active	To enable MAC address filtering, press [SPACE BAR] to select <b>Yes</b> and press [ENTER].
Filter Action	Define the filter action for the list of MAC addresses in the MAC address filter table. To deny access to the ZyWALL, press [SPACE BAR] to select <b>Deny Association</b> and press [ENTER]. MAC addresses not listed will be allowed to access the router. The default action, <b>Allowed Association</b> , permits association with the ZyWALL. MAC addresses not listed will be denied access to the router.
MAC Address Filter	

**Table 207** Menu 7.1.1: WLAN MAC Address Filter

FIELD	DESCRIPTION
Address 1..12	Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the client computers that are allowed or denied access to the ZyWALL in these address fields.
When you have completed this menu, press [ENTER] at the prompt [Press ENTER to Confirm...] to save your configuration, or press [ESC] at any time to cancel.	

## 39.2 TCP/IP Setup

For more detailed information about RIP setup, IP Multicast and IP alias, please refer to [Chapter 5 on page 110](#).

### 39.2.1 IP Address

From the main menu, enter 7 to open **Menu 7 - WLAN Setup** to configure TCP/IP (RFC 1155).

**Figure 300** Menu 7: WLAN Setup

Menu 7 - WLAN Setup
1. Wireless Setup
2. <b>TCP/IP and DHCP Setup</b>
Enter Menu Selection Number:

From menu 7, select the submenu option **2. TCP/IP and DHCP Setup** and press [ENTER]. The screen now displays **Menu 7.2 - TCP/IP and DHCP Ethernet Setup**, as shown next.

**Figure 301** Menu 7.2: TCP/IP and DHCP Ethernet Setup

```

Menu 7.2 - TCP/IP and DHCP Ethernet Setup

DHCP= None
Client IP Pool:
  Starting Address= N/A
  Size of Client IP Pool= N/A

DHCP Server Address= N/A

TCP/IP Setup:
IP Address= 0.0.0.0
IP Subnet Mask= 0.0.0.0
RIP Direction= None
  Version= N/A
Multicast= IGMP-v2
Edit IP Alias= No

Press ENTER to Confirm or ESC to Cancel:

```

The DHCP and TCP/IP setup fields are the same as the ones in **Menu 3.2 - TCP/IP and DHCP Ethernet Setup**. Each public server will need a unique IP address. Refer to [Section 35.4 on page 527](#) for information on how to configure these fields.

**Note:** DMZ, WLAN and LAN IP addresses must be on separate subnets. You must also configure NAT for the WLAN port (see [Chapter 42 on page 562](#)) in menus 15.1 and 15.2.

### 39.2.2 IP Alias Setup

You must use menu 7.2 to configure the first network. Move the cursor to the **Edit IP Alias** field, press [SPACE BAR] to choose **Yes** and press [ENTER] to configure the second and third network.

Pressing [ENTER] opens **Menu 7.2.1 - IP Alias Setup**, as shown next.



**Figure 302** Menu 7.2.1: IP Alias Setup

```
Menu 7.2.1 - IP Alias Setup

IP Alias 1= No
IP Address= N/A
IP Subnet Mask= N/A
RIP Direction= N/A
Version= N/A

IP Alias 2= No
IP Address= N/A
IP Subnet Mask= N/A
RIP Direction= N/A
Version= N/A

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

Refer to [Table 199 on page 530](#) for instructions on configuring IP alias parameters.

# CHAPTER 40

## Remote Node Setup

This chapter shows you how to configure a remote node.

### 40.1 Introduction to Remote Node Setup

A remote node is required for placing calls to a remote gateway. A remote node represents both the remote gateway and the network behind it across a WAN connection. Note that when you use menu 4 to set up Internet access, you are actually configuring a remote node. The following describes how to configure **Menu 11.x (where x is 1 or 2) - Remote Node Profile**, **Menu 11.x.2 - Remote Node Network Layer Options** and **Menu 11.x.4 - Remote Node Filter**.

### 40.2 Remote Node Setup

From the main menu, select menu option 11 to open **Menu 11 - Remote Node Setup** (shown below).

On a ZyWALL with multiple WAN ports, enter **1** or **2** to open **Menu 11.x - Remote Node Profile** and configure the setup for your first or second WAN port. Enter **3** to open **Menu 11.3 Remote Node Profile (Backup ISP)** and configure the setup for your Dial Backup port connection (see [Chapter 34 on page 514](#)).

On a ZyWALL with a single WAN port, enter **1** to open **Menu 11.1 - Remote Node Profile** and configure the setup for your WAN port. Enter **2** to open **Menu 11.2 Remote Node Profile (Backup ISP)** and configure the setup for your Dial Backup port connection.

**Figure 303** Menu 11: Remote Node Setup

```
Menu 11 - Remote Node Setup

1. WAN_1 (ISP, SUA)
2. WAN_2 (ISP, NAT)
3. -Dial (BACKUP_ISP, SUA)

Enter Node # to Edit:
```

## 40.3 Remote Node Profile Setup

The following explains how to configure the remote node profile menu. Not all fields are available on all models.

### 40.3.1 Ethernet Encapsulation

There are three variations of menu 11.x depending on whether you choose **Ethernet Encapsulation**, **PPPoE Encapsulation** or **PPTP Encapsulation**. You must choose the **Ethernet** option when the WAN port is used as a regular Ethernet. The first menu 11.x screen you see is for Ethernet encapsulation shown next.

**Figure 304** Menu 11.1: Remote Node Profile for Ethernet Encapsulation

```
Menu 11.1 - Remote Node Profile

Rem Node Name= WAN_1           Route= IP
Active= Yes

Encapsulation= Ethernet       Edit IP= No
Service Type= Standard        Session Options:
                                Schedules=
                                Edit Filter Sets= No

Outgoing:
  My Login= N/A
  My Password= N/A
  Retype to Confirm= N/A
  Server= N/A
  Relogin Every (min)= N/A

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

The following table describes the fields in this menu.

**Table 208** Menu 11.1: Remote Node Profile for Ethernet Encapsulation

FIELD	DESCRIPTION
Rem Node Name	Enter a descriptive name for the remote node. This field can be up to eight characters.
Active	Press [SPACE BAR] and then [ENTER] to select <b>Yes</b> (activate remote node) or <b>No</b> (deactivate remote node).
Encapsulation	<b>Ethernet</b> is the default encapsulation. Press [SPACE BAR] and then [ENTER] to change to <b>PPPoE</b> or <b>PPTP</b> encapsulation.
Service Type	Press [SPACE BAR] and then [ENTER] to select from <b>Standard</b> , <b>RR-Toshiba</b> (RoadRunner Toshiba authentication method), <b>RR-Manager</b> (RoadRunner Manager authentication method), <b>RR-Telstra</b> or <b>Telia Login</b> . Choose one of the RoadRunner methods if your ISP is Time Warner's RoadRunner; otherwise choose <b>Standard</b> .
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@poelc) to access the PPPoE server.
My Password	Enter the password assigned by your ISP when the ZyWALL calls this remote node. Valid for <b>PPPoE</b> encapsulation only.
Retype to Confirm	Type your password again to make sure that you have entered it correctly.
Server	This field is valid only when <b>RoadRunner</b> is selected in the <b>Service Type</b> field. The ZyWALL will find the RoadRunner Server IP automatically if this field is left blank. If it does not, then you must enter the authentication server IP address here.
Relogin Every (min)	This field is available when you select <b>Telia Login</b> in the <b>Service Type</b> field. The Telia server logs the ZyWALL out if the ZyWALL does not log in periodically. Type the number of minutes from 1 to 59 (30 recommended) for the ZyWALL to wait between logins.
Route	This field refers to the protocol that will be routed by your ZyWALL – IP is the only option for the ZyWALL.
Edit IP	This field leads to a "hidden" menu. Press [SPACE BAR] to select <b>Yes</b> and press [ENTER] to go to <b>Menu 11.x.2 - Remote Node Network Layer Options</b> .
Session Options	
Schedules	You can apply up to four schedule sets here. For more details please refer to <a href="#">Chapter 51 on page 648</a> .
Edit Filter Sets	This field leads to another "hidden" menu. Use [SPACE BAR] to select <b>Yes</b> and press [ENTER] to open menu 11.x.4 to edit the filter sets. See <a href="#">Section 40.5 on page 557</a> for more details.
Edit Traffic Redirect	Press [SPACE BAR] to select <b>Yes</b> or <b>No</b> . Select <b>No</b> (default) if you do not want to configure this feature. Select Yes and press [ENTER] to configure <b>Menu 11.1.5 - Traffic Redirect Setup</b> .
Once you have configured this menu, press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.	

## 40.3.2 PPPoE Encapsulation

The ZyWALL supports PPPoE (Point-to-Point Protocol over Ethernet). You can only use PPPoE encapsulation when you're using the ZyWALL with a DSL modem as the WAN device. If you change the Encapsulation to **PPPoE**, then you will see the next screen. Please see [Appendix F on page 702](#) for more information on PPPoE.

**Figure 305** Menu 11.1: Remote Node Profile for PPPoE Encapsulation

```

Menu 11.1 - Remote Node Profile

Rem Node Name= ChangeMe           Route= IP
Active= Yes

Encapsulation= PPPoE             Edit IP= No
Service Type= Standard          Telco Option:
Service Name=                   Allocated Budget (min)= 0
Outgoing:                       Period (hr)= 0
  My Login=                      Schedules=
  My Password= *****          Nailed-Up Connection= No
  Retype to Confirm= *****
  Authen= CHAP/PAP

                                   Session Options:
                                   Edit Filter Sets= No
                                   Idle Timeout(sec)= 100

Press ENTER to Confirm or ESC to Cancel:

```

### 40.3.2.1 Outgoing Authentication Protocol

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

### 40.3.2.2 Nailed-Up Connection

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

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

The following table describes the fields not already described in [Table 208 on page 552](#).

### 40.3.2.3 Metric

See [Section 7.5 on page 134](#) for details on the **Metric** field.

**Table 209** Fields in Menu 11.1 (PPPoE Encapsulation Specific)

FIELD	DESCRIPTION
Service Name	If you are using <b>PPPoE</b> encapsulation, then type the name of your PPPoE service here. Only valid with <b>PPPoE</b> encapsulation.
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.
Telco Option	
Allocated Budget	The field sets a ceiling for outgoing call time for this remote node. The default for this field is 0 meaning no budget control.
Period(hr)	This field is the time period that the budget should be reset. For example, if we are allowed to call this remote node for a maximum of 10 minutes every hour, then the <b>Allocated Budget</b> is (10 minutes) and the <b>Period(hr)</b> is 1 (hour).
Schedules	You can apply up to four schedule sets here. For more details please refer to <a href="#">Chapter 51 on page 648</a> .
Nailed-Up Connection	This field specifies if you want to make the connection to this remote node a nailed-up connection. More details are given earlier in this section.
Session Options	
Idle Timeout	Type the length of idle time (when there is no traffic from the ZyWALL to the remote node) in seconds that can elapse before the ZyWALL automatically disconnects the PPPoE connection. This option only applies when the ZyWALL initiates the call.

### 40.3.3 PPTP Encapsulation

If you change the Encapsulation to **PPTP** in menu 11.1, then you will see the next screen. Please see [Appendix G on page 704](#) for information on PPTP.

**Figure 306** Menu 11.1: Remote Node Profile for PPTP Encapsulation

```

Menu 11.1 - Remote Node Profile

Rem Node Name= ChangeMe           Route= IP
Active= Yes

Encapsulation= PPTP               Edit IP= No
Service Type= Standard            Telco Option:
                                   Allocated Budget (min)= 0
Outgoing:                          Period(hr)= 0
  My Login=                        Schedules=
  My Password= *****            Nailed-Up Connection= No
  Retype to Confirm= *****
  Authen= CHAP/PAP

PPTP:                               Session Options:
  My IP Addr= 10.0.0.140           Edit Filter Sets= No
  My IP Mask= 255.255.255.0       Idle Timeout(sec)= 100
  Server IP Addr= 10.0.0.138
  Connection ID/Name=

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

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

**Table 210** Menu 11.1: Remote Node Profile for PPTP Encapsulation

FIELD	DESCRIPTION
Encapsulation	Press [SPACE BAR] and then [ENTER] to select <b>PPTP</b> . You must also go to menu 11.3 to check the IP Address setting once you have selected the encapsulation method.
My IP Addr	Enter the IP address of the WAN Ethernet port.
My IP Mask	Enter the subnet mask of the WAN Ethernet port.
Server IP Addr	Enter the IP address of the ANT modem.
Connection ID/ Name	Enter the connection ID or connection name in the ANT. It must follow the "c:id" and "n:name" format. This field is optional and depends on the requirements of your DSL modem.
Schedules	You can apply up to four schedule sets here. For more details refer to <a href="#">Chapter 51 on page 648</a> .
Nailed-Up Connections	Press [SPACE BAR] and then [ENTER] to select <b>Yes</b> if you want to make the connection to this remote node a nailed-up connection.

## 40.4 Edit IP

Move the cursor to the **Edit IP** field in menu 11.1, then press [SPACE BAR] to select **Yes**. Press [ENTER] to open **Menu 11.1.2 - Remote Node Network Layer Options**. Not all fields are available on all models.

**Figure 307** Menu 11.1.2: Remote Node Network Layer Options for Ethernet Encapsulation

```

Menu 11.1.2 - Remote Node Network Layer Options

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

Network Address Translation= SUA Only
NAT Lookup Set= 255
Metric= 1
Private= No
RIP Direction= None
    Version= N/A
Multicast= None

Enter here to CONFIRM or ESC to CANCEL:

```

This menu displays the **My WAN Addr** field for **PPPoE** and **PPTP** encapsulations and **Gateway IP Addr** field for **Ethernet** encapsulation. The following table describes the fields in this menu.

**Table 211** Remote Node Network Layer Options Menu Fields

FIELD	DESCRIPTION
IP Address Assignment	If your ISP did not assign you an explicit IP address, press [SPACE BAR] and then [ENTER] to select <b>Dynamic</b> ; otherwise select <b>Static</b> and enter the IP address & subnet mask in the following fields.
(Rem) IP Address	If you have a static IP Assignment, enter the IP address assigned to you by your ISP.
(Rem) IP Subnet Mask	If you have a static IP Assignment, enter the subnet mask assigned to you.
Gateway IP Addr	This field is applicable to <b>Ethernet</b> encapsulation only. Enter the gateway IP address assigned to you if you are using a static IP address.
My WAN Addr	This field is applicable to <b>PPPoE</b> and <b>PPTP</b> encapsulations only. Some implementations, especially the UNIX derivatives, require the WAN link to have a separate IP network number from the LAN and each end must have a unique address within the WAN network number. If this is the case, enter the IP address assigned to the WAN port of your ZyWALL. Note that this is the address assigned to your local ZyWALL, not the remote router.
Network Address Translation	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet). Choose <b>None</b> to disable NAT. Choose <b>SUA Only</b> if you have a single public IP address. SUA (Single User Account) is a subset of NAT that supports two types of mapping: <b>Many-to-One</b> and <b>Server</b> . Choose <b>Full Feature</b> if you have multiple public IP addresses. <b>Full Feature</b> mapping types include: <b>One-to-One</b> , <b>Many-to-One</b> (SUA/PAT), <b>Many-to-Many Overload</b> , <b>Many- One-to-One</b> and <b>Server</b> . When you select <b>Full Feature</b> you must configure at least one address mapping set. See <a href="#">Chapter 22 on page 374</a> for a full discussion on this feature.



**Table 211** Remote Node Network Layer Options Menu Fields (continued)

FIELD	DESCRIPTION
NAT Lookup Set	If you select <b>SUA Only</b> in the <b>Network Address Translation</b> field, it displays <b>255</b> and indicates the SMT will use the pre-configured <b>Set 255</b> (read only) in menu 15.1. If you select <b>Full Feature</b> or <b>None</b> in the <b>Network Address Translation</b> field, it displays <b>1</b> , <b>2</b> or <b>3</b> and indicates the SMT will use the pre-configured <b>Set 1</b> in menu 15.1 for the first WAN port, <b>Set 2</b> in menu 15.1 for the second WAN port and <b>Set 3</b> for the Backup port. Refer to <a href="#">Section 42.2 on page 564</a> for more information.
Metric	Enter a number from 1 to 15 to set this route's priority among the ZyWALL's routes (see <a href="#">Section 7.5 on page 134</a> ). The smaller the number, the higher priority the route has.
Private	This field is valid only for PPTP/PPPoE encapsulation. This parameter determines if the ZyWALL will include the route to this remote node in its RIP broadcasts. If set to <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.
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP direction from <b>Both/ None/In Only/Out Only</b> . See <a href="#">Chapter 5 on page 110</a> 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.
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version from <b>RIP-1/RIP-2B/RIP-2M</b> or <b>None</b> .
Multicast	IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group. The ZyWALL supports both IGMP version 1 ( <b>IGMP-v1</b> ) and version 2 ( <b>IGMP-v2</b> ). Press [SPACE BAR] to enable IP Multicasting or select <b>None</b> to disable it. See <a href="#">Chapter 5 on page 110</a> for more information on this feature.
Once you have completed filling in <b>Menu 11.3 Remote Node Network Layer Options</b> , press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration and return to menu 11, or press [ESC] at any time to cancel.	

## 40.5 Remote Node Filter

Move the cursor to the field **Edit Filter Sets** in menu 11.1, and then press [SPACE BAR] to set the value to **Yes**. Press [ENTER] to open **Menu 11.1.4 - Remote Node Filter**.

Use menu 11.1.4 to specify the filter set(s) to apply to the incoming and outgoing traffic between this remote node and the ZyWALL to prevent certain packets from triggering calls. You can specify up to 4 filter sets separated by commas, for example, 1, 5, 9, 12, in each filter field. Note that spaces are accepted in this field. For more information on defining the filters, please refer to [Chapter 44 on page 584](#). For PPPoE or PPTP encapsulation, you have the additional option of specifying remote node call filter sets.

**Figure 308** Menu 11.1.4: Remote Node Filter (Ethernet Encapsulation)

```
Menu 11.1.4 - Remote Node Filter

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

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

**Figure 309** Menu 11.1.4: Remote Node Filter (PPPoE or PPTP Encapsulation)

```
Menu 11.1.4 - Remote Node Filter

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

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

## 40.6 Traffic Redirect

Configure parameters that determine when the ZyWALL will forward WAN traffic to the backup gateway using **Menu 11.1.5 - Traffic Redirect Setup**. This section applies to the ZyWALL 5.

**Figure 310** Menu 11.1.5: Traffic Redirect Setup

```

Menu 11.1.5 - Traffic Redirect Setup

Active= Yes
Configuration:
  Backup Gateway IP Address= 0.0.0.0
  Metric= 14
  Check WAN IP Address= 0.0.0.0
    Fail Tolerance= 10
    Period(sec)= 300
    Timeout(sec)= 8

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

The following table describes the fields in this menu.

**Table 212** Menu 11.1.5: Traffic Redirect Setup

FIELD	DESCRIPTION
Active	Press [SPACE BAR] and select Yes (to enable) or No (to disable) traffic redirect setup. The default is No.
Configuration	
Backup Gateway IP Address	Enter the IP address of your backup gateway in dotted decimal notation. The ZyWALL automatically forwards traffic to this IP address if the ZyWALL's Internet connection terminates.
Metric	This field sets this route's priority among the routes the ZyWALL uses. Enter a number from 1 to 15 to set this route's priority among the ZyWALL's routes (see <a href="#">Section 7.2 on page 130</a> in <a href="#">Chapter 7 on page 130</a> ) The smaller the number, the higher priority the route has.
Check WAN IP Address	Enter the IP address of a reliable nearby computer (for example, your ISP's DNS server address) to test your ZyWALL's WAN accessibility. The ZyWALL uses the default gateway IP address if you do not enter an IP address here. If you are using PPTP or PPPoE Encapsulation, enter "0.0.0.0" to configure the ZyWALL to check the PVC (Permanent Virtual Circuit) or PPTP tunnel.
Fail Tolerance	Enter the number of times your ZyWALL may attempt and fail to connect to the Internet before traffic is forwarded to the backup gateway. Two to five is usually a good number.
Period(sec)	Enter the time interval (in seconds) between WAN connection checks. Five to 60 is usually a good number.
Timeout(sec)	Enter the number of seconds the ZyWALL waits for a ping response from the IP Address in the <b>Check WAN IP Address</b> field before it times out. The number in this field should be less than the number in the <b>Period</b> field. Three to 50 is usually a good number. The WAN connection is considered "down" after the ZyWALL times out the number of times specified in the <b>Fail Tolerance</b> field.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.	

# CHAPTER 41

## IP Static Route Setup

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

### 41.1 IP Static Route Setup

Enter 12 from the main menu. Select one of the IP static routes as shown next to configure IP static routes in menu 12.1.

**Note:** The first two static route entries are for default WAN1 and WAN2 routes on a ZyWALL with multiple WAN ports; the first static route entry is for the default WAN route on a ZyWALL with a single WAN port. You cannot modify or delete a static default route. The name of the default static route is left blank unless you configure a static WAN IP address. The route name changes from “default” to “-default” after you change the static WAN IP address to a dynamic WAN IP address, indicating the static route is inactive.

**Figure 311** Menu 12: IP Static Route Setup

Menu 12 - IP Static Route Setup

1. Reserved	16. _____	31. _____	46. _____
2. Reserved	17. _____	32. _____	47. _____
3. _____	18. _____	33. _____	48. _____
4. _____	19. _____	34. _____	49. _____
5. _____	20. _____	35. _____	50. _____
6. _____	21. _____	36. _____	
7. _____	22. _____	37. _____	
8. _____	23. _____	38. _____	
9. _____	24. _____	39. _____	
10. _____	25. _____	40. _____	
11. _____	26. _____	41. _____	
12. _____	27. _____	42. _____	
13. _____	28. _____	43. _____	
14. _____	29. _____	44. _____	
15. _____	30. _____	45. _____	

Enter selection number:

Now, enter the index number of the static route that you want to configure.

**Figure 312** Menu 12. 1: Edit IP Static Route

```

Menu 12.1 - Edit IP Static Route

Route #: 3
Route Name= ?
Active= No
Destination IP Address= ?
IP Subnet Mask= ?
Gateway IP Address= ?
Metric= 2
Private= No

Press ENTER to CONFIRM or ESC to CANCEL:

```

The following table describes the IP Static Route Menu fields.

**Table 213** Menu 12. 1: Edit IP Static Route

FIELD	DESCRIPTION
Route #	This is the index number of the static route that you chose in menu 12.
Route Name	Enter a descriptive name for this route. This is for identification purposes only.
Active	This field allows you to activate/deactivate this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask for this destination.
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your ZyWALL that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your ZyWALL; over the WAN, the gateway must be the IP address of one of the remote nodes.
Metric	Enter a number from 1 to 15 to set this route's priority among the ZyWALL's routes (see <a href="#">Section 7.5 on page 134</a> ). The smaller the number, the higher priority the route has.
Private	This parameter determines if the ZyWALL will include the route to this remote node in its RIP broadcasts. If set to <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 42

## Network Address Translation (NAT)

This chapter discusses how to configure NAT on the ZyWALL.

### 42.1 Using NAT

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

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

SUA (Single User Account) is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. See [Section 42.2.1 on page 565](#) for a detailed description of the NAT set for SUA. The ZyWALL also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types.

**Note:** Choose **SUA Only** if you have just one public WAN IP address for your ZyWALL.

Choose **Full Feature** if you have multiple public WAN IP addresses for your ZyWALL.

#### 42.1.2 Applying NAT

You apply NAT via menus 4 or 11.1.2 as displayed next. The next figure shows you how to apply NAT for Internet access in menu 4. Enter 4 from the main menu to go to **Menu 4 - Internet Access Setup**.

**Figure 313** Menu 4: Applying NAT for Internet Access

```
Menu 4 - Internet Access Setup

ISP's Name= ChangeMe
Encapsulation= Ethernet
  Service Type= Standard
My Login= N/A
My Password= N/A
Retype to Confirm= N/A
Login Server= N/A
Relogin Every (min)= N/A
IP Address Assignment= Dynamic
  IP Address= N/A
  IP Subnet Mask= N/A
  Gateway IP Address= N/A
Network Address Translation= SUA Only

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

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

- 1 Enter 11 from the main menu.
- 2 Enter 1 to open **Menu 11.1 - Remote Node Profile**.
- 3 Move the cursor to the **Edit IP** field, press [SPACE BAR] to select **Yes** and then press [ENTER] to bring up **Menu 11.1.2 - Remote Node Network Layer Options**.

**Figure 314** Menu 11.1.2: Applying NAT to the Remote Node

```
Menu 11.1.2 - Remote Node Network Layer Options

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

Network Address Translation= Full Feature
NAT Lookup Set= 1
Metric= 1
Private= N/A
RIP Direction= None
  Version= N/A
Multicast= None

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

The following table describes the fields in this menu.

**Table 214** Applying NAT in Menus 4 & 11.1.2

FIELD	DESCRIPTION	OPTIONS
Network Address Translation	When you select this option the SMT will use Address Mapping Set 1 (menu 15.1 - see <a href="#">Section 42.2.1 on page 565</a> for further discussion). You can configure any of the mapping types described in <a href="#">Chapter 22 on page 374</a> . Choose <b>Full Feature</b> if you have multiple public WAN IP addresses for your ZyWALL.  When you select <b>Full Feature</b> you must configure at least one address mapping set.	Full Feature
	NAT is disabled when you select this option.	None
	When you select this option the SMT will use Address Mapping Set 255 (menu 15.1 - see <a href="#">Section 42.2.1 on page 565</a> ). Choose <b>SUA Only</b> if you have just one public WAN IP address for your ZyWALL.	SUA Only

## 42.2 NAT Setup

Use the address mapping sets menus and submenus to create the mapping table used to assign global addresses to computers on the LAN and the DMZ. **Set 255** is used for SUA. When you select **Full Feature** in menu 4, menu 11.1.2 or menu 11.2.2, the SMT will use **Set 1** for the first WAN port and **Set 2** for the second WAN port. When you select **SUA Only**, the SMT will use the pre-configured **Set 255** (read only).

The server set is a list of LAN and DMZ servers mapped to external ports. To use this set, a server rule must be set up inside the NAT address mapping set. Please see the section on port forwarding in [Chapter 22 on page 374](#) for further information on these menus. To configure NAT, enter 15 from the main menu to bring up the following screen.

**Note:** On a ZyWALL with two WAN ports, you can configure port forwarding and trigger port rules for the first WAN port and separate sets of rules for the second WAN port.

**Figure 315** Menu 15: NAT Setup

```

Menu 15 - NAT Setup

1. Address Mapping Sets
2. Port Forwarding Setup
3. Trigger Port Setup

Enter Menu Selection Number:

```

**Note:** Configure DMZ, WLAN and LAN IP addresses in NAT menus 15.1 and 15.2. DMZ, WLAN and LAN IP addresses must be on separate subnets.



## 42.2.1 Address Mapping Sets

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

**Figure 316** Menu 15.1: Address Mapping Sets

```

Menu 15.1 - Address Mapping Sets

    1. NAT_SET
    2. example
    255. SUA (read only)

Enter Menu Selection Number:
    
```

### 42.2.1.1 SUA Address Mapping Set

Enter 255 to display the next screen (see also [Section 42.1.1 on page 562](#)). The fields in this menu cannot be changed.

**Figure 317** Menu 15.1.255: SUA Address Mapping Rules

```

Menu 15.1.1 - Address Mapping Rules

Set Name= SUA

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

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

The following table explains the fields in this menu.

**Note:** Menu 15.1.255 is read-only.

**Table 215** SUA Address Mapping Rules

FIELD	DESCRIPTION
Set Name	This is the name of the set you selected in menu 15.1 or enter the name of a new set you want to create.
Idx	This is the index or rule number.
Local Start IP	<b>Local Start IP</b> is the starting local IP address (ILA).
Local End IP	<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.
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> .
Global End IP	This is the ending global IP address (IGA).
Type	These are the mapping types discussed above. <b>Server</b> allows us to specify multiple servers of different types behind NAT to this machine. See later for some examples.
Once you have finished configuring a rule in this menu, press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration, or press [ESC] to cancel.	

#### 42.2.1.2 User-Defined Address Mapping Sets

Now look at option 1 in menu 15.1. Enter 1 to bring up this menu. Look at the differences from the previous menu. Note the extra **Action** and **Select Rule** fields mean you can configure rules in this screen. Note also that the [?] in the **Set Name** field means that this is a required field and you must enter a name for the set.

**Note:** The entire set will be deleted if you leave the Set Name field blank and press [ENTER] at the bottom of the screen.

**Figure 318** Menu 15.1.1: First Set

```

Menu 15.1.1 - Address Mapping Rules

Set Name= NAT_SET

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

Action= None          Select Rule= N/A

Press ENTER to Confirm or ESC to Cancel:

```

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

### 42.2.1.3 Ordering Your Rules

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

Now if you delete rule 4, rules 5 to 7 will be pushed up by 1 rule, so as old rule 5 becomes rule 4, old rule 6 becomes rule 5 and old rule 7 becomes rule 6.

**Table 216** Fields in Menu 15.1.1

FIELD	DESCRIPTION
Set Name	Enter a name for this set of rules. This is a required field. If this field is left blank, the entire set will be deleted.
Action	The default is <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.
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.

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

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

**Note:** An IP End address must be numerically greater than its corresponding IP Start address.

**Figure 319** Menu 15.1.1.1: Editing/Configuring an Individual Rule in a Set

```

Menu 15.1.1.1 Address Mapping Rule

Type= One-to-One

Local IP:
  Start=
  End  = N/A

Global IP:
  Start=
  End  = N/A

Server Mapping Set= N/A

Press ENTER to Confirm or ESC to Cancel:

```

The following table describes the fields in this menu.

**Table 217** Menu 15.1.1.1: Editing/Configuring an Individual Rule in a Set

FIELD	DESCRIPTION
Type	Press [SPACE BAR] and then [ENTER] to select from a total of five types. These are the mapping types discussed in <a href="#">Chapter 22 on page 374</a> . <b>Server</b> allows you to specify multiple servers of different types behind NAT to this computer. See <a href="#">Section 42.4.3 on page 574</a> for an example.
Local IP	Only local IP fields are <b>N/A</b> for server; Global IP fields <b>MUST</b> be set for <b>Server</b> .
Start	Enter the starting local IP address (ILA).
End	Enter the ending local IP address (ILA). If the rule is for all local IPs, then put the Start IP as 0.0.0.0 and the End IP as 255.255.255.255. This field is <b>N/A</b> for One-to-One and Server types.
Global IP	
Start	Enter the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the <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 <b>Many-to-One</b> or <b>Server</b> .
End	Enter 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</b> types.

**Table 217** Menu 15.1.1.1: Editing/Configuring an Individual Rule in a Set

FIELD	DESCRIPTION
Server Mapping Set	This field is available only when you select <b>Server</b> in the <b>Type</b> field.
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.	

## 42.3 Configuring a Server behind NAT

**Note:** If you do not assign a **Default Server** IP address, the ZyWALL discards all packets received for ports that are not specified here or in the remote management setup.

Follow these steps to configure a server behind NAT:

- 1 Enter 15 in the main menu to go to **Menu 15 - NAT Setup**.
- 2 Enter 2 to open menu 15.2 (and configure the address mapping rules for the WAN port on a ZyWALL with a single WAN port).

**Figure 320** Menu 15.2: NAT Server Sets

Menu 15.2 - NAT Server Sets
1. Server Set 1 2. Server Set 2
Enter Set Number to Edit:

- 3 Enter 1 or 2 to go to **Menu 15.2.x - NAT Server Setup** and configure the address mapping rules for the WAN 1 or WAN 2 port on a ZyWALL with multiple WAN ports.

**Figure 321** Menu 15.2.1: NAT Server Sets

```
Menu 15.2.1 - NAT Server Setup

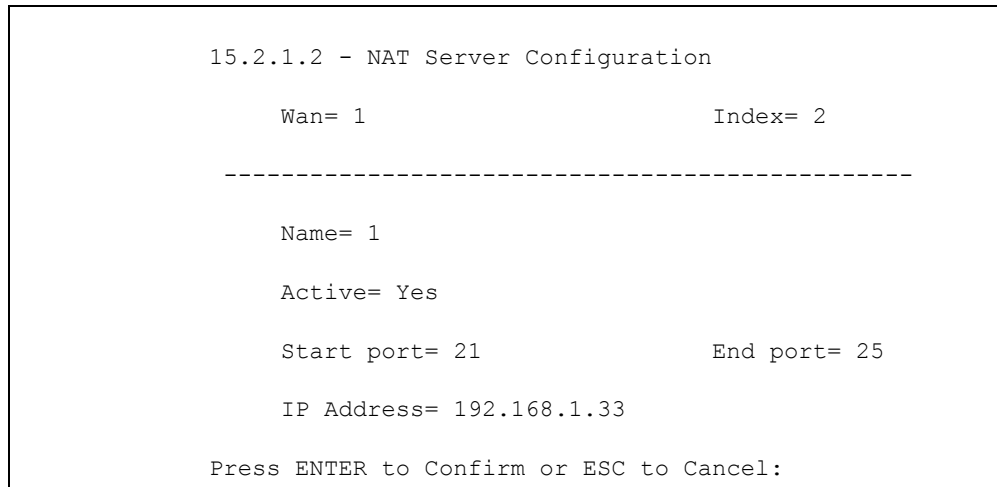
Default Server: 0.0.0.0

Rule  Act.  Start Port  End Port  IP Address
-----
001   No     0           0         0.0.0.0
002   No     0           0         0.0.0.0
003   No     0           0         0.0.0.0
004   No     0           0         0.0.0.0
005   No     0           0         0.0.0.0
006   No     0           0         0.0.0.0
007   No     0           0         0.0.0.0
008   No     0           0         0.0.0.0
009   No     0           0         0.0.0.0
010   No     0           0         0.0.0.0

Select Command= None           Select Rule= N/A
Press ENTER to Confirm or ESC to Cancel:
```

- 4 Select **Edit Rule** in the **Select Command** field; type the index number of the NAT server you want to configure in the **Select Rule** field and press [ENTER] to open **Menu 15.2.1.2 - NAT Server Configuration** (see the next figure).

**Figure 322** 15.2.1.2: NAT Server Configuration



The following table describes the fields in this screen.

**Table 218** 15.2.1.2: NAT Server Configuration

FIELD	DESCRIPTION
WAN	On a ZyWALL with two WAN ports, you can configure port forwarding and trigger port rules for the first WAN port and separate sets of rules for the second WAN port. This is the WAN port (server set) you select in menu 15.2.
Index	This is the index number of an individual port forwarding server entry.
Name	Enter a name to identify this port-forwarding rule.
Active	Press [SPACE BAR] and then [ENTER] to select <b>Yes</b> to enable the NAT server entry.
Start Port	Enter a port number in the <b>Start Port</b> field. To forward only one port, enter it again in the <b>End Port</b> field. To specify a range of ports, enter the last port to be forwarded in the <b>End Port</b> field.
End Port	
IP Address	Enter the inside IP address of the server.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.	

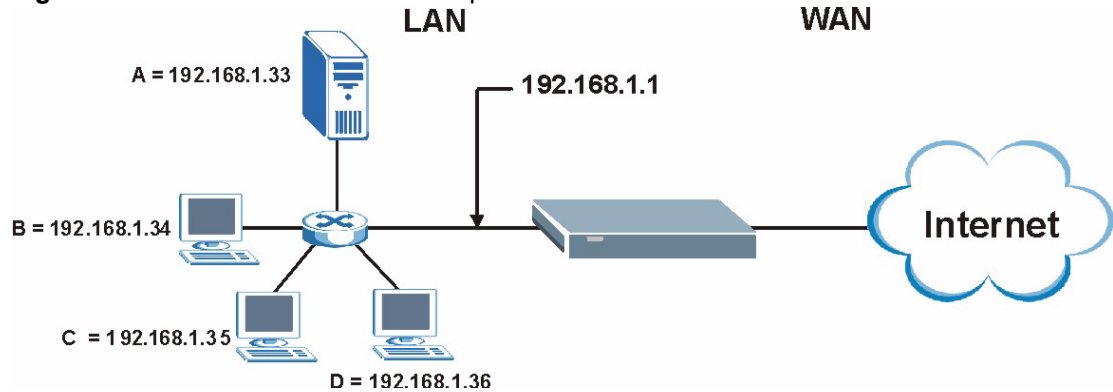
- 5** Enter a port number in the **Start Port** field. To forward only one port, enter it again in the **End Port** field. To specify a range of ports, enter the last port to be forwarded in the **End Port** field.
- 6** Enter the inside IP address of the server in the **IP Address** field. In the following figure, you have a computer acting as an FTP, Telnet and SMTP server (ports 21, 23 and 25) at 192.168.1.33.
- 7** Press [ENTER] at the "Press ENTER to confirm ..." prompt to save your configuration after you define all the servers or press [ESC] at any time to cancel.

**Figure 323** Menu 15.2.1: NAT Server Setup

Menu 15.2.1 - NAT Server Setup				
Default Server: 0.0.0.0				
Rule	Act.	Start Port	End Port	IP Address
001	No	0	0	0.0.0.0
002	Yes	21	25	192.168.1.33
003	No	0	0	0.0.0.0
004	No	0	0	0.0.0.0
005	No	0	0	0.0.0.0
006	No	0	0	0.0.0.0
007	No	0	0	0.0.0.0
008	No	0	0	0.0.0.0
009	No	0	0	0.0.0.0
010	No	0	0	0.0.0.0

Select Command= None                      Select Rule= N/A  
Press ENTER to Confirm or ESC to Cancel:

You assign the private network IP addresses. The NAT network appears as a single host on the Internet. A is the FTP/Telnet/SMTP server.

**Figure 324** Server Behind NAT Example

## 42.4 General NAT Examples

The following are some examples of NAT configuration.

### 42.4.1 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 325 NAT Example 1

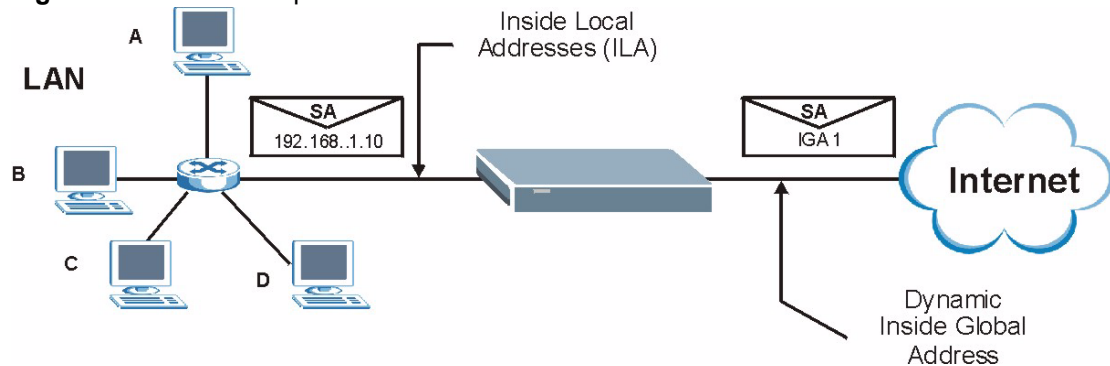


Figure 326 Menu 4: Internet Access &amp; NAT Example

```

Menu 4 - Internet Access Setup

ISP's Name= ChangeMe
Encapsulation= Ethernet
  Service Type= Standard
  My Login= N/A
  My Password= N/A
  Retype to Confirm= N/A
  Login Server= N/A
  Relogin Every (min)= N/A
IP Address Assignment= Dynamic
  IP Address= N/A
  IP Subnet Mask= N/A
  Gateway IP Address= N/A
Network Address Translation= SUA Only

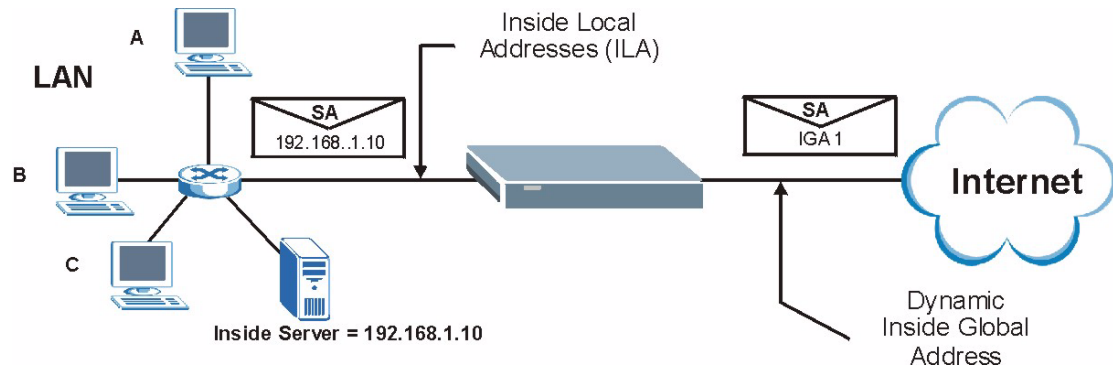
Press ENTER to Confirm or ESC to Cancel:

```

From menu 4 shown above, simply choose the **SUA Only** option from the **Network Address Translation** field. This is the Many-to-One mapping discussed in [Section 42.4 on page 572](#). 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.

## 42.4.2 Example 2: Internet Access with an Default Server

Figure 327 NAT Example 2



In this case, you do exactly as above (use the convenient pre-configured **SUA Only** set) and also go to menu 15.2.1 to specify the **Default Server** behind the NAT as shown in the next figure.

Figure 328 Menu 15.2.1: Specifying an Inside Server

Menu 15.2.1 - NAT Server Setup				
Default Server: 192.168.1.10				
Rule	Act.	Start Port	End Port	IP Address
001	No	0	0	0.0.0.0
002	Yes	21	25	192.168.1.33
003	No	0	0	0.0.0.0
004	No	0	0	0.0.0.0
005	No	0	0	0.0.0.0
006	No	0	0	0.0.0.0
007	No	0	0	0.0.0.0
008	No	0	0	0.0.0.0
009	No	0	0	0.0.0.0
010	No	0	0	0.0.0.0

Select Command= None                      Select Rule= N/A  
Press ENTER to Confirm or ESC to Cancel:

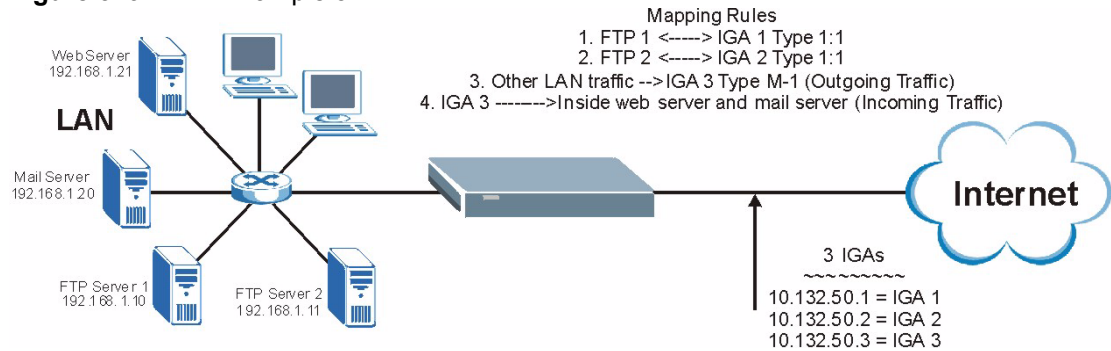
## 42.4.3 Example 3: Multiple Public IP Addresses With Inside Servers

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

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

The example situation looks somewhat like this:

**Figure 329 NAT Example 3**



- 1 In this case you need to configure Address Mapping Set 1 from **Menu 15.1 - Address Mapping Sets**. Therefore you must choose the **Full Feature** option from the **Network Address Translation** field (in menu 4 or menu 11.3) in [Figure 330 on page 576](#).
- 2 Then enter 15 from the main menu.
- 3 Enter 1 to configure the Address Mapping Sets.
- 4 Enter 1 to begin configuring this new set. Enter a Set Name, choose the **Edit Action** and then enter 1 for the **Select Rule** field. Press [ENTER] to confirm.
- 5 Select **Type** as **One-to-One** (direct mapping for packets going both ways), and enter the local **Start IP** as 192.168.1.10 (the IP address of FTP Server 1), the global **Start IP** as 10.132.50.1 (our first IGA). (See [Figure 331 on page 576](#)).
- 6 Repeat the previous step for rules 2 to 4 as outlined above.
- 7 When finished, menu 15.1.1 should look like as shown in [Figure 332 on page 577](#).

**Figure 330** Example 3: Menu 11.1.2

```
Menu 11.1.2 - Remote Node Network Layer Options

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

Network Address Translation= SUA Only
Metric= 2
Private=
RIP Direction= None
    Version= N/A
Multicast= None

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

The following figure shows how to configure the first rule.

**Figure 331** Example 3: Menu 15.1.1.1

```
Menu 15.1.1.1 Address Mapping Rule

Type= One-to-One

Local IP:
    Start= 192.168.1.10
    End = N/A

Global IP:
    Start= 10.132.50.1
    End = N/A

Server Mapping Set= N/A

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

**Figure 332** Example 3: Final Menu 15.1.1

```

Menu 15.1.1 - Address Mapping Rules

Set Name= Example3

Idx  Local Start IP  Local End IP  Global Start IP  Global End IP  Type
---  -
1.  192.168.1.10      10.132.50.1    1-1
2.  192.168.1.11      10.132.50.2    1-1
3.  0.0.0.0           255.255.255.255  10.132.50.3    M-1
4.                                     10.132.50.3    Server
5.
6.
7.
8.
9.
10.

Action= Edit      Select Rule=

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

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

- 1 Enter 15 from the main menu.
- 2 Enter 2 to go to menu 15.2.
- 3 (Enter 1 or 2 from menu 15.2 on a ZyWALL with multiple WAN ports) configure the menu as shown in [Figure 333 on page 577](#).

**Figure 333** Example 3: Menu 15.2.1

```

Menu 15.2.1 - NAT Server Setup

Default Server: 0.0.0.0

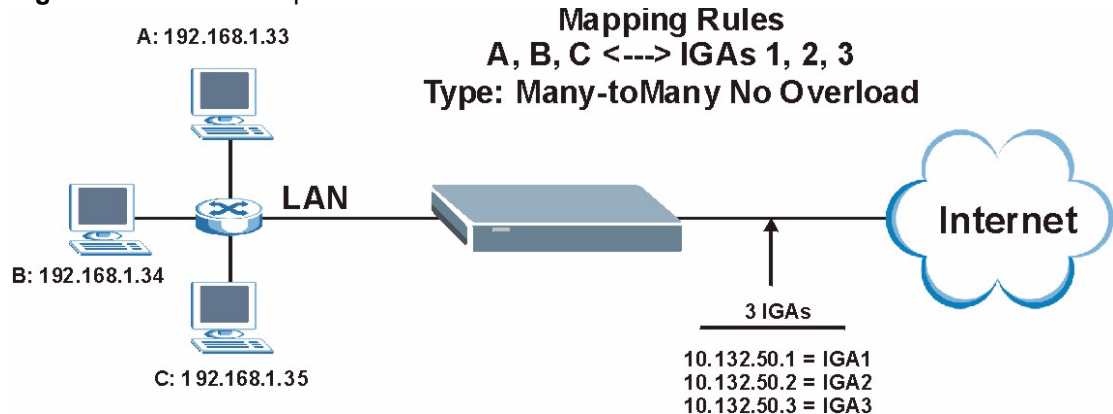
Rule  Act.  Start Port  End Port  IP Address
-----
001  Yes   80          80        192.168.1.21
002  Yes   25          25        192.168.1.20
003  No    0           0         0.0.0.0
004  No    0           0         0.0.0.0
005  No    0           0         0.0.0.0
006  No    0           0         0.0.0.0
007  No    0           0         0.0.0.0
008  No    0           0         0.0.0.0
009  No    0           0         0.0.0.0
010  No    0           0         0.0.0.0

Select Command= None      Select Rule= N/A
Press ENTER to Confirm or ESC to Cancel:
    
```

## 42.4.4 Example 4: NAT Unfriendly Application Programs

Some applications do not support NAT Mapping using TCP or UDP port address translation. In this case it is better to use **Many-One-to-One** mapping as port numbers do *not* change for **Many-One-to-One** (and **One-to-One**) NAT mapping types. The following figure illustrates this.

**Figure 334** NAT Example 4



**Note:** Other applications such as some gaming programs are NAT unfriendly because they embed addressing information in the data stream. These applications won't work through NAT even when using **One-to-One** and **Many-One-to-One** mapping types.

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

**Figure 335** Example 4: Menu 15.1.1.1: Address Mapping Rule

```

Menu 15.1.1.1 Address Mapping Rule

Type= Many-One-to-One

Local IP:
  Start= 192.168.1.10
  End  = 192.168.1.12

Global IP:
  Start= 10.132.50.1
  End  = 10.132.50.3

Press ENTER to Confirm or ESC to Cancel:

```

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

**Figure 336** Example 4: Menu 15.1.1: Address Mapping Rules

Menu 15.1.1 - Address Mapping Rules					
Set Name= Example4					
Idx	Local Start IP	Local End IP	Global Start IP	Global End IP	Type
1.	192.168.1.10	192.168.1.12	10.132.50.1	10.132.50.3	M-1-1
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					

Action= Edit                      Select Rule=

Press ENTER to Confirm or ESC to Cancel:

## 42.5 Trigger Port Forwarding

Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address.

Trigger port forwarding solves this problem by allowing computers on the LAN to dynamically take turns using the service. The ZyWALL records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a "trigger" port). When the ZyWALL's WAN port receives a response with a specific port number and protocol ("incoming" port), the ZyWALL forwards the traffic to the LAN IP address of the computer that sent the request. After that computer's connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

### 42.5.1 Two Points To Remember About Trigger Ports

- 1 Trigger events only happen on data that is going coming from inside the ZyWALL and going to the outside.
- 2 If an application needs a continuous data stream, that port (range) will be tied up so that another computer on the LAN can't trigger it.

**Note:** Only one LAN computer can use a trigger port (range) at a time.

Enter 3 in menu 15 to display **Menu 15.3 - Trigger Ports**. For a ZyWALL with multiple WAN ports, enter 1 or 2 from menu 15.3 to go to **Menu 15.3.1** or **Menu 15.3.2 - Trigger Port Setup** and configure trigger port rules for the first or second WAN port.

**Figure 337** Menu 15.3.1: Trigger Port Setup

Menu 15.3.1 - Trigger Port Setup						
Rule	Name	Incoming		Trigger		
		Start Port	End Port	Start Port	End Port	
1.	<b>Real Audio</b>	<b>6970</b>	<b>7170</b>	<b>7070</b>	<b>7070</b>	
2.		0	0	0	0	
3.		0	0	0	0	
4.		0	0	0	0	
5.		0	0	0	0	
6.		0	0	0	0	
7.		0	0	0	0	
8.		0	0	0	0	
9.		0	0	0	0	
10.		0	0	0	0	
11.		0	0	0	0	
12.		0	0	0	0	

Press ENTER to Confirm or ESC to Cancel:

HTTP:80 FTP:21 Telnet:23 SMTP:25 POP3:110 PPTP:1723

The following table describes the fields in this menu.

**Table 219** Menu 15.3.1: Trigger Port Setup

FIELD	DESCRIPTION
Rule	This is the rule index number.
Name	Enter a unique name for identification purposes. You may enter up to 15 characters in this field. All characters are permitted - including spaces.
Incoming	Incoming is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The ZyWALL forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.
Start Port	Enter a port number or the starting port number in a range of port numbers.
End Port	Enter a port number or the ending port number in a range of port numbers.
Trigger	The trigger port is a port (or a range of ports) that causes (or triggers) the ZyWALL to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Start Port	Enter a port number or the starting port number in a range of port numbers.
End Port	Enter a port number or the ending port number in a range of port numbers.
Press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.	





# CHAPTER 43

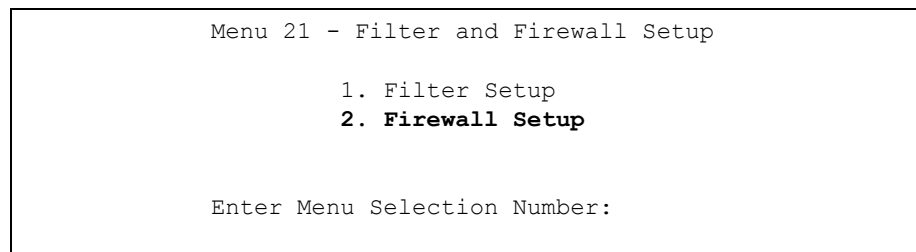
## Introducing the ZyWALL Firewall

This chapter shows you how to get started with the ZyWALL firewall.

### 43.1 Using ZyWALL SMT Menus

From the main menu enter 21 to go to **Menu 21 - Filter Set and Firewall Configuration** to display the screen shown next.

**Figure 338** Menu 21: Filter and Firewall Setup



#### 43.1.1 Activating the Firewall

Enter option 2 in this menu to bring up the following screen. Press [SPACE BAR] and then [ENTER] to select **Yes** in the **Active** field to activate the firewall. The firewall must be active to protect against Denial of Service (DoS) attacks. Use the web configurator to configure firewall rules.

**Figure 339** Menu 21.2: Firewall Setup

```
Menu 21.2 - Firewall Setup

The firewall protects against Denial of Service (DoS) attacks
when it is active.

Your network is vulnerable to attacks when the firewall is
turned off.

Refer to the User's Guide for details about the firewall
default policies.

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

Active: Yes

You can use the Web Configurator to configure the firewall.

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

**Note:** Configure the firewall rules using the web configurator or CLI commands.

# CHAPTER 44

## Filter Configuration

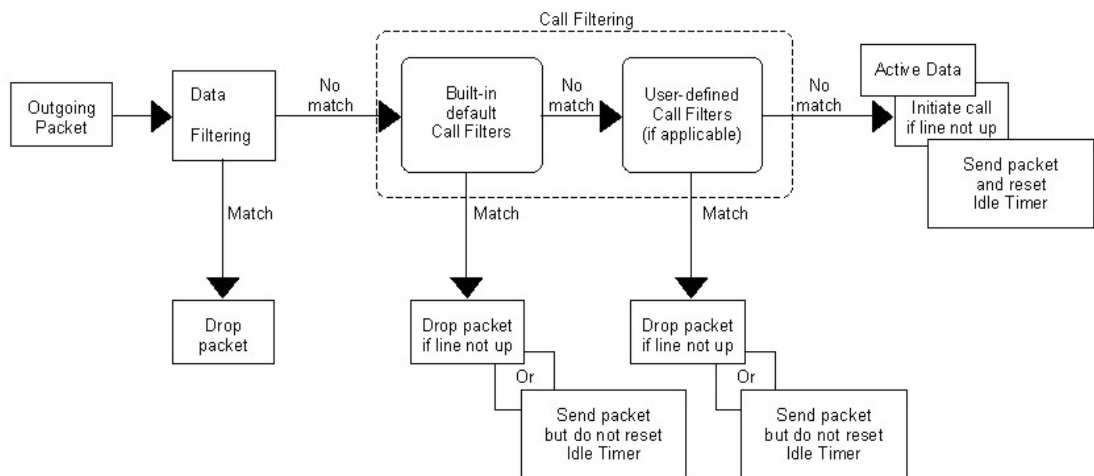
This chapter shows you how to create and apply filters.

### 44.1 Introduction to Filters

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

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

**Figure 340** Outgoing Packet Filtering Process



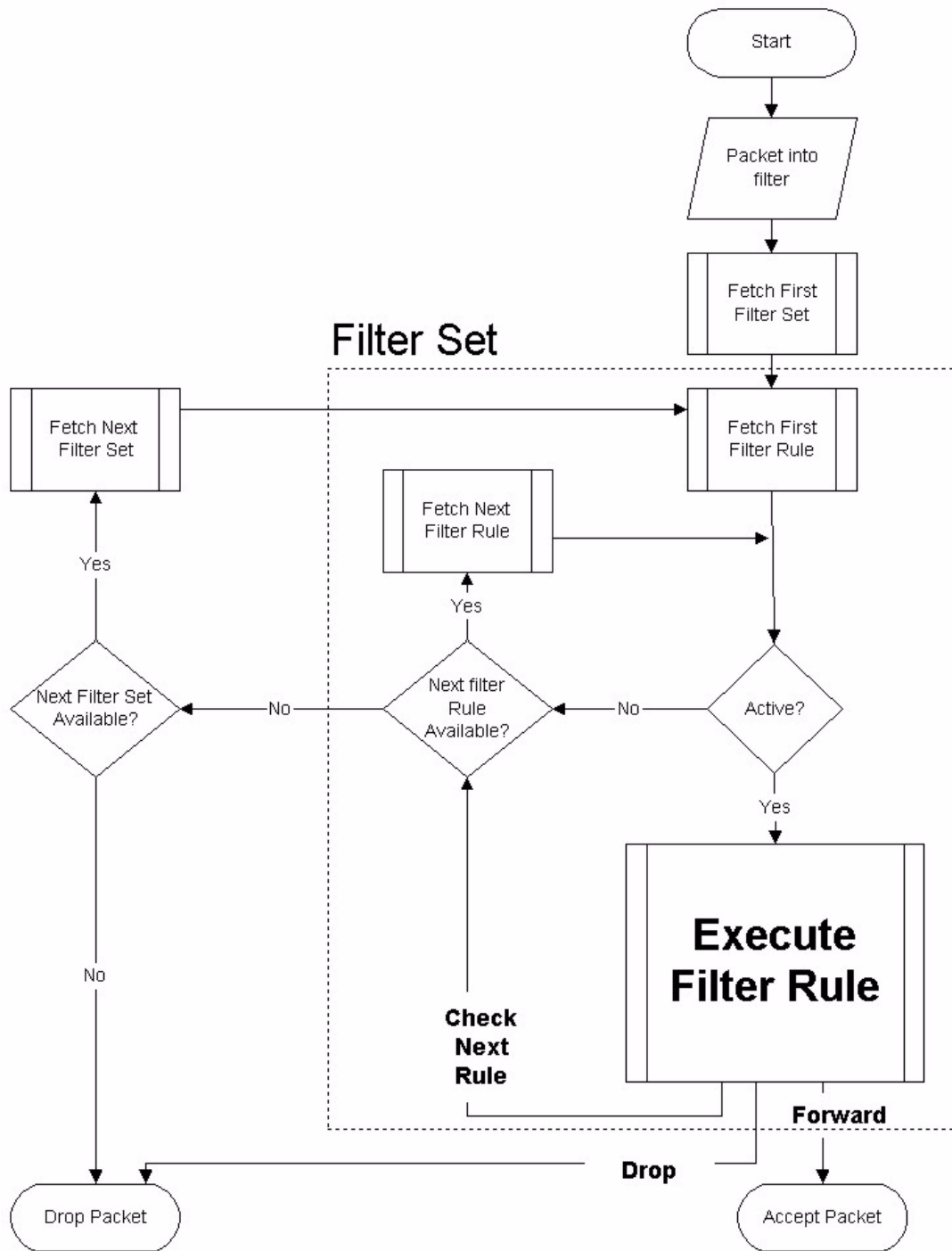
For incoming packets, your ZyWALL applies data filters only. Packets are processed depending upon whether a match is found. The following sections describe how to configure filter sets.

### 44.1.1 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 telnet sessions. A summary of their filter rules is shown in the figures that follow.

The following figure illustrates the logic flow when executing a filter rule. See also [Figure 345 on page 591](#) for the logic flow when executing an IP filter.

**Figure 341** 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.

## 44.2 Configuring a Filter Set

The ZyWALL includes filtering for NetBIOS over TCP/IP packets by default. To configure another filter set, follow the procedure below.

- 1 Enter 21 in the main menu to open menu 21.

**Figure 342** Menu 21: Filter and Firewall Setup

```

Menu 21 - Filter and Firewall Setup

      1. Filter Setup
      2. Firewall Setup

Enter Menu Selection Number:
    
```

- 2 Enter 1 to bring up the following menu.

**Figure 343** Menu 21.1: Filter Set Configuration

```

Menu 21.1 - Filter Set Configuration

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

Enter Filter Set Number to Configure= 0

Edit Comments= N/A

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

- 3 Select the filter set you wish to configure (1-12) and press [ENTER].
- 4 Enter a descriptive name or comment in the **Edit Comments** field and press [ENTER].
- 5 Press [ENTER] at the message [Press ENTER to confirm] to open **Menu 21.1.1 - Filter Rules Summary**.

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

**Table 220** Abbreviations Used in the Filter Rules Summary Menu

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

The protocol dependent filter rules abbreviation are listed as follows:

**Table 221** Rule Abbreviations Used

ABBREVIATION	DESCRIPTION
IP	Pr Protocol
	SA Source Address
	SP Source Port number
	DA Destination Address
	DP Destination Port number
GEN	Off Offset
	Len Length

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

## 44.2.1 Configuring a Filter Rule

To configure a filter rule, type its number in **Menu 21.1.1 - Filter Rules Summary** and press [ENTER] to open menu 21.1.1.1 for the rule.



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

## 44.2.2 Configuring a TCP/IP Filter Rule

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

To configure TCP/IP rules, select **TCP/IP Filter Rule** from the **Filter Type** field and press [ENTER] to open **Menu 21.1.1.1 - TCP/IP Filter Rule**, as shown next.

**Figure 344** Menu 21.1.1.1: TCP/IP Filter Rule

```

Menu 21.1.1.1 - TCP/IP Filter Rule

Filter #: 1,1
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 0      IP Source Route= No
Destination: IP Addr=
                IP Mask=
                Port #=
                Port # Comp= None
Source: IP Addr=
          IP Mask=
          Port #=
          Port # Comp= None
TCP Estab= N/A
More= No          Log= None
Action Matched= Check Next Rule
Action Not Matched= Check Next Rule

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

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

**Table 222** Menu 21.1.1.1: TCP/IP Filter Rule

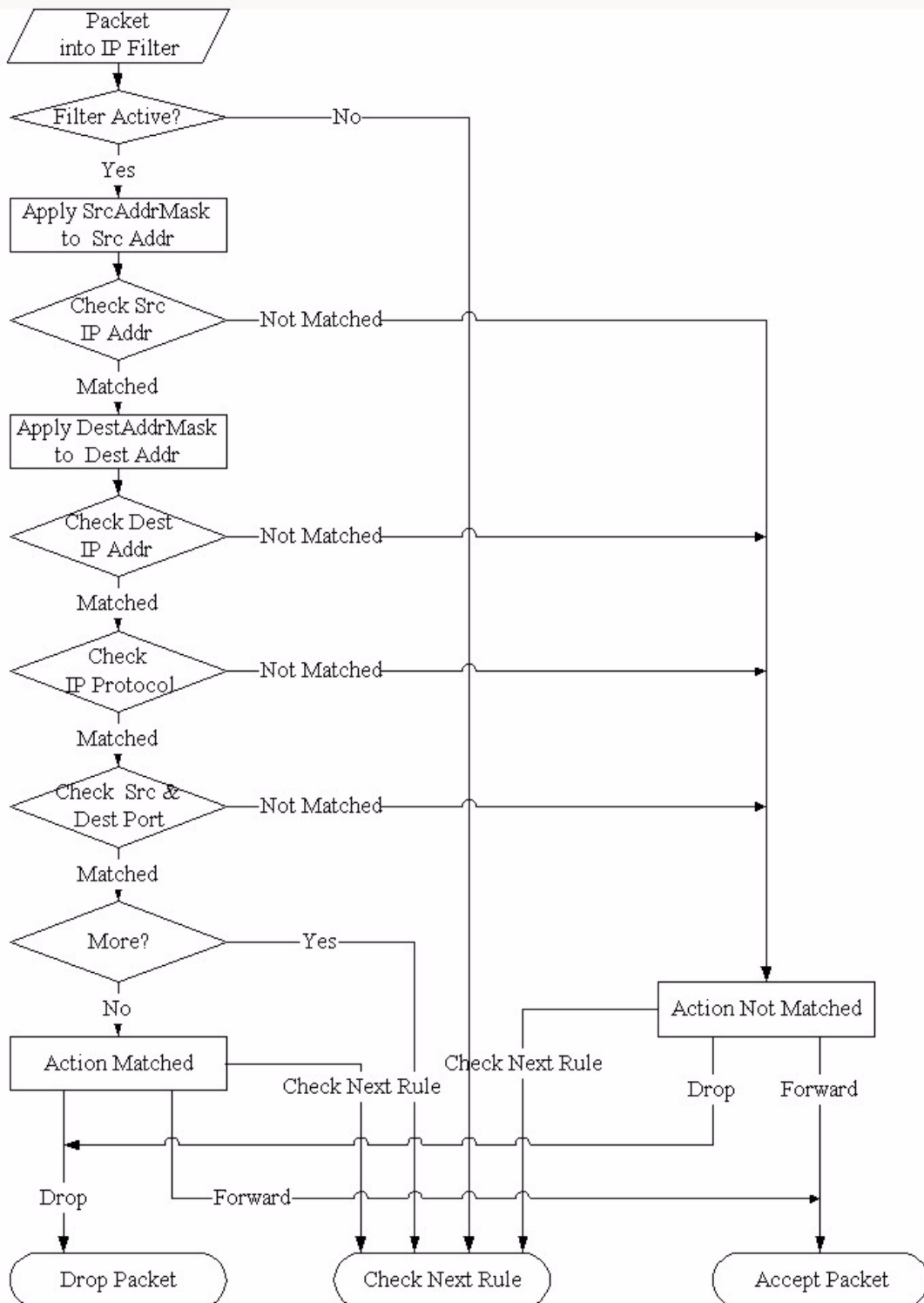
FIELD	DESCRIPTION
Active	Press [SPACE BAR] and then [ENTER] to select <b>Yes</b> to activate the filter rule or <b>No</b> to deactivate it.
IP Protocol	Protocol refers to the upper layer protocol, e.g., TCP is 6, UDP is 17 and ICMP is 1. Type a value between 0 and 255. A value of 0 matches ANY protocol.
IP Source Route	Press [SPACE BAR] and then [ENTER] to select <b>Yes</b> to apply the rule to packets with an IP source route option. Otherwise the packets must not have a source route option. The majority of IP packets do not have source route.

**Table 222** Menu 21.1.1.1: TCP/IP Filter Rule

FIELD	DESCRIPTION
Destination	
IP Addr	Enter the destination IP Address of the packet you wish to filter. This field is ignored if it is 0.0.0.0.
IP Mask	Enter the IP mask to apply to the <b>Destination: IP Addr</b> .
Port #	Enter the destination port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0.
Port # Comp	Press [SPACE BAR] and then [ENTER] to select the comparison to apply to the destination port in the packet against the value given in <b>Destination: Port #</b> . Options are <b>None, Equal, Not Equal, Less</b> and <b>Greater</b> .
Source	
IP Addr	Enter the source IP Address of the packet you wish to filter. This field is ignored if it is 0.0.0.0.
IP Mask	Enter the IP mask to apply to the <b>Source: IP Addr</b> .
Port #	Enter the source port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0.
Port # Comp	Press [SPACE BAR] and then [ENTER] to select the comparison to apply to the source port in the packet against the value given in <b>Source: Port #</b> . Options are <b>None, Equal, Not Equal, Less</b> and <b>Greater</b> .
TCP Estab	This field is applicable only when the IP Protocol field is 6, TCP. Press [SPACE BAR] and then [ENTER] to select <b>Yes</b> , to have the rule match packets that want to establish a TCP connection (SYN=1 and ACK=0); if <b>No</b> , it is ignored.
More	Press [SPACE BAR] and then [ENTER] to select <b>Yes</b> or <b>No</b> . 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 according to the action fields. 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> .
Log	Press [SPACE BAR] and then [ENTER] to select a 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.
Action Matched	Press [SPACE BAR] and then [ENTER] to select the action for a matching packet. Options are <b>Check Next Rule, Forward</b> and <b>Drop</b> .
Action Not Matched	Press [SPACE BAR] and then [ENTER] to select the action for a packet not matching the rule. Options are <b>Check Next Rule, Forward</b> and <b>Drop</b> .
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> .	

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

**Figure 345** Executing an IP Filter



### 44.2.3 Configuring a Generic Filter Rule

This section shows you how to configure a generic filter rule. The purpose of generic rules is

to allow you to filter non-IP packets. For IP, it is generally easier to use the IP rules directly.

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

To configure a generic rule, select **Generic Filter Rule** in the **Filter Type** field in menu 21.1.1.1 and press [ENTER] to open Generic Filter Rule, as shown below.

**Figure 346** Menu 21.1.1.1: Generic Filter Rule

```

Menu 21.1.1.1 - Generic Filter Rule

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

Press ENTER to Confirm or ESC to Cancel:

```

The following table describes the fields in the **Generic Filter Rule** menu.

**Table 223** Generic Filter Rule Menu Fields

FIELD	DESCRIPTION
Filter #	This is the filter set, filter rule co-ordinates, i.e., 2,3 refers to the second filter set and the third rule of that set.
Filter Type	Use [SPACE BAR] and then [ENTER] to select a rule type. Parameters displayed below each type will be different. TCP/IP filter rules are used to filter IP packets while generic filter rules allow filtering of non-IP packets. Options are <b>Generic Filter Rule</b> and <b>TCP/IP Filter Rule</b> .
Active	Select <b>Yes</b> to turn on the filter rule or <b>No</b> to turn it off.
Offset	Enter the starting byte of the data portion in the packet that you wish to compare. The range for this field is from 0 to 255.
Length	Enter the byte count of the data portion in the packet that you wish to compare. The range for this field is 0 to 8.
Mask	Enter the mask (in Hexadecimal notation) to apply to the data portion before comparison.
Value	Enter the value (in Hexadecimal notation) to compare with the data portion.

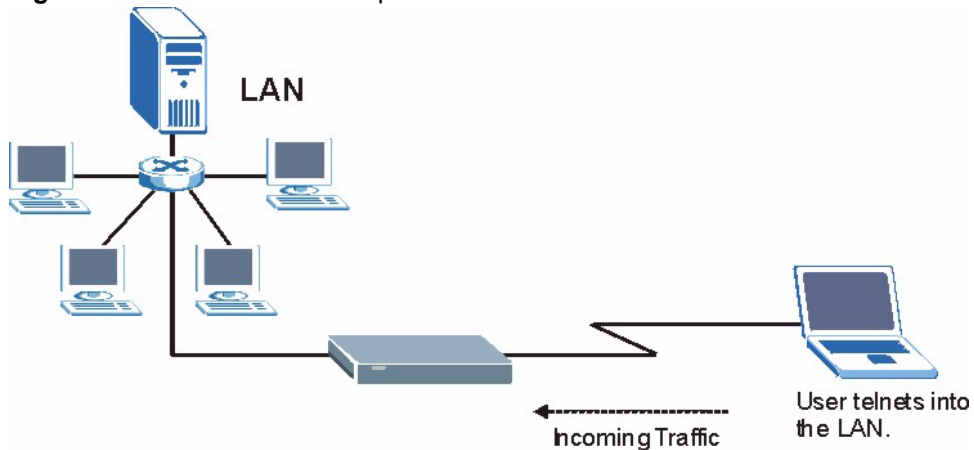
**Table 223** Generic Filter Rule Menu Fields

FIELD	DESCRIPTION
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> .
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.
Action Matched	Select the action for a packet matching the rule. Options are <b>Check Next Rule</b> , <b>Forward</b> and <b>Drop</b> .
Action Not Matched	Select the action for a packet not matching the rule. Options are <b>Check Next Rule</b> , <b>Forward</b> and <b>Drop</b> .
Once you have completed filling in <b>Menu 21.1.1.1 - 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> .	

### 44.3 Example Filter

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

**Figure 347** Telnet Filter Example



- 1 Enter 21 from the main menu to open **Menu 21 - Filter and Firewall Setup**.
- 2 Enter 1 to open Menu 21.1 - Filter Set Configuration.
- 3 Enter the index of the filter set you wish to configure (say 3) and press [ENTER].
- 4 Enter a descriptive name or comment in the **Edit Comments** field and press [ENTER].
- 5 Press [ENTER] at the message [Press ENTER to confirm] to open **Menu 21.1.3 - Filter Rules Summary**.
- 6 Enter 1 to configure the first filter rule (the only filter rule of this set). Make the entries in this menu as shown in the following figure.

**Figure 348** Example Filter: Menu 21.1.3.1

```

Menu 21.1.3.1 - TCP/IP Filter Rule

Filter #: 3,1
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 6      IP Source Route= No
Destination: IP Addr= 0.0.0.0
               IP Mask= 0.0.0.0
               Port # = 23
               Port # Comp= Equal
Source: IP Addr= 0.0.0.0
          IP Mask= 0.0.0.0
          Port # = 0
          Port # Comp= None

TCP Estab= No
More= No          Log= None
Action Matched= Drop
Action Not Matched= Forward

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

```

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

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

**Figure 349** Example Filter Rules Summary: Menu 21.1.3

```

Menu 21.1.3 - Filter Rules Summary

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

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

```

This shows you that you have configured and activated (**A = Y**) a TCP/IP filter rule (**Type = IP, Pr = 6**) for destination telnet ports (**DP = 23**).

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

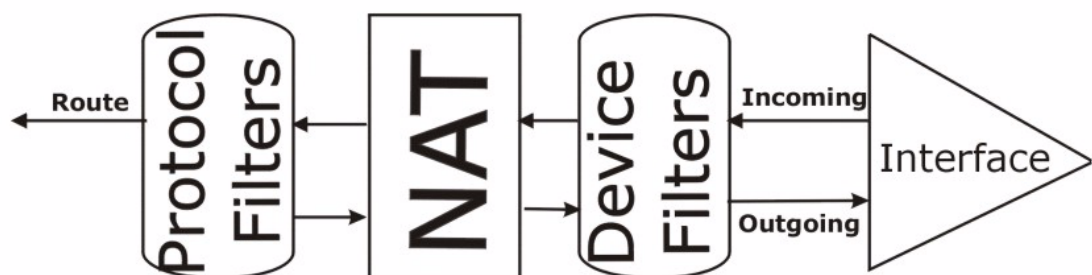
After you've created the filter set, you must apply it.

- 1 Enter 11 from the main menu to go to menu 11.
- 2 Enter 1 or 2 to open **Menu 11.x - Remote Node Profile**.
- 3 Go to the **Edit Filter Sets** field, press [SPACE BAR] to select **Yes** and press [ENTER].
- 4 This brings you to menu 11.1.4. Apply a filter set (our example filter set 3) as shown in [Figure 353 on page 597](#).
- 5 Press [ENTER] to confirm after you enter the set numbers and to leave menu 11.1.4.

## 44.4 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 350** Protocol and Device Filter Sets



## 44.5 Firewall Versus Filters

Firewall configuration is discussed in [Chapter 11 on page 214](#). Further comparisons are also made between filtering, NAT and the firewall.

## 44.6 Applying a Filter

This section shows you where to apply the filter(s) after you design it (them). The ZyWALL already has filters to prevent NetBIOS traffic from triggering calls, and block incoming telnet, FTP and HTTP connections.

**Note:** If you do not activate the firewall, it is advisable to apply filters.

### 44.6.1 Applying LAN Filters

LAN traffic filter sets may be useful to block certain packets, reduce traffic and prevent security breaches. Go to menu 3.1 (shown next) and enter the number(s) of the filter set(s) that you want to apply as appropriate. You can choose up to four filter sets (from twelve) by entering their numbers separated by commas, e.g., 3, 4, 6, 11. Input filter sets filter incoming traffic to the ZyWALL and output filter sets filter outgoing traffic from the ZyWALL. For PPPoE or PPTP encapsulation, you have the additional option of specifying remote node call filter sets.

**Figure 351** Filtering LAN Traffic

```
Menu 3.1 - LAN Port Filter Setup

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

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

### 44.6.2 Applying DMZ Filters

DMZ traffic filter sets may be useful to block certain packets, reduce traffic and prevent security breaches. Go to menu 5.1 (shown next) and enter the number(s) of the filter set(s) that you want to apply as appropriate. You can choose up to four filter sets (from twelve) by entering their numbers separated by commas, e.g., 3, 4, 6, 11. Input filter sets filter incoming traffic to the ZyWALL and output filter sets filter outgoing traffic from the ZyWALL. The ZyWALL already has filters to prevent NetBIOS traffic from triggering calls, and block incoming telnet, FTP and HTTP connections.



**Figure 352** Filtering DMZ Traffic

```
Menu 5.1 - DMZ Port Filter Setup

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

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

### 44.6.3 Applying Remote Node Filters

Go to menu 11.1.4 (shown below – note that call filter sets are only present for PPPoE encapsulation) and enter the number(s) of the filter set(s) as appropriate. You can cascade up to four filter sets by entering their numbers separated by commas. The ZyWALL already has filters to prevent NetBIOS traffic from triggering calls, and block incoming telnet, FTP and HTTP connections.

**Figure 353** Filtering Remote Node Traffic

```
Menu 11.1.4 - Remote Node Filter Setup

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

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

# CHAPTER 45

## SNMP Configuration

This chapter explains SNMP configuration menu 22.

### 45.1 SNMP Configuration

To configure SNMP, enter 22 from the main menu to display **Menu 22 - SNMP Configuration** as shown next. The “community” for **Get**, **Set** and **Trap** fields is SNMP terminology for password.

**Figure 354** Menu 22: SNMP Configuration

```

Menu 22 - SNMP Configuration

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

Press ENTER to Confirm or ESC to Cancel:

```

The following table describes the SNMP configuration parameters.

**Table 224** SNMP Configuration Menu Fields

FIELD	DESCRIPTION
Get Community	Type the Get community, which is the password for the incoming Get- and GetNext requests from the management station.
Set Community	Type the Set community, which is the password for incoming Set requests from the management station.
Trusted Host	If you enter a trusted host, your ZyWALL will only respond to SNMP messages from this address. A blank (default) field means your ZyWALL will respond to all SNMP messages it receives, regardless of source.
Trap	
Community	Type the Trap community, which is the password sent with each trap to the SNMP manager.

**Table 224** SNMP Configuration Menu Fields (continued)

FIELD	DESCRIPTION
Destination	Type the IP address of the station to send your SNMP traps to.
When you have completed this menu, press [ENTER] at the prompt "Press [ENTER] to confirm or [ESC] to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

## 45.2 SNMP Traps

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

**Table 225** SNMP Traps

TRAP #	TRAP NAME	DESCRIPTION
0	coldStart (defined in <i>RFC-1215</i> )	A trap is sent after booting (power on).
1	warmStart (defined in <i>RFC-1215</i> )	A trap is sent after booting (software reboot).
4	authenticationFailure (defined in <i>RFC-1215</i> )	A trap is sent to the manager when receiving any SNMP get or set requirements with the wrong community (password).
6	whyReboot (defined in ZYXEL-MIB)	A trap is sent with the reason of restart before rebooting when the system is going to restart (warm start).
6a	For intentional reboot:	A trap is sent with the message "System reboot by user!" if reboot is done intentionally, (for example, download new files, CLI command "sys reboot", etc.).
6b	For fatal error:	A trap is sent with the message of the fatal code if the system reboots because of fatal errors.

# CHAPTER 46

## System Information & Diagnosis

This chapter covers SMT menus 24.1 to 24.4.

### 46.1 Introduction to System Status

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

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

**Figure 355** Menu 24: System Maintenance

```
Menu 24 - System Maintenance

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

Enter Menu Selection Number:
```

### 46.2 System Status

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

To get to the System Status:

- 1 Enter number 24 to go to Menu 24 - System Maintenance.
- 2 In this menu, enter 1 to open System Maintenance - Status.

**3** There are three commands in **Menu 24.1 - System Maintenance - Status**. Entering 1 drops the WAN connection, 9 resets the counters and [ESC] takes you back to the previous screen.

**Figure 356** Menu 24.1: System Maintenance: Status

```

Menu 24.1 - System Maintenance - Status
                                                    08:17:55
                                                    Wed. Jul. 27, 2005
Port  Status      TxPkts    RxPkts    Cols    Tx B/s    Rx B/s    Up Time
WAN1  100M/Full    9439     332111    0        0         1062     2:35:42
WAN2  Down         0         0         0         0         0        0:00:00
LAN   100M/Full    7802     11353     0        354       192     2:35:42
WCRD  Down         0         0         0         0         0        0:00:00
DMZ   100M/Full    0         0         0         0         0        2:35:42
WLAN  100M/Full    0         0         0         0         0        2:35:42

Port  Ethernet Address      IP Address      IP Mask      DHCP
WAN1  00:A0:C5:01:23:46     172.22.1.162   255.255.0.0  Client
WAN2  00:A0:C5:01:23:48     0.0.0.0        0.0.0.0      Client
LAN   00:A0:C5:01:23:45     192.168.1.1    255.255.255.0 Server
WLAN  00:00:00:00:00:00
DMZ   00:A0:C5:01:23:47     10.10.2.1      255.255.255.0 None

System up Time:      2:35:47
CARD bridged to: LAN

Press Command:

COMMANDS: 1, 2-Drop WAN1,2 9-Reset Counters  ESC-Exit
    
```

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

**Table 226** System Maintenance: Status Menu Fields

FIELD	DESCRIPTION
Port	This field identifies a port (WAN, LAN, WCRD (wireless LAN card), DMZ or WLAN) on the ZyWALL.
Status	For the LAN, DMZ, and WLAN Interfaces, this displays the port speed and duplex setting. For the WAN port, it displays the port speed and duplex setting if you're using Ethernet encapsulation and <b>Down</b> (line is down or not connected), <b>Idle</b> (line (ppp) idle), <b>Dial</b> (starting to trigger a call) or <b>Drop</b> (dropping a call) if you're using PPPoE encapsulation. For the wireless card, it displays the transmission rate when a wireless LAN card is inserted and WLAN is enabled or <b>Down</b> when a wireless LAN is not inserted or WLAN is disabled.
TxPkts	This is the number of transmitted packets on this port.
RxPkts	This is the number of received packets on this port.
Cols	This is the number of collisions on this port.
Tx B/s	This field shows the transmission speed in Bytes per second on this port.

**Table 226** System Maintenance: Status Menu Fields (continued)

FIELD	DESCRIPTION
Rx B/s	This field shows the reception speed in Bytes per second on this port.
Up Time	This is the total amount of time the line has been up.
Ethernet Address	This is the Ethernet address of the port listed on the left.
IP Address	This is the IP address of the port listed on the left.
IP Mask	This is the IP mask of the port listed on the left.
DHCP	This is the DHCP setting of the port listed on the left.
System up Time	This is the total time the ZyWALL has been on.
CARD bridged to	This field shows whether the wireless card is set to be part of the LAN, DMZ or WLAN.
You may enter 1 to drop the WAN connection, 9 to reset the counters or [ESC] to return to menu 24.	

## 46.3 System Information and Console Port Speed

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

- 1 Enter 24 to go to **Menu 24 - System Maintenance**.
- 2 Enter 2 to open **Menu 24.2 - System Information and Console Port Speed**.
- 3 From this menu you have two choices as shown in the next figure:

**Figure 357** Menu 24.2: System Information and Console Port Speed

```

Menu 24.2 - System Information and Console Port Speed

    1. System Information
    2. Console Port Speed

Please enter selection:

```

### 46.3.1 System Information

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

**Figure 358** Menu 24.2.1: System Maintenance: Information

```

Menu 24.2.1 - System Maintenance - Information

Name:
Routing: IP
ZyNOS F/W Version: V4.00(WM.0)b2 | 07/25/2005
Country Code: 255

LAN
Ethernet Address: 00:A0:C5:01:23:45
IP Address: 192.168.1.1
IP Mask: 255.255.255.0
DHCP: Server

Press ESC or RETURN to Exit:

```

The following table describes the fields in this screen.

**Table 227** Fields in System Maintenance: Information

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

### 46.3.2 Console Port Speed

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

**Figure 359** Menu 24.2.2: System Maintenance: Change Console Port Speed

```
Menu 24.2.2 - System Maintenance - Change Console Port Speed

      Console Port Speed: 9600

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

## 46.4 Log and Trace

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

### 46.4.1 Viewing Error Log

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

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

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

**Figure 360** Menu 24.3: System Maintenance: Log and Trace

```
Menu 24.3 - System Maintenance - Log and Trace

1. View Error Log
2. UNIX Syslog

4. Call-Triggering Packet

      Please enter selection
```

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



**Figure 361** Examples of Error and Information Messages

```

52 Thu Jul 1 05:54:53 2004 PP05 ERROR Wireless LAN init fail, code=15
53 Thu Jul 1 05:54:53 2004 PINI INFO Channel 0 ok
54 Thu Jul 1 05:54:56 2004 PP05 -WARN SNMP TRAP 3: interface 3: link up
55 Thu Jul 1 05:54:56 2004 PP0d INFO LAN promiscuous mode <0>
57 Thu Jul 1 05:54:56 2004 PP0d INFO LAN promiscuous mode <1>
58 Thu Jul 1 05:54:56 2004 PINI INFO Last errorlog repeat 1 Times
59 Thu Jul 1 05:54:56 2004 PINI INFO main: init completed
60 Thu Jul 1 05:55:26 2004 PSSV -WARN SNMP TRAP 0: cold start
61 Thu Jul 1 05:56:56 2004 PINI INFO SMT Session Begin
62 Thu Jul 1 07:50:58 2004 PINI INFO SMT Session End
63 Thu Jul 1 07:53:28 2004 PINI INFO SMT Session Begin
Clear Error Log (y/n):
    
```

### 46.4.2 Syslog Logging

The ZyWALL uses the 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 Logging**, as shown next.

**Figure 362** Menu 24.3.2: System Maintenance: Syslog Logging

```

Menu 24.3.2 - System Maintenance - Syslog Logging

Syslog:
Active= No
Syslog Server IP Address= 0.0.0.0
Log Facility= Local 1

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

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

**Table 228** System Maintenance Menu Syslog Parameters

FIELD	DESCRIPTION
Syslog:	
Active	Press [SPACE BAR] and then [ENTER] to turn syslog on or off.
Syslog Server IP Address	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
Log Facility	Press [SPACE BAR] and then [ENTER] to select a location. The log facility allows you to log the messages to different files in the syslog server. Refer to the documentation of your syslog program for more details.
When finished configuring this screen, press [ENTER] to confirm or [ESC] to cancel.	

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

### 1 CDR

CDR Message Format
<pre>SdcmdSyslogSend( SYSLOG_CDR, SYSLOG_INFO, String ); String = board xx line xx channel xx, call xx, str board = the hardware board ID line = the WAN ID in a board Channel = channel ID within the WAN call = the call reference number which starts from 1 and increments by 1 for each new call str = C01 Outgoing Call dev xx ch xx (dev:device No. ch:channel No.)       L02 Tunnel Connected(L2TP)       C02 OutCall Connected xxxx (means connected speed) xxxxx (means Remote Call Number)       L02 Call Terminated       C02 Call Terminated Jul 19 11:19:27 192.168.102.2 ZyXEL: board 0 line 0 channel 0, call 1, C01 Outgoing Call dev=2 ch=0 40002 Jul 19 11:19:32 192.168.102.2 ZyXEL: board 0 line 0 channel 0, call 1, C02 OutCall Connected 64000 40002 Jul 19 11:20:06 192.168.102.2 ZyXEL: board 0 line 0 channel 0, call 1, C02 Call Terminated</pre>

### 2 Packet triggered

Packet triggered Message Format
<pre>SdcmdSyslogSend( SYSLOG_PKTTRI, SYSLOG_NOTICE, String ); String = Packet trigger: Protocol=xx Data=xxxxxxxxxx...x Protocol: (1:IP 2:IPX 3:IPXHC 4:BPDU 5:ATALK 6:IPNG) Data: We will send forty-eight Hex characters to the server Jul 19 11:28:39 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1, Data=4500003c100100001f010004c0a86614ca849a7b08004a5c020001006162636465666768696a 6b6c6d6e6f7071727374 Jul 19 11:28:56 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1, Data=4500002c1b0140001f06b50ec0a86614ca849a7b0427001700195b3e00000000600220008cd4 0000020405b4 Jul 19 11:29:06 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1, Data=45000028240140001f06ac12c0a86614ca849a7b0427001700195b451d143013500400007760 0000</pre>

### 3 Filter log

```

Filter log Message Format

SdcmdSyslogSend(SYSLOG_FILLOG, SYSLOG_NOTICE, String );
String = IP[Src=xx.xx.xx.xx Dst=xx.xx.xx.xx prot spo=xxxx dpo=xxxx] S04>R01mD
IP[...] is the packet header and S04>R01mD means filter set 4 (S) and rule 1 (R),
match (m) drop (D).
    Src: Source Address
    Dst: Destination Address
    prot: Protocol ("TCP","UDP","ICMP")
spo: Source port
dpo: Destination 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 12:00:52 202.132.155.97 ZyXEL:
GEN[fffffffffff0080] }S05>R01mF
Mar 03 12:00:57 202.132.155.97 ZyXEL:
GEN[00a0c5f502010080] }S05>R01mF
Mar 03 12:01:06 202.132.155.97 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_PPPLLOG, SYSLOG_NOTICE, String );
String = ppp:Proto Starting / ppp:Proto Opening / ppp:Proto Closing / ppp:Proto
Shutdown
Proto = LCP / ATCP / BACP / BCP / CBCP / CCP / CHAP/ PAP / IPCP /
IPXCP
Jul 19 11:42:44 192.168.102.2 ZyXEL: ppp:LCP Closing
Jul 19 11:42:49 192.168.102.2 ZyXEL: ppp:IPCP Closing
Jul 19 11:42:54 192.168.102.2 ZyXEL: ppp:CCP Closing
    
```

#### 5 Firewall log

```

Firewall Log Message Format

SdcmdSyslogSend(SYSLOG_FIREWALL, SYSLOG_NOTICE, buf);
buf = IP[Src=xx.xx.xx.xx : spo=xxxx Dst=xx.xx.xx.xx : dpo=xxxx | prot | rule |
action]
Src: Source Address
spo: Source port (empty means no source port information)
Dst: Destination Address
dpo: Destination port (empty means no destination port information)
prot: Protocol ("TCP","UDP","ICMP", "IGMP", "GRE", "ESP")
rule: <a,b> where a means "set" number; b means "rule" number.
Action: nothing(N) block (B) forward (F)
08-01-200011:48:41Local1.Notice192.168.10.10RAS: FW 172.21.1.80 :137 -
>172.21.1.80 :137 |UDP|default permit:<2,0>|B
08-01-200011:48:41Local1.Notice192.168.10.10RAS: FW 192.168.77.88 :520 -
>192.168.77.88 :520 |UDP|default permit:<2,0>|B
08-01-200011:48:39Local1.Notice192.168.10.10RAS: FW 172.21.1.50 ->172.21.1.50
|IGMP<2>|default permit:<2,0>|B
08-01-200011:48:39Local1.Notice192.168.10.10RAS: FW 172.21.1.25 ->172.21.1.25
|IGMP<2>|default permit:<2,0>|B
    
```

### 46.4.3 Call-Triggering Packet

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

**Figure 363** Call-Triggering Packet Example

```

IP Frame: ENETO-RECV Size:  44/  44   Time: 17:02:44.262
Frame Type:

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

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

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

```

## 46.5 Diagnostic

The diagnostic facility allows you to test the different aspects of your ZyWALL to determine if it is working properly. Menu 24.4 allows you to choose among various types of diagnostic tests to evaluate your system, as shown next. Not all fields are available on all models.

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

- 1 From the main menu, select option 24 to open **Menu 24 - System Maintenance**.
- 2 From this menu, select option 4. Diagnostic. This will open **Menu 24.4 - System Maintenance - Diagnostic**.

**Figure 364** Menu 24.4: System Maintenance: Diagnostic

```

Menu 24.4 - System Maintenance - Diagnostic

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

System
  11. Reboot System

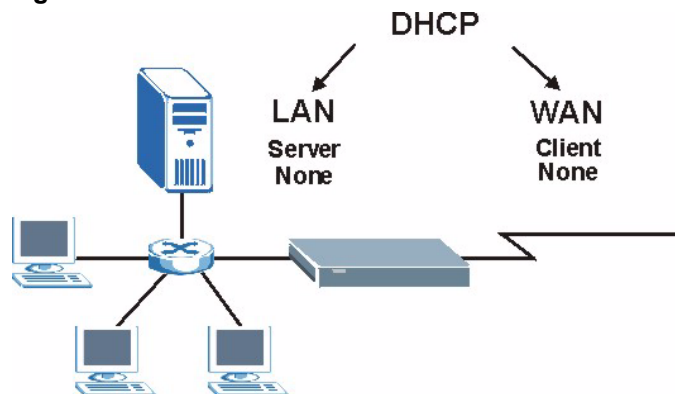
Enter Menu Selection Number:

WAN=
Host IP Address= N/A
    
```

### 46.5.1 WAN DHCP

DHCP functionality can be enabled on the LAN or WAN as shown in [Figure 365 on page 609](#). 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.x.2 is **Dynamic** and the **Encapsulation** field in menu 4 or menu 11 is **Ethernet**) or **None**, (when you have a static IP). The **WAN Release** and **Renewal** fields in menu 24.4 conveniently allow you to release and/or renew the assigned WAN IP address, subnet mask and default gateway in a fashion similar to winipcfg.

**Figure 365** WAN & LAN DHCP



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

**Table 229** System Maintenance Menu Diagnostic

<b>FIELD</b>	<b>DESCRIPTION</b>
Ping Host	Enter 1 to ping any machine (with an IP address) on your LAN or WAN. Enter its IP address in the <b>Host IP Address</b> 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 <a href="#">Chapter 36 on page 532</a> for more details. This feature is only available for dial-up connections using PPPoE or PPTP encapsulation.
Reboot System	Enter 11 to reboot the ZyWALL.
WAN	If you entered 2 or 3 in the <b>Enter Menu Selection Number</b> field, enter the number of the WAN port in this field.
Host IP Address	If you entered 1 in the <b>Enter Menu Selection Number</b> field, then enter the IP address of the computer you want to ping in this field.
Enter the number of the selection you would like to perform or press [ESC] to cancel.	



# CHAPTER 47

## 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.

### 47.1 Introduction

Use the instructions in this chapter to change the ZyWALL's configuration file or upgrade its firmware. After you configure your ZyWALL, you can backup the configuration file to a computer. That way if you later misconfigure the ZyWALL, you can upload the backed up configuration file to return to your previous settings. You can alternately upload the factory default configuration file if you want to return the ZyWALL to the original default settings. The firmware determines the ZyWALL's available features and functionality. You can download new firmware releases from your nearest ZyXEL FTP site to use to upgrade your ZyWALL's performance.

### 47.2 Filename Conventions

The configuration file (often called the romfile or rom-0) contains the factory default settings in the menus such as password, DHCP Setup, TCP/IP Setup, etc. It arrives from ZyXEL with a "rom" filename extension. Once you have customized the ZyWALL's settings, they can be saved back to your computer under a filename of your choosing.

ZyNOS (ZyXEL Network Operating System sometimes referred to as the "ras" file) is the system firmware and has a "bin" filename extension. With many FTP and TFTP clients, the filenames are similar to those seen next.

```
ftp> put firmware.bin ras
```

This is a sample FTP session showing the transfer of the computer file " firmware.bin" to the ZyWALL.

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

This is a sample FTP session saving the current configuration to the computer file "config.cfg".

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



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

**Table 230** Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	Rom-0	This is the configuration filename on the ZyWALL. Uploading the rom-0 file replaces the entire ROM file system, including your ZyWALL configurations, system-related data (including the default password), the error log and the trace log.	*.rom
Firmware	Ras	This is the generic name for the ZyNOS firmware on the ZyWALL.	*.bin

## 47.3 Backup Configuration

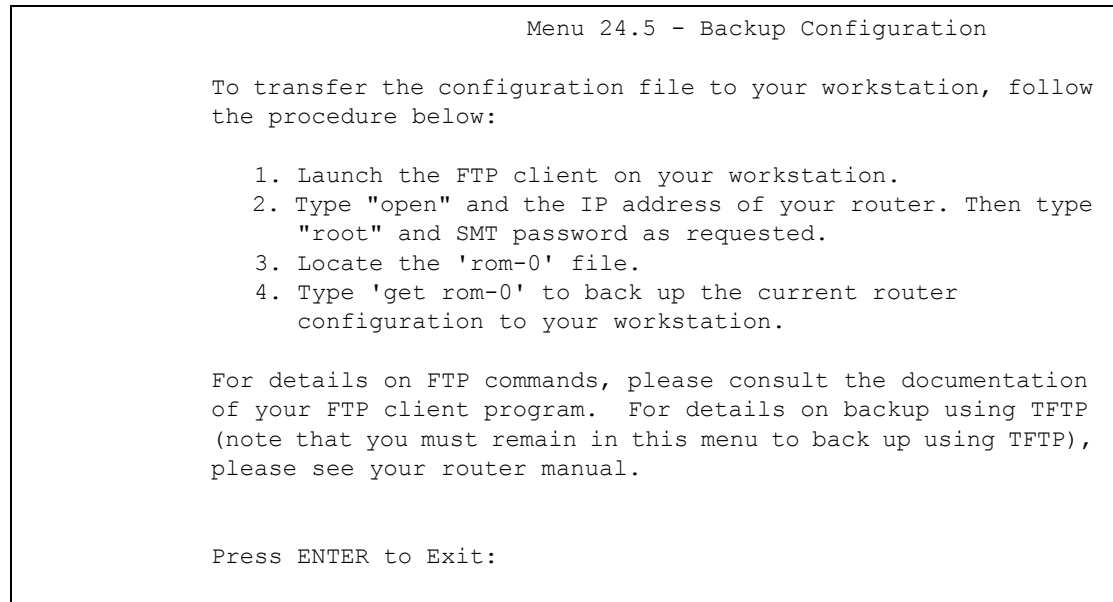
**Note:** The ZyWALL displays different messages explaining different ways to backup, restore and upload files in menus 24.5, 24.6, 24. 7.1 and 24.7.2 depending on whether you use the console port or Telnet.

Option 5 from **Menu 24 - System Maintenance** allows you to backup the current ZyWALL configuration to your computer. Backup is highly recommended once your ZyWALL is functioning properly. FTP is the preferred method for backing up your current configuration to your computer since it is faster. You can also perform backup and restore using menu 24 through the console port. Any serial communications program should work fine; however, you must use Xmodem protocol to perform the download/upload and you don't have to rename the files.

Please note that terms “download” and “upload” are relative to the computer. Download means to transfer from the ZyWALL to the computer, while upload means from your computer to the ZyWALL.

### 47.3.1 Backup Configuration

Follow the instructions as shown in the next screen.

**Figure 366** Telnet into Menu 24.5

### 47.3.2 Using the FTP Command from the Command Line

- 1 Launch the FTP client on your computer.
- 2 Enter “open”, followed by a space and the IP address of your ZyWALL.
- 3 Press [ENTER] when prompted for a username.
- 4 Enter your password as requested (the default is “1234”).
- 5 Enter “bin” to set transfer mode to binary.
- 6 Use “get” to transfer files from the ZyWALL to the computer, for example, “get rom-0 config.rom” transfers the configuration file on the ZyWALL to your computer and renames it “config.rom”. See earlier in this chapter for more information on filename conventions.
- 7 Enter “quit” to exit the ftp prompt.

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

**Figure 367** FTP Session Example

```

331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> get rom-0 zyxel.rom
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 16384 bytes sent in 1.10Seconds
297.89Kbytes/sec.
ftp> quit

```

### 47.3.4 GUI-based FTP Clients

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

**Table 231** General Commands for GUI-based FTP Clients

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

### 47.3.5 File Maintenance Over WAN

TFTP, FTP and Telnet over the WAN will not work when:

- 1** The firewall is active (turn the firewall off in menu 21.2 or create a firewall rule to allow access from the WAN).
- 2** You have disabled Telnet service in menu 24.11.
- 3** You have applied a filter in menu 3.1 (LAN) or in menu 11.5 (WAN) to block Telnet service.

- 4 The IP you entered in the **Secured Client IP** field in menu 24.11 does not match the client IP. If it does not match, the ZyWALL will disconnect the Telnet session immediately.
- 5 You have an SMT console session running.

### 47.3.6 Backup Configuration Using TFTP

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

To use TFTP, your computer must have both telnet and TFTP clients. To backup the configuration file, follow the procedure shown next.

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

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

### 47.3.7 TFTP Command Example

The following is an example TFTP command:

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

Where “i” specifies binary image transfer mode (use this mode when transferring binary files), “host” is the ZyWALL IP address, “get” transfers the file source on the ZyWALL (rom-0, name of the configuration file on the ZyWALL) to the file destination on the computer and renames it config.rom.

### 47.3.8 GUI-based TFTP Clients

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

**Table 232** General Commands for GUI-based TFTP Clients

COMMAND	DESCRIPTION
Host	Enter the IP address of the ZyWALL. 192.168.1.1 is the ZyWALL's default IP address when shipped.
Send/Fetch	Use "Send" to upload the file to the ZyWALL and "Fetch" to back up the file on your computer.
Local File	Enter the path and name of the firmware file (*.bin extension) or configuration file (*.rom extension) on your computer.
Remote File	This is the filename on the ZyWALL. The filename for the firmware is "ras" and for the configuration file, is "rom-0".
Binary	Transfer the file in binary mode.
Abort	Stop transfer of the file.

Refer to [Section 47.3.5 on page 615](#) to read about configurations that disallow TFTP and FTP over WAN.

### 47.3.9 Backup Via Console Port

Back up configuration via console port by following the HyperTerminal procedure shown next. Procedures using other serial communications programs should be similar.

- 1 Display menu 24.5 and enter "y" at the following screen.

**Figure 368** System Maintenance: Backup Configuration

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

- 2 The following screen indicates that the Xmodem download has started.

**Figure 369** System Maintenance: Starting Xmodem Download Screen

```
You can enter ctrl-x to terminate operation any
time.
Starting XMODEM download...
```

- 3 Run the HyperTerminal program by clicking **Transfer**, then **Receive File** as shown in the following screen.

**Figure 370** Backup Configuration Example

Type a location for storing the configuration file or click **Browse** to look for one.

Choose the **Xmodem** protocol.

Then click **Receive**.

- 4 After a successful backup you will see the following screen. Press any key to return to the SMT menu.

**Figure 371** Successful Backup Confirmation Screen

```
** Backup Configuration completed. OK.
### Hit any key to continue.###
```

## 47.4 Restore Configuration

This section shows you how to restore a previously saved configuration. Note that this function erases the current configuration before restoring a previous back up configuration; please do not attempt to restore unless you have a backup configuration file stored on disk.

FTP is the preferred method for restoring your current computer configuration to your ZyWALL since FTP is faster. Please note that you must wait for the system to automatically restart after the file transfer is complete.

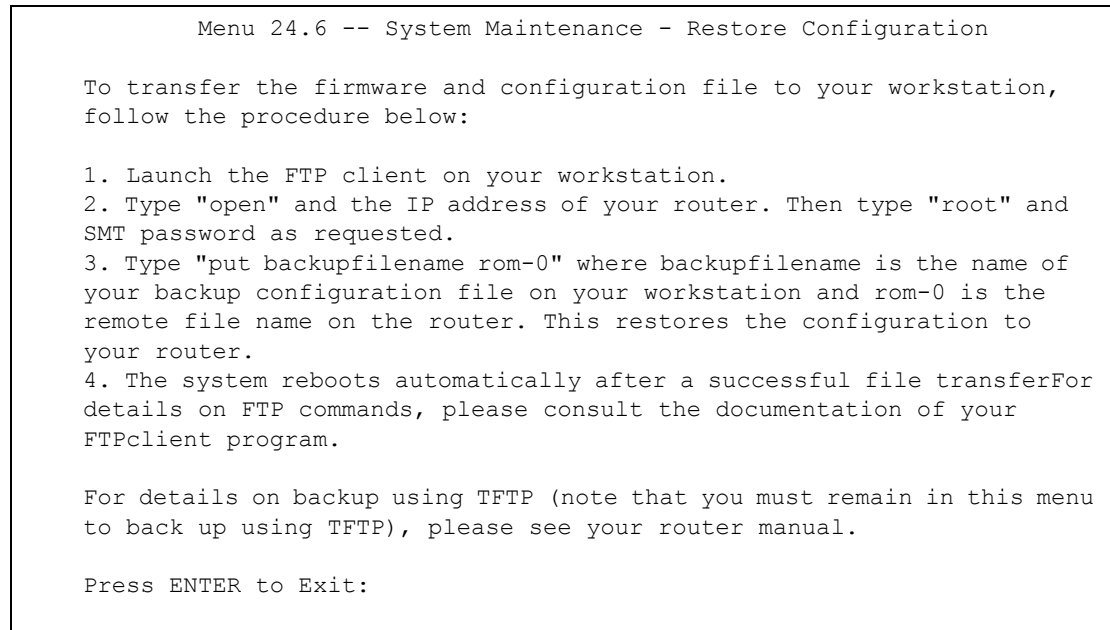
**Note:** WARNING!

Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE YOUR ZyWALL. When the Restore Configuration process is complete, the ZyWALL will automatically restart.

### 47.4.1 Restore Using FTP

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

**Figure 372** Telnet into Menu 24.6



- 1** Launch the FTP client on your computer.
- 2** Enter “open”, followed by a space and the IP address of your ZyWALL.
- 3** Press [ENTER] when prompted for a username.
- 4** Enter your password as requested (the default is “1234”).
- 5** Enter “bin” to set transfer mode to binary.
- 6** Find the “rom” file (on your computer) that you want to restore to your ZyWALL.
- 7** Use “put” to transfer files from the ZyWALL to the computer, for example, “put config.rom rom-0” transfers the configuration file “config.rom” on your computer to the ZyWALL. See earlier in this chapter for more information on filename conventions.
- 8** Enter “quit” to exit the ftp prompt. The ZyWALL will automatically restart after a successful restore process.

## 47.4.2 Restore Using FTP Session Example

**Figure 373** Restore Using FTP Session Example

```
ftp> put config.rom rom-0
200 Port command okay
150 Opening data connection for STOR rom-0
226 File received OK
221 Goodbye for writing flash
ftp: 16384 bytes sent in 0.06Seconds 273.07Kbytes/sec.
ftp>quit
```

Refer to [Section 47.3.5 on page 615](#) to read about configurations that disallow TFTP and FTP over WAN.

## 47.4.3 Restore Via Console Port

Restore configuration via console port by following the HyperTerminal procedure shown next. Procedures using other serial communications programs should be similar.

- 1 Display menu 24.6 and enter “y” at the following screen.

**Figure 374** System Maintenance: Restore Configuration

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

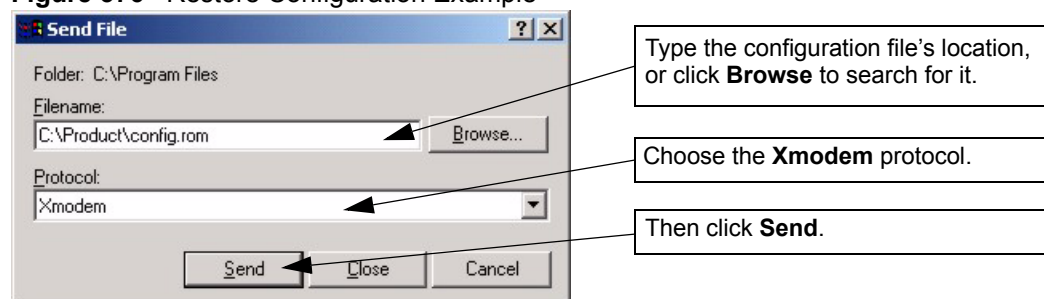
- 2 The following screen indicates that the Xmodem download has started.

**Figure 375** System Maintenance: Starting Xmodem Download Screen

```
Starting XMODEM download (CRC mode) ...CCCCCCCC
```

- 3 Run the HyperTerminal program by clicking **Transfer**, then **Send File** as shown in the following screen.

**Figure 376** Restore Configuration Example





- 4 After a successful restoration you will see the following screen. Press any key to restart the ZyWALL and return to the SMT menu.

**Figure 377** Successful Restoration Confirmation Screen

```
Save to ROM
Hit any key to start system reboot.
```

## 47.5 Uploading Firmware and Configuration Files

This section shows you how to upload firmware and configuration files. You can upload configuration files by following the procedure in [Section 47.4 on page 618](#) or by following the instructions in **Menu 24.7.2 - System Maintenance - Upload System Configuration File** (for console port).

**Note:** WARNING!

Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE YOUR ZyWALL.

### 47.5.1 Firmware File Upload

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

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

**Figure 378** Telnet Into Menu 24.7.1: Upload System Firmware

```
Menu 24.7.1 - System Maintenance - Upload System Firmware

To upload the system firmware, follow the procedure below:

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

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

Press ENTER to Exit:
```

## 47.5.2 Configuration File Upload

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

**Figure 379** Telnet Into Menu 24.7.2: System Maintenance

```
Menu 24.7.2 - System Maintenance - Upload System Configuration File

To upload the system configuration file, follow the procedure below:

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

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

Press ENTER to Exit:
```

To upload the firmware and the configuration file, follow these examples

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

- 1 Launch the FTP client on your computer.
- 2 Enter “open”, followed by a space and the IP address of your ZyWALL.
- 3 Press [ENTER] when prompted for a username.
- 4 Enter your password as requested (the default is “1234”).
- 5 Enter “bin” to set transfer mode to binary.
- 6 Use “put” to transfer files from the computer to the ZyWALL, for example, “put firmware.bin ras” transfers the firmware on your computer (firmware.bin) to the ZyWALL and renames it “ras”. Similarly, “put config.rom rom-0” transfers the configuration file on your computer (config.rom) to the ZyWALL and renames it “rom-0”. Likewise “get rom-0 config.rom” transfers the configuration file on the ZyWALL to your computer and renames it “config.rom.” See earlier in this chapter for more information on filename conventions.
- 7 Enter “quit” to exit the ftp prompt.

### 47.5.4 FTP Session Example of Firmware File Upload

**Figure 380** FTP Session Example of Firmware File Upload

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

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

Refer to [Section 47.3.5 on page 615](#) to read about configurations that disallow TFTP and FTP over WAN.

### 47.5.5 TFTP File Upload

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

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

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

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

## 47.5.6 TFTP Upload Command Example

The following is an example TFTP command:

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

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

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

## 47.5.7 Uploading Via Console Port

FTP or TFTP are the preferred methods for uploading firmware to your ZyWALL. However, in the event of your network being down, uploading files is only possible with a direct connection to your ZyWALL via the console port. Uploading files via the console port under normal conditions is not recommended since FTP or TFTP is faster. Any serial communications program should work fine; however, you must use the Xmodem protocol to perform the download/upload.

## 47.5.8 Uploading Firmware File Via Console Port

- 1 Select 1 from Menu 24.7 – System Maintenance – Upload Firmware to display Menu 24.7.1 - System Maintenance - Upload System Firmware, and then follow the instructions as shown in the following screen.

**Figure 381** Menu 24.7.1 As Seen Using the Console Port

```

Menu 24.7.1 - System Maintenance - Upload System Firmware

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

Warning: Proceeding with the upload will erase the current system
firmware.

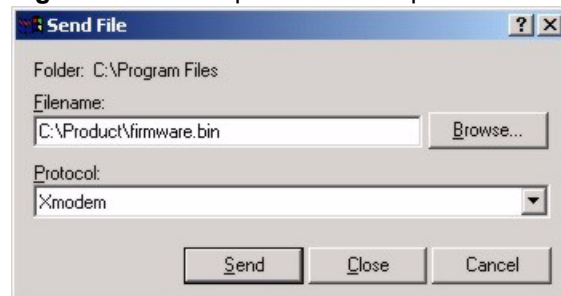
Do You Wish To Proceed: (Y/N)

```

- 2 After the "Starting Xmodem upload" message appears, activate the Xmodem protocol on your computer. Follow the procedure as shown previously for the HyperTerminal program. The procedure for other serial communications programs should be similar.

### 47.5.9 Example Xmodem Firmware Upload Using HyperTerminal

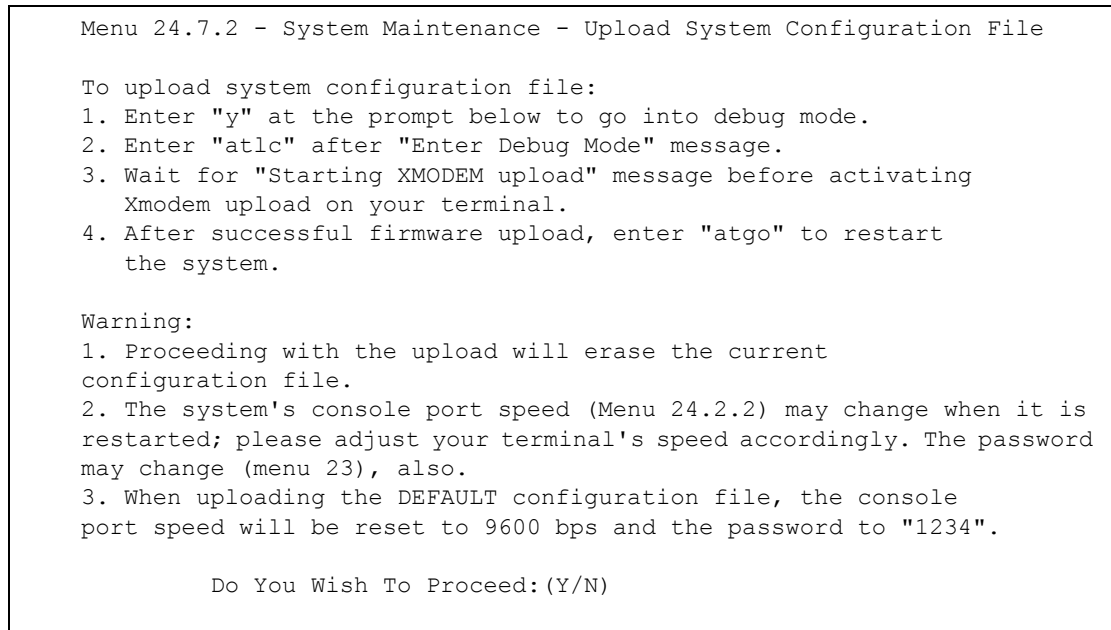
Click **Transfer**, then **Send File** to display the following screen.

**Figure 382** Example Xmodem Upload

After the firmware upload process has completed, the ZyWALL will automatically restart.

### 47.5.10 Uploading Configuration File Via Console Port

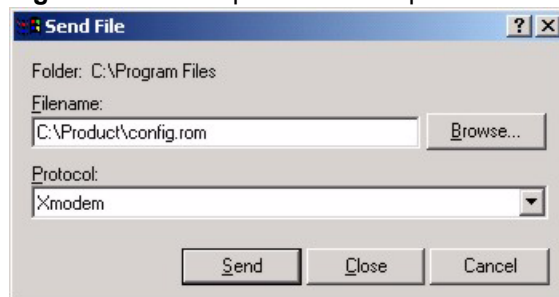
- 1 Select 2 from Menu 24.7 – System Maintenance – Upload Firmware to display Menu 24.7.2 - System Maintenance - Upload System Configuration File. Follow the instructions as shown in the next screen.

**Figure 383** Menu 24.7.2 As Seen Using the Console Port

- 2** After the "Starting Xmodem upload" message appears, activate the Xmodem protocol on your computer. Follow the procedure as shown previously for the HyperTerminal program. The procedure for other serial communications programs should be similar.
- 3** Enter "atgo" to restart the ZyWALL.

### 47.5.11 Example Xmodem Configuration Upload Using HyperTerminal

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

**Figure 384** Example Xmodem Upload

After the configuration upload process has completed, restart the ZyWALL by entering "atgo".



# CHAPTER 48

## System Maintenance Menus 8 to 10

This chapter leads you through SMT menus 24.8 to 24.10.

### 48.1 Command Interpreter Mode

The Command Interpreter (CI) is a part of the main router firmware. The CI provides much of the same functionality as the SMT, while adding some low-level setup and diagnostic functions. Enter the CI from the SMT by selecting menu 24.8. Access can be by Telnet or by a serial connection to the console port, although some commands are only available with a serial connection. See the included disk or [zyxel.com](http://zyxel.com) for more detailed information on CI commands. Enter 8 from **Menu 24 - System Maintenance**.

**Note:** Use of undocumented commands or misconfiguration can damage the unit and possibly render it unusable.

**Figure 385** Command Mode in Menu 24

```
Menu 24 - System Maintenance

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

Enter Menu Selection Number:
```

#### 48.1.1 Command Syntax

The command keywords are in `courier new` font.

Enter the command keywords exactly as shown, do not abbreviate.



The required fields in a command are enclosed in angle brackets <>.

The optional fields in a command are enclosed in square brackets [ ].

The | symbol means “or”.

For example,

```
sys filter netbios config <type> <on|off>
```

means that you must specify the type of netbios filter and whether to turn it on or off.

### 48.1.2 Command Usage

A list of commands can be found by typing `help` or `?` at the command prompt. Always type the full command. Type `exit` to return to the SMT main menu when finished.

**Figure 386** Valid Commands

```
Copyright (c) 1994 - 2005 ZyXEL Communications Corp.
ras> ?
Valid commands are:
sys          ls          exit          device
ether        poe         pptp          aux
config       ip           ipsec         ppp
bridge       bm           certificates  idp
av           as           cnm           8021x
radius
ras>
```

The following table describes some commands in this screen.

**Table 233** Valid Commands

COMMAND	DESCRIPTION
sys	The system commands display device information and configure device settings.
exit	This command returns you to the SMT main menu.
ether	These commands display Ethernet information and configure Ethernet settings.
aux	These commands display dial backup information and control dial backup connections.
ip	These commands display IP information and configure IP settings.
ipsec	These commands display IPSec information and configure IPSec settings.
bridge	These commands display bridge information.
bm	These commands configure bandwidth management settings and display bandwidth management information.
certificates	These commands display certificate information and configure certificate settings.
8021x	These commands configure 802.1x settings and display 802.1x information.
radius	These commands display RADIUS information and configure RADIUS settings.

## 48.2 Call Control Support

The ZyWALL provides two call control functions: budget management and call history. Please note that this menu is only applicable when **Encapsulation** is set to **PPPoE** or **PPTP** in menu 4 or menu 11.1.

The budget management function allows you to set a limit on the total outgoing call time of the ZyWALL within certain times. When the total outgoing call time exceeds the limit, the current call will be dropped and any future outgoing calls will be blocked.

Call history chronicles preceding incoming and outgoing calls.

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

**Figure 387** Call Control

```
Menu 24.9 - System Maintenance - Call Control

1.Budget Management
2.Call History

Enter Menu Selection Number:
```

### 48.2.1 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. Not all fields are available on all models.

**Figure 388** Budget Management

Menu 24.9.1 - Budget Management		
Remote Node	Connection Time/Total Budget	Elapsed Time/Total Period
1.WAN_1	No Budget	No Budget
2.WAN_2	No Budget	No Budget
3.Dial	No Budget	No Budget
Reset Node (0 to update screen):		

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

**Table 234** 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.		

## 48.2.2 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 389** Call History

```

Menu 24.9.2 - Call History

      Phone Number   Dir   Rate #call  Max   Min   Total
1.
2.
3.
4.
5.
6.
7.
8.
9.
10.

Enter Entry to Delete(0 to exit):

```

The following table describes the fields in this screen.

**Table 235** Call History

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

## 48.3 Time and Date Setting

The ZyWALL's Real Time Chip (RTC) keeps track of the time and date. There is also a software mechanism to set the time manually or get the current time and date from an external server when you turn on your ZyWALL. Menu 24.10 allows you to update the time and date settings of your ZyWALL. The real time is then displayed in the ZyWALL error logs and firewall logs.

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

**Figure 390** Menu 24: System Maintenance

```
Menu 24 - System Maintenance

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

Enter Menu Selection Number:
```

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

**Figure 391** Menu 24.10 System Maintenance: Time and Date Setting

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

Time Protocol= NTP (RFC-1305)
Time Server Address= a.ntp.alphazed.net

Current Time:                08 : 24 : 26
New Time (hh:mm:ss):        N/A  N/A  N/A

Current Date:                2005 - 07 - 27
New Date (yyyy-mm-dd):      N/A   N/A  N/A

Time Zone= GMT

Daylight Saving= No
Start Date (mm-nth-week-hr): Jan. - 1st - Sun. - 00
End Date (mm-nth-week-hr):  Jan. - 1st - Sun. - 00

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

The following table describes the fields in this screen.

**Table 236** Menu 24.10 System Maintenance: Time and Date Setting

FIELD	DESCRIPTION
Time Protocol	<p>Enter the time service protocol that your timeserver uses. 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>The default, <b>NTP (RFC-1305)</b>, is similar to <b>Time (RFC-868)</b>.</p> <p>Select <b>Manual</b> to enter the new time and new date manually.</p>
Time Server Address	Enter the IP address or domain name of your timeserver. Check with your ISP/network administrator if you are unsure of this information. The default is tick.stdtime.gov.tw
Current Time	This field displays an updated time only when you reenter this menu.
New Time	Enter the new time in hour, minute and second format. This field is available when you select <b>Manual</b> in the <b>Time Protocol</b> field.
Current Date	This field displays an updated date only when you reenter this menu.
New Date	Enter the new date in year, month and day format. This field is available when you select <b>Manual</b> in the <b>Time Protocol</b> field.
Time Zone	Press [SPACE BAR] and then [ENTER] to set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Saving	Daylight Saving Time is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daylight time in the evenings. If you use daylight savings time, then choose <b>Yes</b> .
Start Date (mm-nth-week-hr)	<p>Configure the day and time when Daylight Saving Time starts if you selected <b>Yes</b> in the <b>Daylight Saving</b> field. The <b>hr</b> field uses the 24 hour format. Here are a couple of examples:</p> <p>Daylight Saving Time starts in most parts of the United States on the first Sunday of April. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select <b>Apr., 1st, Sun.</b> and type 02 in the <b>hr</b> field.</p> <p>Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select <b>Mar., Last, Sun.</b> The time you type in the <b>hr</b> field depends on your time zone. In Germany for instance, you would type 02 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).</p>

**Table 236** Menu 24.10 System Maintenance: Time and Date Setting

FIELD	DESCRIPTION
End Date (mm-nth-week-hr)	<p>Configure the day and time when Daylight Saving Time ends if you selected <b>Yes</b> in the <b>Daylight Saving</b> field. The <b>hr</b> field uses the 24 hour format. Here are a couple of examples:</p> <p>Daylight Saving Time ends in the United States on the last Sunday of October. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select <b>Oct., Last, Sun.</b> and type 02 in the <b>hr</b> field.</p> <p>Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select <b>Oct., Last, Sun.</b> The time you type in the <b>hr</b> field depends on your time zone. In Germany for instance, you would type 02 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).</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.	

# CHAPTER 49

## Remote Management

This chapter covers remote management found in SMT menu 24.11.

### 49.1 Remote Management

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

You may manage your ZyWALL from a remote location via:

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

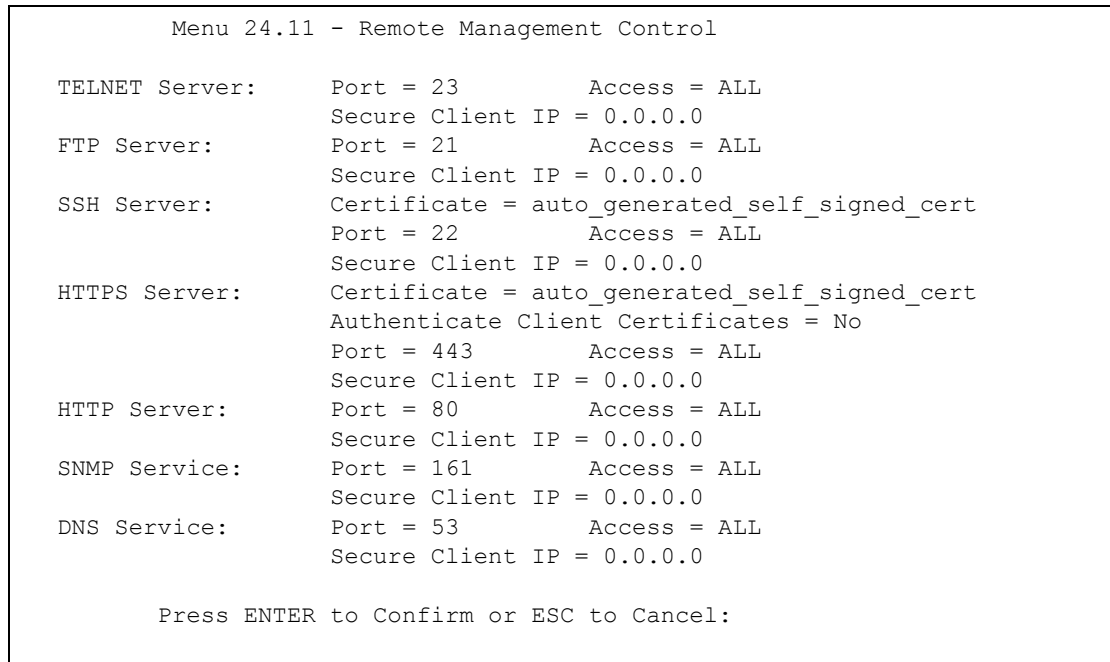
**Note:** When you choose **DMZ only**, **WAN only**, **WLAN only** or **ALL** (LAN & WAN& DMZ& WLAN), you still need to configure a firewall rule to allow access

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

Enter 11 from menu 24 to bring up **Menu 24.11 - Remote Management Control**.



**Figure 392** Menu 24.11 – Remote Management Control



The following table describes the fields in this screen.

**Table 237** Menu 24.11 – Remote Management Control

FIELD	DESCRIPTION
Telnet Server FTP Server SSH Server HTTPS Server HTTP Server SNMP Service DNS Service	Each of these read-only labels denotes a service that you may use to remotely manage the ZyWALL.
Port	This field shows the port number for the service or protocol. You may change the port number if needed, but you must use the same port number to access the ZyWALL.
Access	Select the access interface (if any) by pressing [SPACE BAR], then [ENTER] to choose from: <b>LAN only</b> , <b>WAN only</b> , <b>DMZ only</b> , <b>WLAN only</b> , <b>ALL</b> or <b>Disable</b> .
Secure Client IP	The default 0.0.0.0 allows any client to use this service to remotely manage the ZyWALL. Enter an IP address to restrict access to a client with a matching IP address.
Certificate	Press [SPACE BAR] and then [ENTER] to select the certificate that the ZyWALL will use to identify itself. The ZyWALL is the SSL server and must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the ZyWALL).
Authenticate Client Certificates	Select <b>Yes</b> by pressing [SPACE BAR], then [ENTER] to require the SSL client to authenticate itself to the ZyWALL by sending the ZyWALL a certificate. To do that the SSL client must have a CA-signed certificate from a CA that has been imported as a trusted CA on the ZyWALL (see <a href="#">Appendix L on page 742</a> for details).
Once you have filled in this menu, press [ENTER] at the message "Press ENTER to Confirm or ESC to Cancel" to save your configuration, or press [ESC] to cancel.	

## 49.1.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

- 1** A filter in menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a Telnet, FTP or Web service.
- 2** You have disabled that service in menu 24.11.
- 3** The IP address in the **Secure Client IP** field (menu 24.11) does not match the client IP address. If it does not match, the ZyWALL will disconnect the session immediately.
- 4** There is an SMT console session running.
- 5** There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.
- 6** There is a firewall rule that blocks it.



# CHAPTER 50

## IP Policy Routing

This chapter covers setting and applying policies used for IP routing. This chapter applies to the ZyWALL 35 and ZyWALL 70.

### 50.1 IP Routing Policy Summary

Menu 25 shows the summary of a policy rule, including the criteria and the action of a single policy, and whether a policy is active or not. Each policy contains two lines. The former part is the criteria of the incoming packet and the latter is the action. Between these two parts, separator "|" means the action is taken on criteria matched and separator "=" means the action is taken on criteria not matched.

**Figure 393** Menu 25: Sample IP Routing Policy Summary

```

Menu 25 - IP Routing Policy Summary

#   A   Criteria/Action
-----
001 N SA=1.1.1.1-1.1.1.1 DA=2.2.2.2-2.2.2.5
    SP=20-25 DP=20-25 P=6 T=NM PR=0      |GW=192.168.1.1 T=MT PR=0
002 N _____
003 N _____
004 N _____
005 N _____
006 N _____

          Select Command= None          Select Rule= N/A
          Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.

```

The following table describes the fields in this screen.

**Table 238** Menu 25: Sample IP Routing Policy Summary

FIELD	DESCRIPTION
#	This is the policy index number.
A	This displays whether a policy is active (Y) or not (N).

**Table 238** Menu 25: Sample IP Routing Policy Summary (continued)

FIELD	DESCRIPTION
Criteria/Action	This displays the details about to which packets the policy applies and how the policy has the ZyWALL handle those packets. Refer to <a href="#">Table 239 on page 641</a> for detailed information.
Select Command	<p>Press [SPACE BAR] to choose from <b>None</b>, <b>Edit</b>, <b>Delete</b>, <b>Go To Rule</b>, <b>Next Page</b> or <b>Previous Page</b> and then press [ENTER]. You must select a rule in the next field when you choose the <b>Edit</b>, <b>Delete</b> or <b>Go To</b> commands.</p> <p>Select <b>None</b> and then press [ENTER] to go to the "Press ENTER to Confirm..." prompt.</p> <p>Use <b>Edit</b> to create or edit a rule. Use <b>Delete</b> to remove a rule. To edit or delete a rule, first make sure you are on the correct page. When a rule is deleted, subsequent rules do not move up in the page list.</p> <p>Use <b>Go To Rule</b> to view the page where your desired rule is listed.</p> <p>Select <b>Next Page</b> or <b>Previous Page</b> to view the next or previous page of rules (respectively).</p>
Select Rule	Type the policy index number you wish to edit or delete and then press [ENTER].
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.	

**Table 239** IP Routing Policy Setup

ABBREVIATION	MEANING
<b>Criterion</b> SA	Source IP Address
SP	Source Port
DA	Destination IP Address
DP	Destination Port
P	IP layer 4 protocol number (TCP=6, UDP=17...)
T	Type of service of incoming packet
PR	Precedence of incoming packet
<b>Action</b> GW	Gateway IP address
T	Outgoing Type of service
P	Outgoing Precedence
<b>Service</b> NM	Normal
MD	Minimum Delay
MT	Maximum Throughput
MR	Maximum Reliability
MC	Minimum Cost

## 50.2 IP Routing Policy Setup

To setup a routing policy, perform the following procedures:

- 1 Type 25 in the main menu to open **Menu 25 - IP Routing Policy Summary**.
- 2 Select **Edit** in the **Select Command** field; type the index number of the rule you want to configure in the **Select Rule** field and press [ENTER] to open **Menu 25.1 - IP Routing Policy Setup** (see the next figure).

**Figure 394** Menu 25.1: IP Routing Policy Setup

```

Menu 25.1 - IP Routing Policy Setup

Rule Index= 1                               Active= Yes
Criteria:
  IP Protocol      = 6
  Type of Service = Normal                   Packet length= 40
  Precedence      = 0                       Len Comp= Equal
Source:
  addr start= 1.1.1.1                       end= 1.1.1.1
  port start= 20                             end= 25
Destination:
  addr start= 2.2.2.2                       end= 2.2.2.5
  port start= 20                             end= 25
Action= Matched
  Gateway Type= IP Address
  Gateway addr = 192.168.1.1                Redirect packet= N/A
  Type of Service= Max Thruput              Log= No
  Precedence   = 0
Edit policy to packets received from= No

Press ENTER to Confirm or ESC to Cancel:

```

The following table describes the fields in this screen.

**Table 240** Menu 25.1: IP Routing Policy Setup

FIELD	DESCRIPTION
Rule Index	This is the index number of the routing policy selected in <b>Menu 25 - IP Routing Policy Summary</b> .
Active	Press [SPACE BAR] and then [ENTER] to select <b>Yes</b> to activate the policy.
Criteria	
IP Protocol	Enter a number that represents an IP layer 4 protocol, for example, UDP=17, TCP=6, ICMP=1 and Don't care=0.
Type of Service	Prioritize incoming network traffic by choosing from <b>Don't Care, Normal, Min Delay, Max Thruput</b> or <b>Max Reliable</b> .
Precedence	Precedence value of the incoming packet. Press [SPACE BAR] and then [ENTER] to select a value from <b>0 to 7</b> or <b>Don't Care</b> .
Packet Length	Type the length of incoming packets (in bytes). The operators in the <b>Len Comp</b> (next field) apply to packets of this length.
Len Comp	Press [SPACE BAR] and then [ENTER] to choose from <b>Equal, Not Equal, Less, Greater, Less or Equal</b> or <b>Greater or Equal</b> .
Source	
addr start / end	Source IP address range from start to end.

**Table 240** Menu 25.1: IP Routing Policy Setup

FIELD	DESCRIPTION
port start / end	Source port number range from start to end; applicable only for TCP/UDP.
Destination	
addr start / end	Destination IP address range from start to end.
port start / end	Destination port number range from start to end; applicable only for TCP/UDP.
Action	Specifies whether action should be taken on criteria Matched or Not Matched.
Gateway Type	Press [SPACE BAR] and then [ENTER] to select <b>IP Address</b> and enter the IP address of the gateway if you want to specify the IP address of the gateway. The gateway is an immediate neighbor of your ZyWALL that will forward the packet to the destination. The gateway must be a router on the same segment as your ZyWALL's LAN or WAN port. Press [SPACE BAR] and then [ENTER] to select <b>Remote Node</b> to have the ZyWALL send traffic that matches the policy route through a specific WAN port.
Gateway addr	This field displays if you selected <b>IP Address</b> in the <b>Gateway Type</b> field. Defines the outgoing gateway address. The gateway must be on the same subnet as the ZYWALL if it is on the LAN, otherwise, the gateway must be the IP address of a remote node. The default gateway is specified as 0.0.0.0.
Remote Node Idx	This field displays if you selected <b>Remote Node</b> in the <b>Gateway Type</b> field. Type <b>1</b> for WAN port 1 or <b>2</b> for WAN port 2.
Redirect Packet	This field applies if you selected <b>Remote Node</b> in the <b>Gateway Type</b> field. Press [SPACE BAR] and then [ENTER] to select <b>Yes</b> to have the ZyWALL send traffic that matches the policy route through the other WAN interface if it cannot send the traffic through the WAN interface you selected.
Type of Service	Set the new TOS value of the outgoing packet. Prioritize incoming network traffic by choosing <b>Don't Care</b> , <b>Normal</b> , <b>Min Delay</b> , <b>Max Thruput</b> , <b>Max Reliable</b> or <b>Min Cost</b> .
Precedence	Set the new outgoing packet precedence value. Values are <b>0</b> to <b>7</b> or <b>Don't Care</b> .
Log	Press [SPACE BAR] and then [ENTER] to select <b>Yes</b> to make an entry in the system log when a policy is executed.
Edit policy to packets received from	Press [SPACE BAR] and then [ENTER] to select <b>Yes</b> or <b>No</b> (default). Select <b>Yes</b> to configure Menu 25.1.1: IP Routing Policy Setup discussed next.
When you have completed this menu, press [ENTER] at the prompt "Press [ENTER] to confirm or [ESC] to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

## 50.2.1 Applying Policy to Packets

To apply the policy to packets received on the selected interface(s), go to **Menu 25.1: IP Routing Policy Setup** and press [SPACE BAR] to select **Yes** in the **Edit policy to packets received from** field. Press [ENTER] to display **Menu 25.1.1 - IP Routing Policy Setup** (shown next).

**Figure 395** Menu 25.1.1: IP Routing Policy Setup

```

Menu 25.1.1 - IP Routing Policy Setup

Apply policy to packets received from:
LAN= No
DMZ= No
WLAN= No
ALL WAN= Yes
Selected Remote Node index= N/A

Press ENTER to Confirm or ESC to Cancel:

```

The following table describes the fields in this screen.

**Table 241** Menu 25.1.1: IP Routing Policy Setup

FIELD	DESCRIPTION
LAN/DMZ/WLAN/ ALL WAN	Press [SPACE BAR] to select <b>Yes</b> or <b>No</b> . Choose <b>Yes</b> and press [ENTER] to apply the policy to packets received on the specific interface(s).
Selected Remote Node index	If you select <b>No</b> in the <b>ALL WAN</b> field, enter the number of the WAN port.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.	

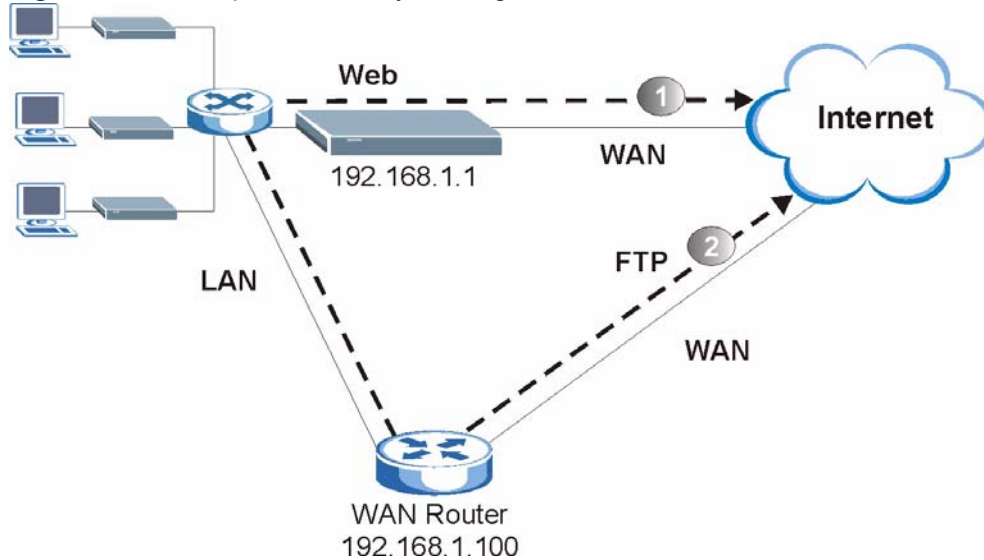
## 50.3 IP Policy Routing Example

If a network has both Internet and remote node connections, you can route Web packets to the Internet using one policy and route FTP packets to a remote network using another policy. See the next figure.

Route 1 represents the default IP route and route 2 represents the configured IP route.



**Figure 396** Example of IP Policy Routing



To force Web packets coming from clients with IP addresses of 192.168.1.33 to 192.168.1.64 to be routed to the Internet via the WAN port of the ZyWALL, follow the steps as shown next.

- 1 Create a rule in **Menu 25.1 - IP Routing Policy Setup** as shown next.

**Figure 397** IP Routing Policy Example 1

```

Menu 25.1 - IP Routing Policy Setup

Rule Index= 1                               Active= Yes
Criteria:
  IP Protocol      = 6
  Type of Service= Don't Care                 Packet length= 10
  Precedence      = Don't Care                 Len Comp= Equal
Source:
  addr start= 192.168.1.33                    end= 192.168.1.64
  port start= 0                               end= N/A
Destination:
  addr start= 0.0.0.0                         end= N/A
  port start= 80                              end= 80
Action= Matched
  Gateway Type= IP Address
  Gateway addr  = 192.168.1.1                 Redirect packet= N/A
  Type of Service= Max Thruput                 Log= No
  Precedence    = 0
Edit policy to packets received from= No

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

- 2 Select **Yes** in the **LAN** field in menu 25.1.1 to apply the policy to packets received on the LAN port.
- 3 Check **Menu 25 - IP Routing Policy Summary** to see if the rule is added correctly.

- 4** Create another rule in menu 25.1 for this rule to route packets from any host (IP=0.0.0.0 means any host) with protocol TCP and port FTP access through another gateway (192.168.1.100).

**Figure 398** IP Routing Policy Example 2

```

Menu 25.1 - IP Routing Policy Setup

Rule Index= 2                               Active= No
Criteria:
  IP Protocol      = 6
  Type of Service= Don't Care                Packet length= 10
  Precedence      = Don't Care                Len Comp= Equal
Source:
  addr start= 0.0.0.0                        end= N/A
  port start= 0                              end= N/A
Destination:
  addr start= 0.0.0.0                        end= N/A
  port start= 20                             end= 21
Action= Matched
  Gateway Type= IP Address
  Gateway addr  = 192.168.1.100             Redirect packet= N/A
  Type of Service= Don't Care             Log= No
  Precedence      = Don't Care
Edit policy to packets received from= No

                                Press ENTER to Confirm or ESC to Cancel:

```

- 5** Select **Yes** in the **LAN** field in menu 25.1.1 to apply the policy to packets received on the LAN port.
- 6** Check **Menu 25 - IP Routing Policy Summary** to see if the rule is added correctly.



# CHAPTER 51

## Call Scheduling

Call scheduling allows you to dictate when a remote node should be called and for how long.

### 51.1 Introduction to Call Scheduling

The call scheduling feature allows the ZyWALL to manage a remote node and dictate when a remote node should be called and for how long. This feature is similar to the scheduler in a videocassette recorder (you can specify a time period for the VCR to record). You can apply up to 4 schedule sets in **Menu 11.1 - Remote Node Profile**. From the main menu, enter **26** to access **Menu 26 - Schedule Setup** as shown next.

**Figure 399** Schedule Setup

Menu 26 - Schedule Setup			
Schedule Set #	Name	Schedule Set #	Name
1	_____	7	_____
2	_____	8	_____
3	_____	9	_____
4	_____	10	_____
5	_____	11	_____
6	_____	12	_____

Enter Schedule Set Number to Configure= 0  
 Edit Name= N/A  
 Press ENTER to Confirm or ESC to Cancel:

Lower numbered sets take precedence over higher numbered sets thereby avoiding scheduling conflicts. For example, if sets 1, 2, 3 and 4 are applied in the remote node, then set 1 will take precedence over set 2, 3 and 4 as the ZyWALL, by default, applies the lowest numbered set first. Set 2 will take precedence over set 3 and 4, and so on.

You can design up to 12 schedule sets but you can only apply up to four schedule sets for a remote node.

**Note:** To delete a schedule set, enter the set number and press [SPACE BAR] and then [ENTER] or [DEL] in the Edit Name field.

To set up a schedule set, select the schedule set you want to setup from menu 26 (1-12) and press [ENTER] to see **Menu 26.1 - Schedule Set Setup** as shown next.

**Figure 400** Schedule Set Setup

```

Menu 26.1 - Schedule Set Setup

Active= Yes
How Often= Once
Start Date (yyyy-mm-dd) = N/A
Once:
    Date (yyyy-mm-dd)= 2000 - 01 - 01
Weekdays:
    Sunday= N/A
    Monday= N/A
    Tuesday= N/A
    Wednesday= N/A
    Thursday= N/A
    Friday= N/A
    Saturday= N/A
Start Time (hh:mm)= 00 : 00
Duration (hh:mm)= 00 : 00
Action= Forced On

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

If a connection has been already established, your ZyWALL will not drop it. Once the connection is dropped manually or it times out, then that remote node can't be triggered up until the end of the **Duration**.

**Table 242** Schedule Set Setup

FIELD	DESCRIPTION
Active	Press [SPACE BAR] to select <b>Yes</b> or <b>No</b> . Choose <b>Yes</b> and press [ENTER] to activate the schedule set.
How Often	Should this schedule set recur weekly or be used just once only? Press [SPACE BAR] and then [ENTER] to select <b>Once</b> or <b>Weekly</b> . Both these options are mutually exclusive. If <b>Once</b> is selected, then all weekday settings are <b>N/A</b> . When <b>Once</b> is selected, the schedule rule deletes automatically after the scheduled time elapses.
Start Date	Enter the start date when you wish the set to take effect in year -month-date format. Valid dates are from the present to 2036-February-5.
Once:	
Date	If you selected <b>Once</b> in the <b>How Often</b> field above, then enter the date the set should activate here in year-month-date format.
Weekdays:	
Day	If you selected <b>Weekly</b> in the <b>How Often</b> field above, then select the day(s) when the set should activate (and recur) by going to that day(s) and pressing [SPACE BAR] to select <b>Yes</b> , then press [ENTER].
Start Time	Enter the start time when you wish the schedule set to take effect in hour-minute format.
Duration	The duration determines how long the ZyWALL is to apply the action configured in the <b>Action</b> field. Enter the maximum length of time in hour-minute format.

**Table 242** Schedule Set Setup (continued)

FIELD	DESCRIPTION
Action	<p><b>Forced On</b> means that the connection is maintained whether or not there is a demand call on the line and will persist for the time period specified in the <b>Duration</b> field.</p> <p><b>Forced Down</b> means that the connection is blocked whether or not there is a demand call on the line.</p> <p><b>Enable Dial-On-Demand</b> means that this schedule permits a demand call on the line.</p> <p><b>Disable Dial-On-Demand</b> means that this schedule prevents a demand call on the line.</p>
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.	

Once your schedule sets are configured, you must then apply them to the desired remote node(s). Enter 11 from the Main Menu and then enter the target remote node index. Press [SPACE BAR] and then [ENTER] to select **PPPoE** in the **Encapsulation** field to make the schedule sets field available as shown next.

**Figure 401** Applying Schedule Set(s) to a Remote Node (PPPoE)

```

Menu 11.1 - Remote Node Profile

Rem Node Name= ChangeMe      Route= IP
Active= Yes

Encapsulation= PPPoE         Edit IP= No
Service Type= Standard       Telco Option:
Service Name=                 Allocated Budget (min)= 0
Outgoing=                     Period(hr)= 0
  My Login=                    Schedules= 1,2,3,4
  My Password= *****        Nailed-Up Connection= No
  Authen= CHAP/PAP

Session Options:
  Edit Filter Sets= No
  Idle Timeout(sec)= 100

Press ENTER to Confirm or ESC to Cancel:

```

You can apply up to four schedule sets, separated by commas, for one remote node. Change the schedule set numbers to your preference(s).

**Figure 402** Applying Schedule Set(s) to a Remote Node (PPTP)

```
Menu 11.1 - Remote Node Profile

Rem Node Name= ChangeMe           Route= IP
Active= Yes

Encapsulation= PPTP              Edit IP= No
Service Type= Standard           Telco Option:
                                   Allocated Budget(min)= 0
                                   Period(hr)= 0
                                   Schedules= 1,2,3,4
                                   Nailed-up Connections= No

Outgoing=
  My Login=
  My Password= *****
  Retype to Confirm= *****
  Authen= CHAP/PAP
PPTP:
  My IP Addr=
  My IP Mask=
  Server IP Addr=
  Connection ID/Name=

                                   Session Options:
                                   Edit Filter Sets= No
                                   Idle Timeout(sec)= 100

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

# CHAPTER 52

## 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.

### 52.1 Problems Starting Up the ZyWALL

**Table 243** Troubleshooting the Start-Up of Your ZyWALL

PROBLEM	CORRECTIVE ACTION	
None of the LEDs turn on when you turn on the ZyWALL.	Make sure that you have the included power adaptor or cord connected to the ZyWALL and to an appropriate power source.	
	If the error persists, you may have a hardware problem. In this case, you should contact your vendor.	
Cannot access the ZyWALL via the console port.	1. Check to see if the ZyWALL is connected to your computer's console port.	
	2. Check to see if the communications program is configured correctly. The communications software should be configured as follows:	VT100 terminal emulation
		9600 bps is the default speed on leaving the factory. Try other speeds in case the speed has been changed.
No parity, 8 data bits, 1 stop bit, data flow set to none.		

### 52.2 Problems with the LAN Interface

**Table 244** Troubleshooting the LAN Interface

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



## 52.3 Problems with the DMZ Interface

**Table 245** Troubleshooting the DMZ Interface

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

## 52.4 Problems with the WAN Interface

**Table 246** Troubleshooting the WAN Interface

PROBLEM	CORRECTIVE ACTION
Cannot get WAN IP address from the ISP.	The ISP provides the WAN IP address after authentication. Authentication may be through the user name and password, the MAC address or the host name. Use the following corrective actions to make sure the ISP can authenticate your connection.
	You need a user name and password if you're using PPPoE or PPTP encapsulation. Make sure that you have entered the correct <b>Service Type</b> , <b>User Name</b> and <b>Password</b> (the user name and password are case sensitive). Refer to <a href="#">Chapter 7 on page 130</a> or <a href="#">Chapter 36 on page 532</a> .
	If your ISP requires MAC address authentication, you should clone the MAC address from your computer on the LAN as the ZyWALL's WAN MAC address. Refer to <a href="#">Chapter 7 on page 130</a> or <a href="#">Chapter 34 on page 514</a> . It is recommended that you clone your computer's MAC address, even if your ISP presently does not require MAC address authentication.
	If your ISP requires host name authentication, configure your computer's name as the ZyWALL's system name. Refer to <a href="#">Chapter 3 on page 84</a> or <a href="#">Chapter 33 on page 508</a> .

## 52.5 Problems Accessing the ZyWALL

**Table 247** Troubleshooting Accessing the ZyWALL

PROBLEM	CORRECTIVE ACTION
Cannot access the ZyWALL.	The default password is "1234". The password field is case sensitive. Make sure that you enter the correct password using the proper casing.
	Use the Reset button to restore the factory default configuration file. This will restore all of the factory defaults including the password. See <a href="#">Section 2.3 on page 67</a> in <a href="#">Chapter 2 on page 66</a> for details.
Cannot access the ZyWALL via the console port.	<ol style="list-style-type: none"> <li>1. Check to see if the ZyWALL is connected to your computer's console port.</li> <li>2. Check to see if the communications program is configured correctly. The communications software should be configured as follows: <ul style="list-style-type: none"> <li>• VT100 terminal emulation.</li> <li>• 9600 bps is the default speed on leaving the factory. Try other speeds in case the speed has been changed.</li> <li>• No parity, 8 data bits, 1 stop bit, data flow set to none.</li> </ul> </li> </ol>
Cannot access the web configurator.	<p>Make sure that there is not an SMT console session running.</p> <p>Use the ZyWALL's WAN IP address when configuring from the WAN. Refer to the instructions on checking your WAN connection.</p> <p>Use the ZyWALL's LAN IP address when configuring from the LAN. Refer to for instructions on checking your LAN connection.</p> <p>Check that you have enabled web service access. If you have configured a secured client IP address, your computer's IP address must match it. Refer to the chapter on remote management for details.</p> <p>Your computer's and the ZyWALL's IP addresses must be on the same subnet for LAN access.</p> <p>If you changed the ZyWALL's LAN IP address, then enter the new one as the URL.</p> <p>Remove any filters in SMT menu 3.1 (LAN) or menu 11.5 (WAN) that block web service.</p> <p>See the following section to check that pop-up windows, JavaScripts and Java permissions are allowed.</p>
	<p>You may also need to clear your Internet browser's cache.</p> <p>In Internet Explorer, click <b>Tools</b> and then <b>Internet Options</b> to open the <b>Internet Options</b> screen.</p> <p>In the <b>General</b> tab, click <b>Delete Files</b>. In the pop-up window, select the <b>Delete all offline content</b> check box and click <b>OK</b>. Click <b>OK</b> in the <b>Internet Options</b> screen to close it.</p>
	<p>If you disconnect your computer from one device and connect it to another device that has the same IP address, your computer's ARP (Address Resolution Protocol) table may contain an entry that maps the management IP address to the previous device's MAC address).</p> <p>In Windows, use <b>arp -d</b> at the command prompt to delete all entries in your computer's ARP table.</p>

### 52.5.1 Pop-up Windows, JavaScripts and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

**Note:** Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

### 52.5.1.1 Internet Explorer Pop-up Blockers

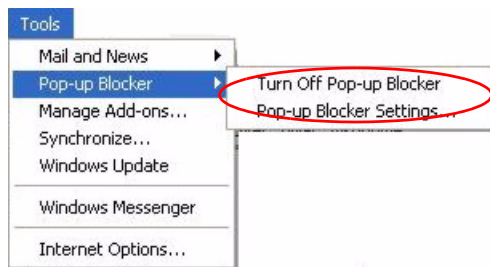
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

#### 52.5.1.1.1 Disable pop-up Blockers

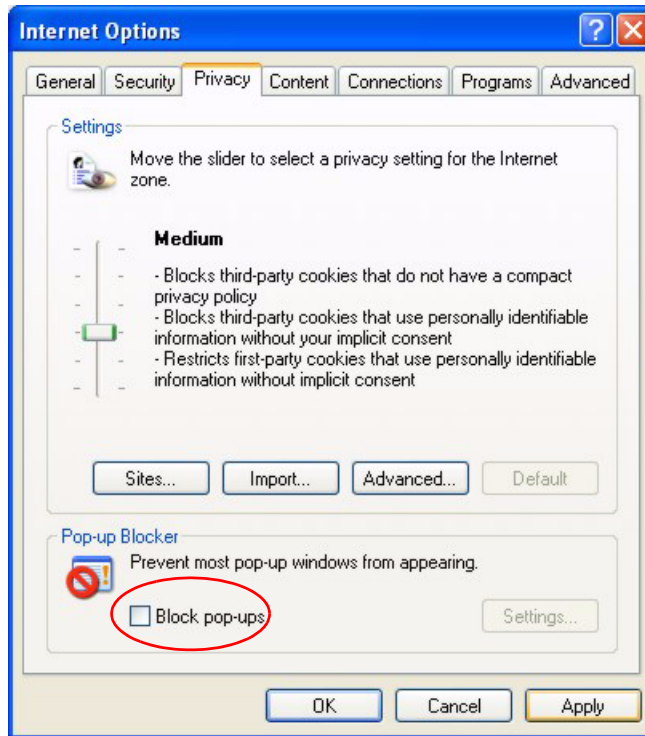
- 1 In Internet Explorer, select **Tools, Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

**Figure 403** Pop-up Blocker



You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

- 1 In Internet Explorer, select **Tools, Internet Options, Privacy**.
- 2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

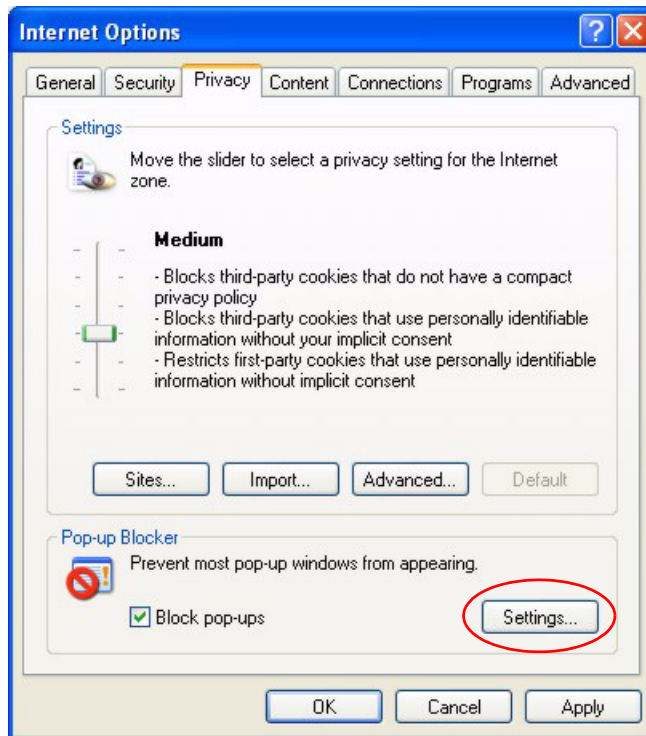
**Figure 404** Internet Options: Privacy

**3** Click **Apply** to save this setting.

#### 52.5.1.1.2 Enable pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

- 1** In Internet Explorer, select **Tools, Internet Options** and then the **Privacy** tab.
- 2** Select **Settings...** to open the **Pop-up Blocker Settings** screen.

**Figure 405** Internet Options: Privacy

- 3** Type the IP address of your device (the web page that you do not want to have blocked) with the prefix “http://”. For example, http://192.168.1.1.
- 4** Click **Add** to move the IP address to the list of **Allowed sites**.

**Figure 406** Pop-up Blocker Settings

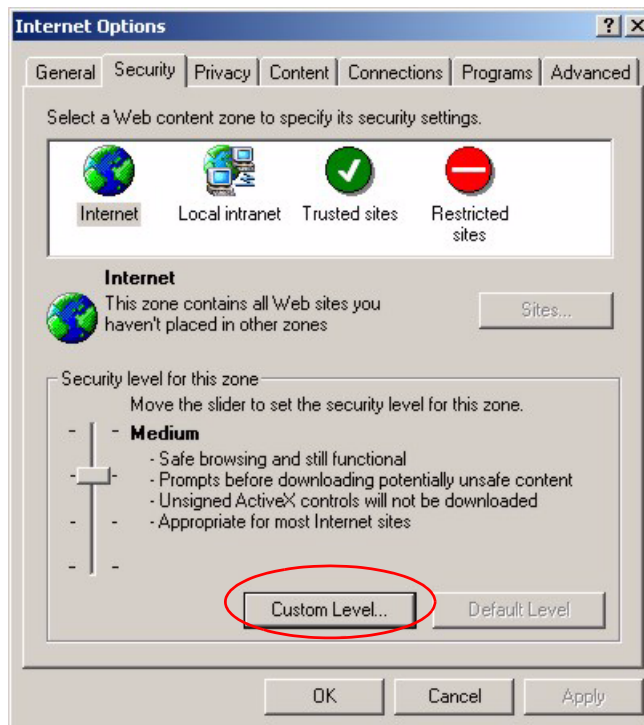
**5** Click **Close** to return to the **Privacy** screen.

**6** Click **Apply** to save this setting.

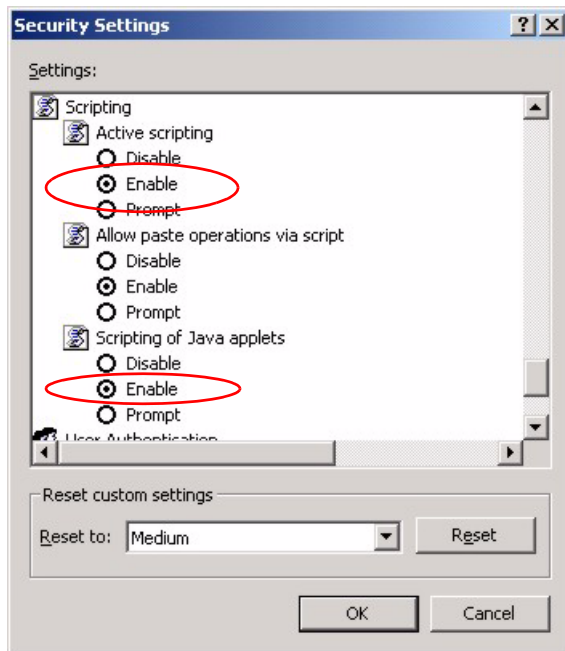
### 52.5.1.2 JavaScripts

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

**1** In Internet Explorer, click **Tools, Internet Options** and then the **Security** tab.

**Figure 407** Internet Options: Security

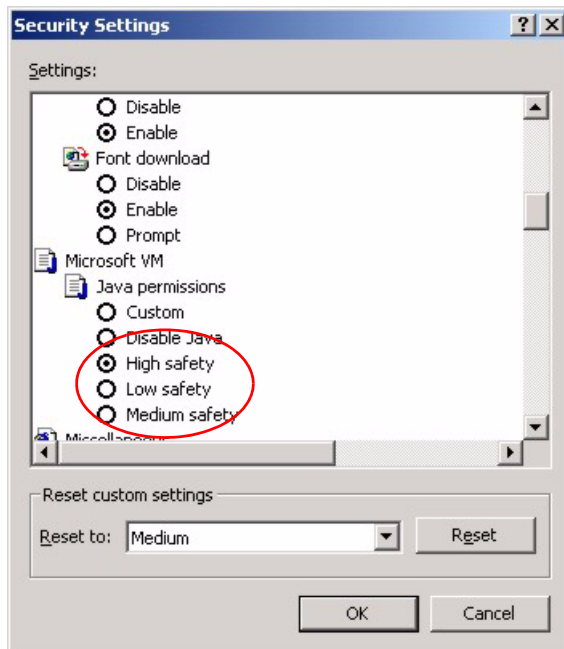
- 2** Click the **Custom Level...** button.
- 3** Scroll down to **Scripting**.
- 4** Under **Active scripting** make sure that **Enable** is selected (the default).
- 5** Under **Scripting of Java applets** make sure that **Enable** is selected (the default).
- 6** Click **OK** to close the window.

**Figure 408** Security Settings - Java Scripting

### 52.5.1.3 Java Permissions

- 1 From Internet Explorer, click **Tools, Internet Options** and then the **Security** tab.
- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Microsoft VM**.
- 4 Under **Java permissions** make sure that a safety level is selected.
- 5 Click **OK** to close the window.

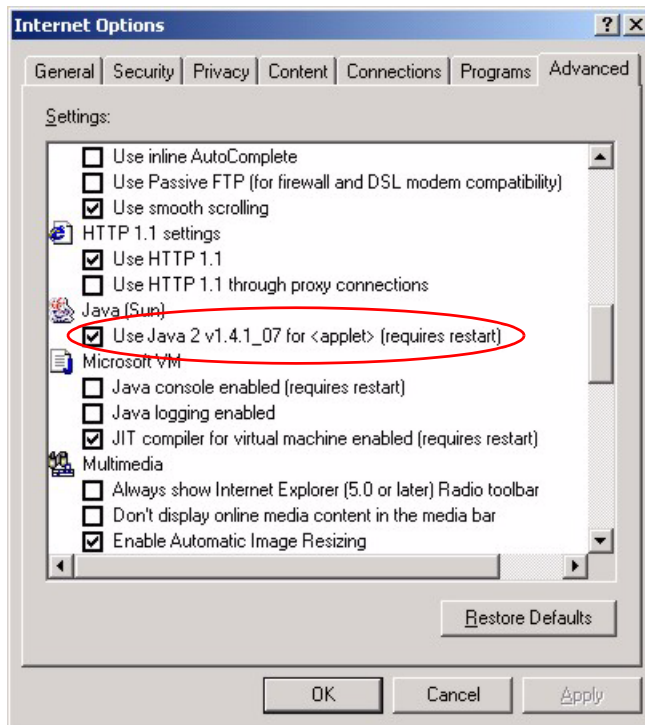


**Figure 409** Security Settings - Java

#### 52.5.1.3.1 JAVA (Sun)

- 1 From Internet Explorer, click **Tools, Internet Options** and then the **Advanced** tab.
- 2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.
- 3 Click **OK** to close the window.

Figure 410 Java (Sun)



## 52.6 Packet Flow

The following is the packet check flow on the ZyWALL.

**LAN/DMZ/WLAN to WAN:** LAN/DMZ Data and Call Filtering (in SMT menu 21) -> Firewall -> IDP -> Anti-Virus -> Anti-Spam -> Remote Node Data Filtering (in SMT menu 21) -> Content Filtering -> NAT

**WAN to LAN/DMZ/WLAN:** Remote Node Data Filtering (in SMT menu 21) -> NAT -> Firewall -> IDP -> Anti-Virus -> Anti-Spam -> LAN/DMZ Data Filtering (in SMT menu 21) -> Content Filtering



# APPENDIX A

## Product Specifications

See also the Introduction chapter for a general overview of the key features.

### Specification Tables

**Table 248** Device Specifications

Default IP Address	192.168.1.1
Default Subnet Mask	255.255.255.0 (24 bits)
Default Password	1234
DHCP Pool	192.168.1.33 to 192.168.1.160
Dimensions	ZyWALL 70: 355(L) x 200(D) x 55(H) mm ZyWALL 5 and ZyWALL 35: 242.0(W) x 175.0(D) x 35.5(H) mm
Weight	ZyWALL 70: 2,600g ZyWALL 5 and ZyWALL 35: 1,200g
Power Specification	ZyWALL 70: 100 ~ 240 VAC ZyWALL 5 and ZyWALL 35: 12V DC
Fuse Specifications	ZyWALL 70: T 0.5 Amp, 250 VAC
Ethernet Interface	
LAN	ZyWALL 70: One auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet port ZyWALL 5 and 35: Four LAN/DMZ auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet ports.
WAN	ZyWALL 35 and 70: Dual auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet ports ZyWALL 5: One auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet port
DMZ	ZyWALL 70: Four auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet ports. ZyWALL 5 and 35: Four LAN/DMZ auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet ports.
Reset Button	Restores factory default settings
Console	RS-232 DB9F
Dial Backup	RS-232 DB9M
Extension Card Slot	For installing an optional ZyXEL wireless LAN card or a ZyWALL Turbo extension card
Operation Temperature	0° C ~ 50° C
Storage Temperature	-30° C ~ 60° C

**Table 248** Device Specifications (continued)

Operation Humidity	20% ~ 95% RH (non-condensing)
Storage Humidity	20% ~ 95% RH (non-condensing)
Certifications	EMC: FCC Class B, CE-EMC Class B, C-Tick Class B, VCCI Class B Safety: CSA International, CE EN60950-1
MTBF (Mean Time Between Failures) (Bellcore model)	ZyWALL 70: 40.9 years ZyWALL 35: 41.8 years ZyWALL 5: 41.7 years

**Table 249** Performance

	ZYWALL 70	ZYWALL 35	ZYWALL 5
Firewall Throughput	100Mbps	90Mbps	80Mbps
VPN 3DES/AES Throughput	50Mbps	40Mbps	25Mbps
User Licenses	Unlimited	Unlimited	Unlimited
Concurrent Sessions	10,000	10,000	4,000
Simultaneous IPSec VPN Connections	100	35	10

**Table 250** Firmware Features

Modes of Operation	Routing/NAT/SUA Mode Transparent Mode
Firewall (ICSA Certified)	IP Protocol/Packet Filter DoS and DDoS Protections Stateful Packet Inspection Real time E-mail alerts Reports and Logs Transparent Firewall
VPN (ICSA Certified)	Manual key, IKE PKI (X.509) Encryption (DES, 3DES and AES) Authentication (SHA-1 and MD5) IPSec NAT Traversal Xauth User Authentication (Internal Database and External RADIUS) DH1/2, RSA signature
Anti-Virus/IDP (Intrusion Detection and Prevention)	Accelerated by a ZyWALL Turbo Card Kaspersky anti-virus signatures Virus, worm, trojan, backdoor, buffer overflow and port scan protection P2P, IM, web attack, protection Automatic scheduled signatures updates Real-time attack alerts and logs

**Table 250** Firmware Features (continued)

Anti-Spam	Spam, Phishing detection Configurable white and black lists SMTP, POP3 support External Spam database
Content Filtering	Web page blocking by URL keyword IKE + PKI support External database content filtering Java/ActiveX /Cookie/News blocking
Traffic Management	Guaranteed/Maximum Bandwidth Policy-based Traffic shaping Priority-bandwidth utilization Load Balancing (for the ZyWALL 35 and ZyWALL 70) Bandwidth Management Static Routes
High Availability (HA)	Auto fail-over, fall-back (for the ZyWALL 35 and ZyWALL 70) Dual WAN ports for WAN backup and Load Balancing (for the ZyWALL 35 and ZyWALL 70) Dial Backup
System Management	Embedded Web Configurator (HTTP and HTTPS) Menu-driven SMT (System Management Terminal) management CLI (Command Line Interpreter) Remote Management via Telnet or Web SNMP manageable Firmware Upgrade (web configurator, TFTP/FTP/SFTP) Vantage CNM
Wireless	IEEE 802.11b Compliant IEEE 802.11g Compliant Frequency Range: 2.4 GHz Advanced Orthogonal Frequency Division Multiplexing (OFDM) IEEE 802.1x Authentication (Internal Database and External RADIUS) Store up to 32 built-in user profiles using EAP-MD5 (Internal Database) External Radius server using EAP-MD5, TLS, TTLS Wired Equivalent Privacy (WEP) Data Encryption 64/128/256 bit MAC Address filters WPA, WPA-PSK
Logging/Monitoring	Centralized Logs Attack alert System status monitoring Syslog

**Table 250** Firmware Features (continued)

Other Protocol Support	PPP (Point-to-Point Protocol) link layer protocol. Transparent bridging for unsupported network layer protocols. DHCP Server/Client/Relay RIP I/RIP II ICMP SNMP v1 and v2c with MIB II support (RFC 1213) IP Multicasting IGMP v1 and v2 IGMP Proxy UPnP
Other Features	Transparent Firewall (Bridge mode) Dynamic DNS IP Alias Static Routes IP Policy Routing (for the ZyWALL 35 and ZyWALL 70)

**Table 251** Feature Specifications

FEATURE	SPECIFICATION		
	ZYWALL 70	ZYWALL 35	ZYWALL 5
Number of Static DHCP Table Entries	128	128	128
Number of Static Routes	50	50	30
Number of Policy Routes	48	48	N/A
Number of Port Forwarding Rules	100	50	30
Number of NAT Sessions	10,000	10,000	4,000
Number of Address Mapping Rules	100	50	30
Number of IPSec VPN Tunnels/Security Associations	100	35	10
Number of Bandwidth Management Classes	100	50	20
Number of Bandwidth Management Class Levels	5	3	1
Number of DNS Address Record Entries	30	30	30
Number of DNS Name Server Record Entries	16	16	16
Number of Concurrent E-mail Sessions with Anti-Spam Enabled	30	15	5
Number of Anti-Spam Whitelist and Blacklist Entries	12,288 Kb. Individual entries may vary in size. The total number you can configure is less than 860.	6,144 Kb. Individual entries may vary in size. The total number you can configure is less than 450.	3,072 Kb. Individual entries may vary in size. The total number you can configure is less than 220.

## Compatible ZyXEL WLAN Cards

The following table lists the ZyXEL WLAN cards that you can use in the ZyWALL at the time of writing. It also shows the security features that each card supports.

**Note:** Check the product page on the [www.zyxel.com](http://www.zyxel.com) website for updates on ZyXEL WLAN cards that you can use in the ZyWALL.

**Table 252** Compatible ZyXEL WLAN Cards and Security Features

	B-100	B-101	B-120	G-100	G-110
No Security	Yes	Yes	Yes	Yes	Yes
Static WEP	Yes	Yes	Yes	Yes	Yes
WPA-PSK	No	No	Yes	Yes	Yes
WPA (MD5 is not supported)	No	No	Yes	Yes	Yes
802.1x + Dynamic WEP (MD5 is not supported)	No	No	Yes	Yes	Yes
802.1x + Static WEP	Yes	Yes	Yes	Yes	Yes
802.1x + No WEP	Yes	Yes	Yes	Yes	Yes
No Access 802.1x + Static WEP	Yes	Yes	Yes	Yes	Yes
No Access 802.1x + No WEP	Yes	Yes	Yes	Yes	Yes

## WLAN Card and ZyWALL Turbo Card Installation

**Note:** Do not insert or remove a card with the ZyWALL turned on.

Make sure the ZyWALL is off before inserting or removing an 802.11b/g-compliant wireless LAN PCMCIA or CardBus card or ZyWALL Turbo Card (to avoid damage). Slide the connector end of the card into the slot as shown next.

**Note:** Only certain ZyXEL wireless LAN cards are compatible with the ZyWALL.

Do not force, bend or twist the wireless LAN card or ZyWALL Turbo Card.



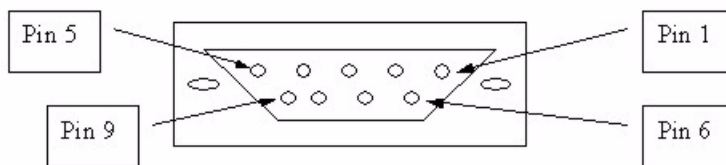
**Figure 411** WLAN Card Installation



## Cable Pin Assignments

In a serial communications connection, generally a computer is DTE (Data Terminal Equipment) and a modem is DCE (Data Circuit-terminating Equipment). The ZyWALL is DCE when you connect a computer to the console port. The ZyWALL is DTE when you connect a modem to the dial backup port.<sup>2</sup>

**Figure 412** Console/Dial Backup Port Pin Layout



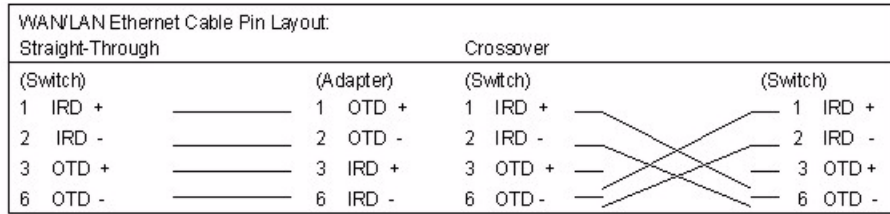

---

2. Pins 2,3 and 5 are used.

**Table 253** Console/Dial Backup Port Pin Assignments

CONSOLE Port RS – 232 (Female) DB-9F	DIAL BACKUP RS – 232 (Male) DB-9M (Not on all models)
Pin 1 = NON Pin 2 = DCE-TXD Pin 3 = DCE –RXD Pin 4 = DCE –DSR Pin 5 = GND Pin 6 = DCE –DTR Pin 7 = DCE –CTS Pin 8 = DCE –RTS PIN 9 = NON	Pin 1 = NON Pin 2 = DTE-RXD Pin 3 = DTE-TXD Pin 4 = DTE-DTR Pin 5 = GND Pin 6 = DTE-DSR Pin 7 = DTE-RTS Pin 8 = DTE-CTS PIN 9 = NON.
The CON/AUX port also has these pin assignments. The CON/AUX switch changes the setting in the firmware only and does not change the CON/AUX port's pin assignments.	ZyWALLs with a CON/AUX port also have a 9-pin adaptor for the console cable with these pin assignments on the male end.

**Figure 413** Ethernet Cable Pin Assignments





# APPENDIX B

## Hardware Installation

The ZyWALL can be placed on a desktop or rack-mounted on a standard EIA rack. Use the brackets in a rack-mounted installation.

### General Installation Instructions

Read all the safety warnings in the beginning of this User's Guide before you begin and make sure you follow them.

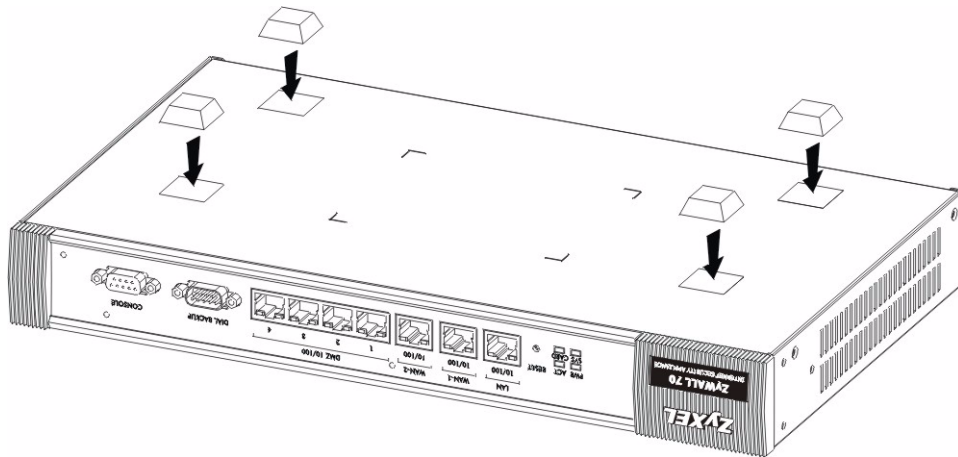
Perform the installation as follows:

- 1 Make sure the ZyWALL is off.
- 2 Install the hardware first.
- 3 See the Quick Start Guide for instructions on making power and panel connections and turning on the ZyWALL.

**Note:** For proper ventilation, allow at least 4 inches (10 cm) of clearance at the front and two sides and 3.4 inches (8 cm) at the back of the ZyWALL. This is especially important for enclosed rack installations.

### Desktop Installation

- 1 Make sure the ZyWALL is clean and dry.
- 2 Set the ZyWALL on a smooth, level surface strong enough to support the weight of the ZyWALL and the connected cables. Make sure there is a power outlet nearby.
- 3 Make sure there is enough clearance around the ZyWALL to allow air circulation and the attachment of cables and the power cord or power adaptor.
- 4 Remove the adhesive backing from the rubber feet.
- 5 Attach the rubber feet to each corner on the bottom of the ZyWALL. These rubber feet help protect the ZyWALL from shock or vibration and ensure space between devices when stacking.

**Figure 414** Attaching Rubber Feet

**Note:** Do not block the ventilation holes. Leave space between ZyWALLs when stacking.

## Rack-mounted Installation Requirements

The ZyWALL can be mounted on an EIA standard size, 19-inch rack or in a wiring closet with other equipment. Follow the steps below to mount your ZyWALL on a standard EIA rack using a rack-mounting kit.

**Note:** Make sure the rack will safely support the combined weight of all the equipment it contains.

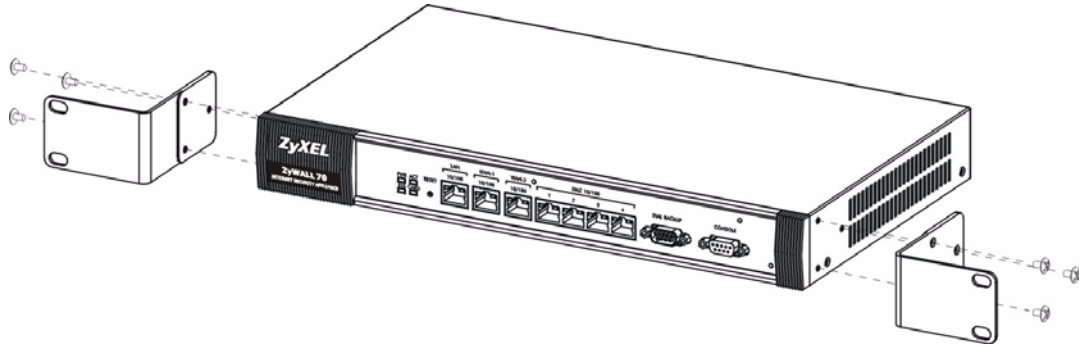
Make sure the position of the ZyWALL does not make the rack unstable or top-heavy. Take all necessary precautions to anchor the rack securely before installing the unit.

Use a #2 Philips screwdriver to install the screws.

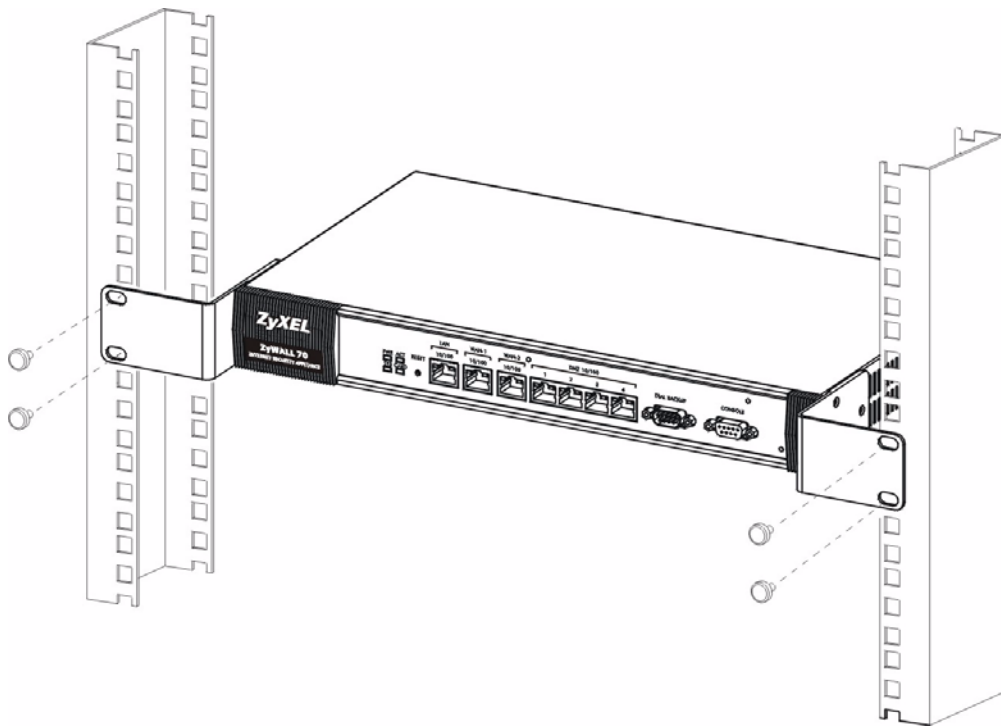
**Note:** Failure to use the proper screws may damage the unit.

## Rack-Mounted Installation

- 1 Align one bracket with the holes on one side of the ZyWALL and secure it with the bracket screws (smaller than the rack-mounting screws).
- 2 Attach the other bracket in a similar fashion.

**Figure 415** Attaching Mounting Brackets and Screws

- 3 After attaching both mounting brackets, position the ZyWALL in the rack by lining up the holes in the brackets with the appropriate holes on the rack. Secure the ZyWALL to the rack with the rack-mounting screws.

**Figure 416** Rack Mounting



# APPENDIX C

## Removing and Installing a Fuse

This appendix shows you how to remove and install fuses for the ZyWALL.

If you need to install a new fuse, follow the procedure below.

**Note:** If you use a fuse other than the included fuses, make sure it matches the fuse specifications in the appendix on product specifications.

### Removing a Fuse

**Note:** Disconnect all power from the ZyWALL before you begin this procedure.

- 1 Place the rear panel of the ZyWALL in front of you.
- 2 Remove the power cord from the back of the unit.
- 3 The fuse housing is located between the power switch and the power port. Use a small flat-head screwdriver to carefully pry out the fuse housing.
- 4 A burnt-out fuse is blackened, darkened or cloudy inside its glass casing. A working fuse has a completely clear glass casing. Pull gently, but firmly, to remove the burnt out fuse from the fuse housing. Dispose of the burnt-out fuse.

### Installing a Fuse

- 1 The ZyWALL is shipped from the factory with one spare fuse included in a box-like section of the fuse housing. Push the middle part of the box-like section to access the spare fuse. Put another spare fuse in its place in order to always have one on hand.
- 2 Push the replacement fuse into the fuse housing until you hear a click.
- 3 Firmly, but gently, push the fuse housing back into the ZYWALL until you hear a click.
- 4 Plug the power cord back into the unit.





# APPENDIX D

## Setting up Your Computer's IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

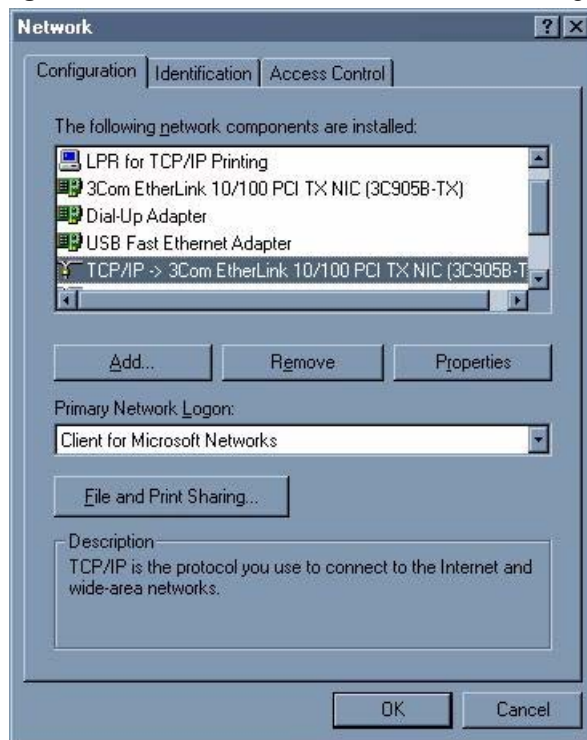
TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the Prestige's LAN port.

### Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window.

**Figure 417** Windows 95/98/Me: Network: Configuration

## Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

- 1 In the **Network** window, click **Add**.
- 2 Select **Adapter** and then click **Add**.
- 3 Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

- 1 In the **Network** window, click **Add**.
- 2 Select **Protocol** and then click **Add**.
- 3 Select **Microsoft** from the list of **manufacturers**.
- 4 Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

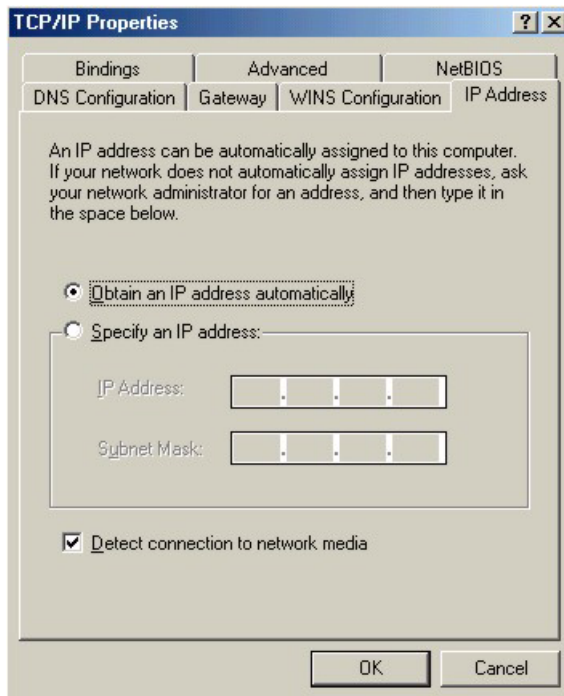
- 1 Click **Add**.
- 2 Select **Client** and then click **Add**.

- 3 Select **Microsoft** from the list of manufacturers.
- 4 Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.
- 5 Restart your computer so the changes you made take effect.

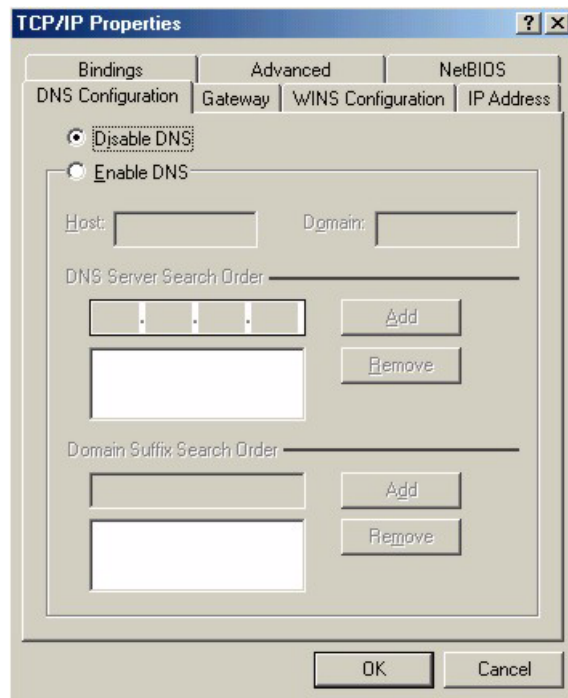
## Configuring

- 1 In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**
- 2 Click the **IP Address** tab.
  - If your IP address is dynamic, select **Obtain an IP address automatically**.
  - If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

**Figure 418** Windows 95/98/Me: TCP/IP Properties: IP Address



- 3 Click the **DNS Configuration** tab.
  - If you do not know your DNS information, select **Disable DNS**.
  - If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).

**Figure 419** Windows 95/98/Me: TCP/IP Properties: DNS Configuration**4** Click the **Gateway** tab.

- If you do not know your gateway's IP address, remove previously installed gateways.
- If you have a gateway IP address, type it in the **New gateway field** and click **Add**.

**5** Click **OK** to save and close the **TCP/IP Properties** window.**6** Click **OK** to close the **Network** window. Insert the Windows CD if prompted.**7** Turn on your Prestige and restart your computer when prompted.

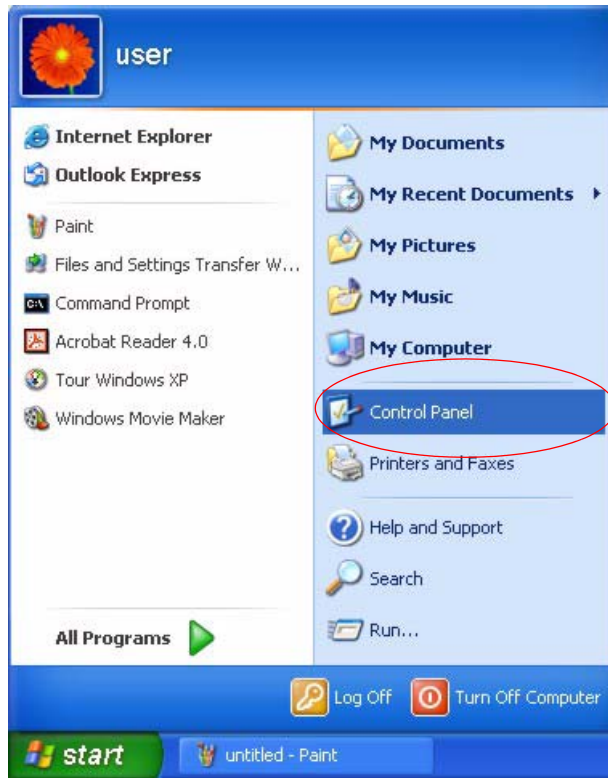
## Verifying Settings

**1** Click **Start** and then **Run**.**2** In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.**3** Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

## Windows 2000/NT/XP

The following example figures use the default Windows XP GUI theme.

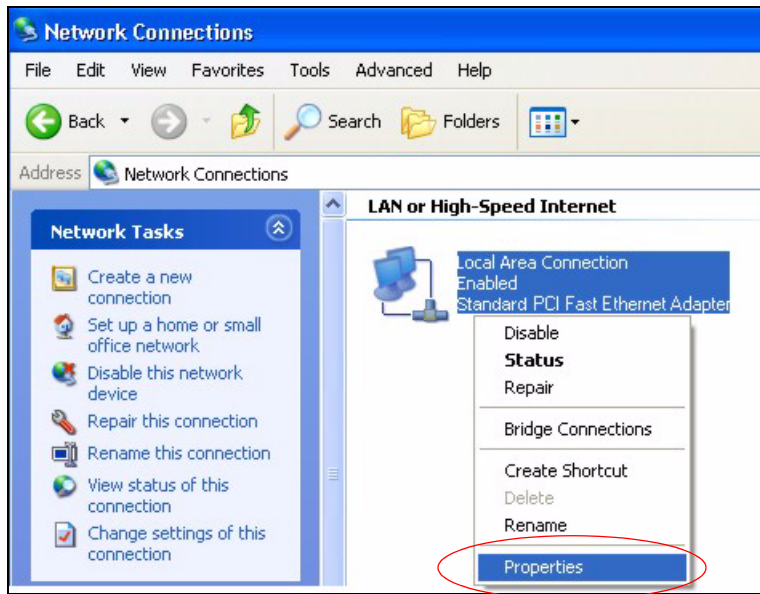
**1** Click **start** (**Start** in Windows 2000/NT), **Settings**, **Control Panel**.

**Figure 420** Windows XP: Start Menu

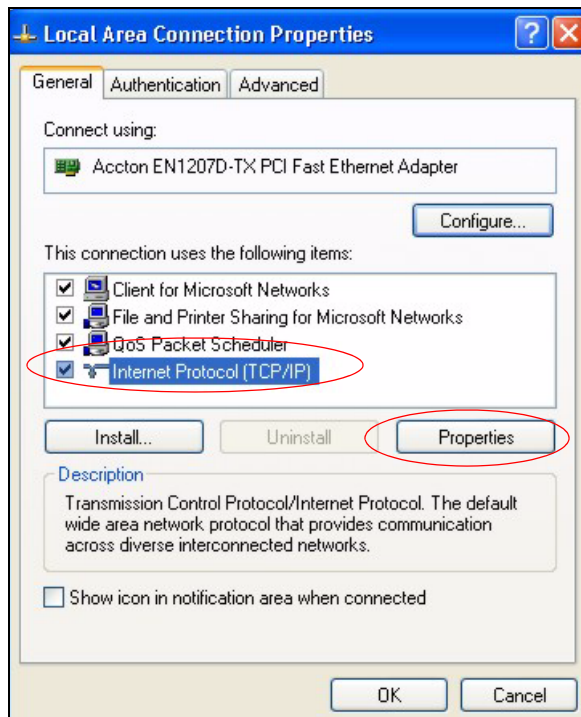
**2** In the **Control Panel**, double-click **Network Connections (Network and Dial-up Connections)** in Windows 2000/NT).

**Figure 421** Windows XP: Control Panel

**3** Right-click **Local Area Connection** and then click **Properties**.

**Figure 422** Windows XP: Control Panel: Network Connections: Properties

- 4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and then click **Properties**.

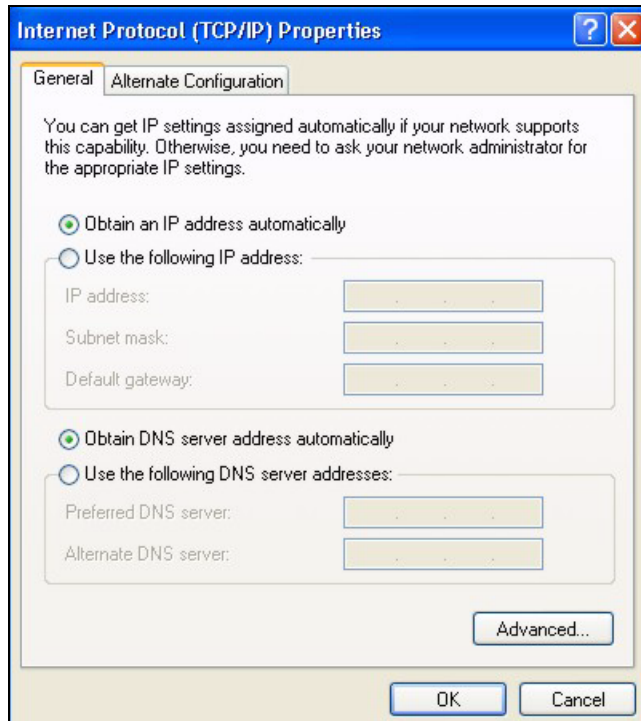
**Figure 423** Windows XP: Local Area Connection Properties

- 5 The **Internet Protocol TCP/IP Properties** window opens (the **General** tab in Windows XP).

- If you have a dynamic IP address click **Obtain an IP address automatically**.

- If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.
- Click **Advanced**.

**Figure 424** Windows XP: Internet Protocol (TCP/IP) Properties

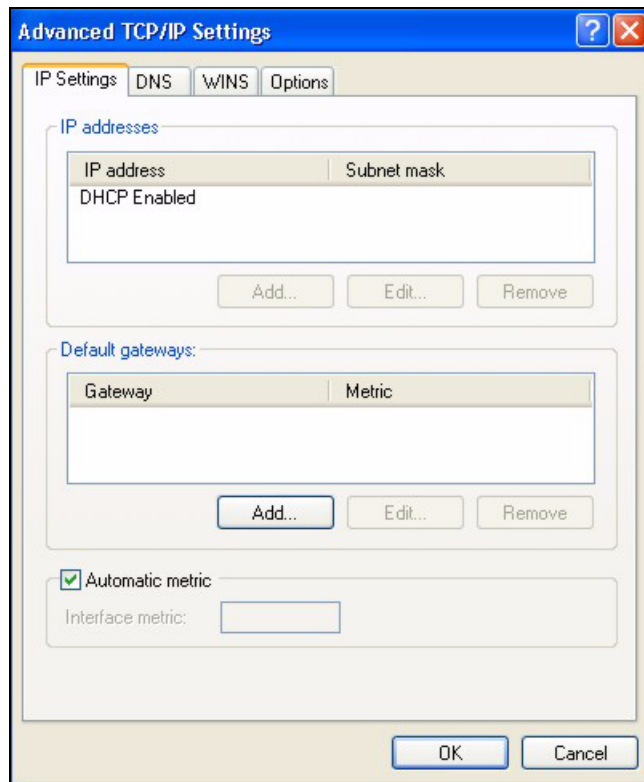


- 6 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.
- Click **OK** when finished.

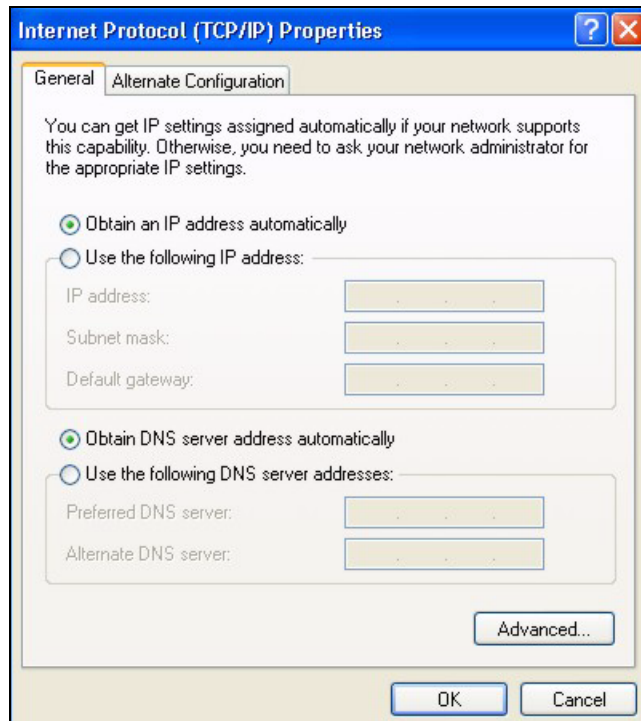


**Figure 425** Windows XP: Advanced TCP/IP Properties

**7** In the **Internet Protocol TCP/IP Properties** window (the **General** tab in Windows XP):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

**Figure 426** Windows XP: Internet Protocol (TCP/IP) Properties

- 8** Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
- 9** Click **Close (OK in Windows 2000/NT)** to close the **Local Area Connection Properties** window.
- 10** Close the **Network Connections** window (**Network and Dial-up Connections** in Windows 2000/NT).
- 11** Turn on your Prestige and restart your computer (if prompted).

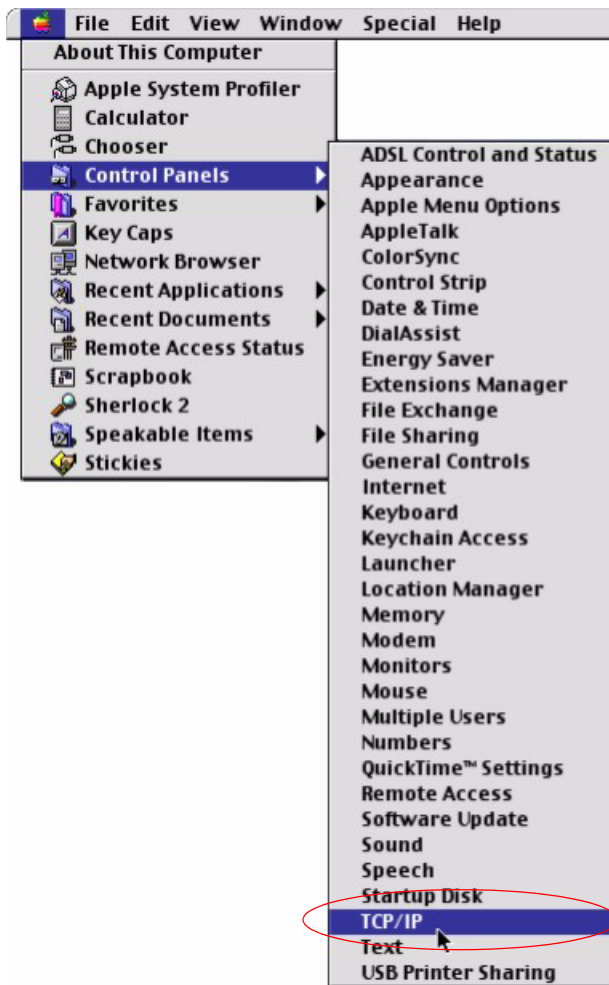
## Verifying Settings

- 1** Click **Start, All Programs, Accessories** and then **Command Prompt**.
- 2** In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

## Macintosh OS 8/9

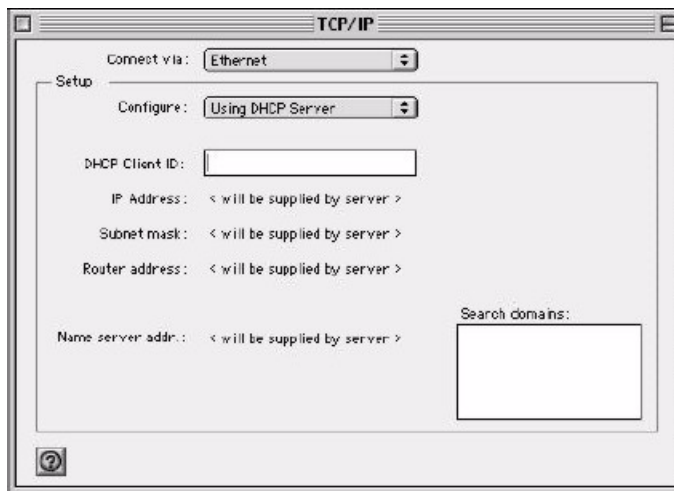
- 1** Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 427 Macintosh OS 8/9: Apple Menu



2 Select **Ethernet built-in** from the **Connect via** list.

Figure 428 Macintosh OS 8/9: TCP/IP



3 For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.

- 4 For statically assigned settings, do the following:
  - From the **Configure** box, select **Manually**.
  - Type your IP address in the **IP Address** box.
  - Type your subnet mask in the **Subnet mask** box.
  - Type the IP address of your Prestige in the **Router address** box.
- 5 Close the **TCP/IP Control Panel**.
- 6 Click **Save** if prompted, to save changes to your configuration.
- 7 Turn on your Prestige and restart your computer (if prompted).

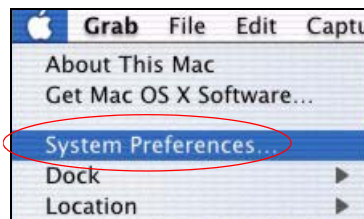
## Verifying Settings

Check your TCP/IP properties in the **TCP/IP Control Panel** window.

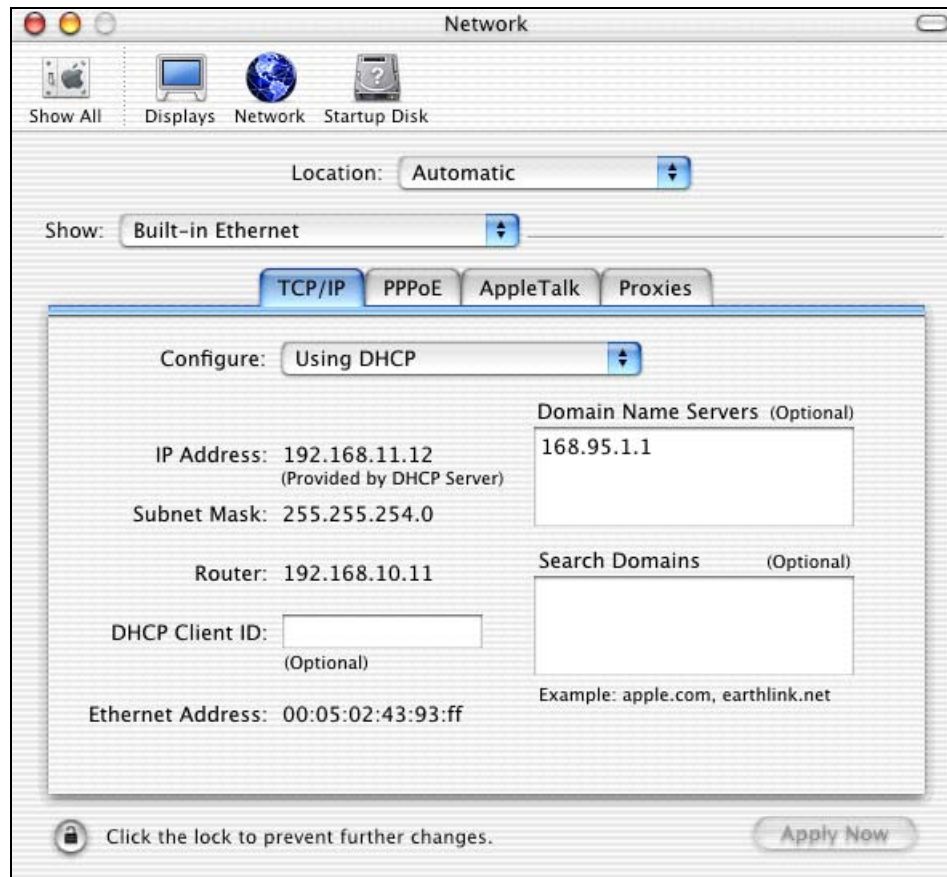
## Macintosh OS X

- 1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

**Figure 429** Macintosh OS X: Apple Menu



- 2 Click **Network** in the icon bar.
  - Select **Automatic** from the **Location** list.
  - Select **Built-in Ethernet** from the **Show** list.
  - Click the **TCP/IP** tab.
- 3 For dynamically assigned settings, select **Using DHCP** from the **Configure** list.

**Figure 430** Macintosh OS X: Network

**4** For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your Prestige in the **Router address** box.

**5** Click **Apply Now** and close the window.

**6** Turn on your Prestige and restart your computer (if prompted).

## Verifying Settings

Check your TCP/IP properties in the **Network** window.

## Linux

This section shows you how to configure your computer's TCP/IP settings in Red Hat Linux 9.0. Procedure, screens and file location may vary depending on your Linux distribution and release version.

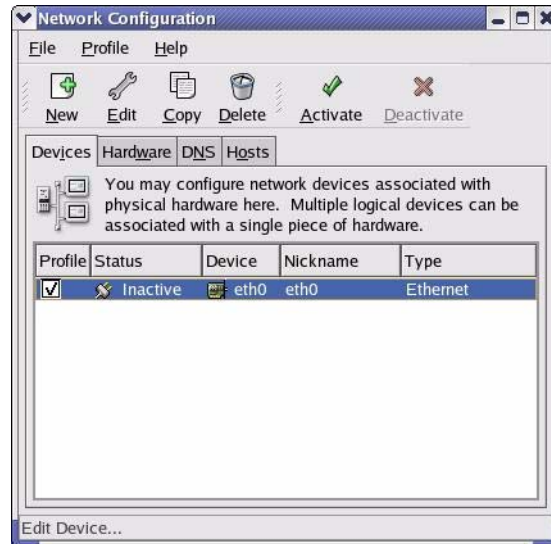
**Note:** Make sure you are logged in as the root administrator.

## Using the K Desktop Environment (KDE)

Follow the steps below to configure your computer IP address using the KDE.

- 1 Click the Red Hat button (located on the bottom left corner), select **System Setting** and click **Network**.

**Figure 431** Red Hat 9.0: KDE: Network Configuration: Devices



- 2 Double-click on the profile of the network card you wish to configure. The **Ethernet Device General** screen displays as shown.

**Figure 432** Red Hat 9.0: KDE: Ethernet Device: General

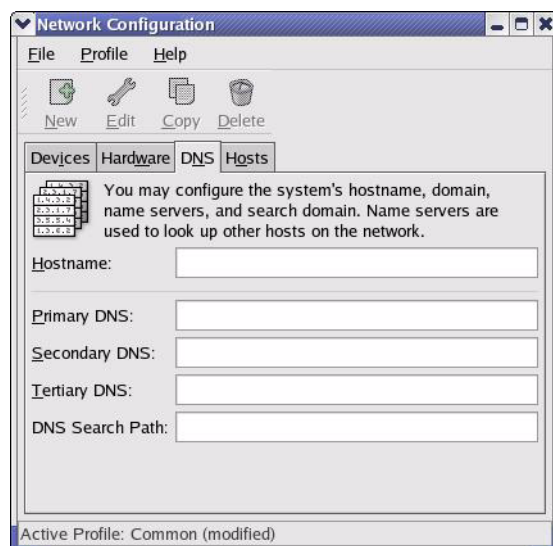


- If you have a dynamic IP address, click **Automatically obtain IP address settings with** and select **dhcp** from the drop down list.
- If you have a static IP address, click **Statically set IP Addresses** and fill in the **Address**, **Subnet mask**, and **Default Gateway Address** fields.

3 Click **OK** to save the changes and close the **Ethernet Device General** screen.

4 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Configuration** screen. Enter the DNS server information in the fields provided.

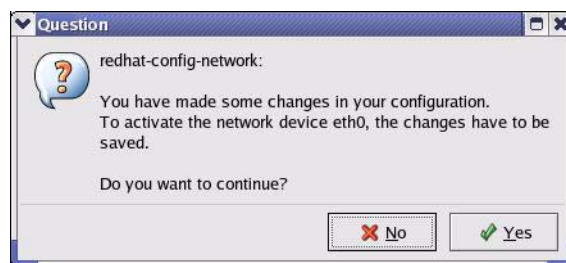
**Figure 433** Red Hat 9.0: KDE: Network Configuration: DNS



5 Click the **Devices** tab.

6 Click the **Activate** button to apply the changes. The following screen displays. Click **Yes** to save the changes in all screens.

**Figure 434** Red Hat 9.0: KDE: Network Configuration: Activate



7 After the network card restart process is complete, make sure the **Status** is **Active** in the **Network Configuration** screen.

## Using Configuration Files

Follow the steps below to edit the network configuration files and set your computer IP address.

**1** Assuming that you have only one network card on the computer, locate the `ifconfig-eth0` configuration file (where `eth0` is the name of the Ethernet card). Open the configuration file with any plain text editor.

- If you have a dynamic IP address, enter **dhcp** in the `BOOTPROTO=` field. The following figure shows an example.

**Figure 435** Red Hat 9.0: Dynamic IP Address Setting in `ifconfig-eth0`

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

- If you have a static IP address, enter **static** in the `BOOTPROTO=` field. Type `IPADDR=` followed by the IP address (in dotted decimal notation) and type `NETMASK=` followed by the subnet mask. The following example shows an example where the static IP address is 192.168.1.10 and the subnet mask is 255.255.255.0.

**Figure 436** Red Hat 9.0: Static IP Address Setting in `ifconfig-eth0`

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.1.10
NETMASK=255.255.255.0
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

**2** If you know your DNS server IP address(es), enter the DNS server information in the `resolv.conf` file in the `/etc` directory. The following figure shows an example where two DNS server IP addresses are specified.

**Figure 437** Red Hat 9.0: DNS Settings in `resolv.conf`

```
nameserver 172.23.5.1
nameserver 172.23.5.2
```

**3** After you edit and save the configuration files, you must restart the network card. Enter `./network restart` in the `/etc/rc.d/init.d` directory. The following figure shows an example.



**Figure 438** Red Hat 9.0: Restart Ethernet Card

```
[root@localhost init.d]# network restart

Shutting down interface eth0:                [OK]
Shutting down loopback interface:           [OK]
Setting network parameters:                 [OK]
Bringing up loopback interface:             [OK]
Bringing up interface eth0:                 [OK]
```

## Verifying Settings

Enter `ifconfig` in a terminal screen to check your TCP/IP properties.

**Figure 439** Red Hat 9.0: Checking TCP/IP Properties

```
[root@localhost]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:BA:72:5B:44
          inet addr:172.23.19.129  Bcast:172.23.19.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:717 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:730412 (713.2 Kb)  TX bytes:1570 (1.5 Kb)
          Interrupt:10 Base address:0x1000
[root@localhost]#
```

# APPENDIX E

## IP Subnetting

### IP Addressing

Routers “route” based on the network number. The router that delivers the data packet to the correct destination host uses the host ID.

### IP Classes

An IP address is made up of four octets (eight bits), written in dotted decimal notation, for example, 192.168.1.1. IP addresses are categorized into different classes. The class of an address depends on the value of its first octet.

- Class “A” addresses have a 0 in the left most bit. In a class “A” address the first octet is the network number and the remaining three octets make up the host ID.
- Class “B” addresses have a 1 in the left most bit and a 0 in the next left most bit. In a class “B” address the first two octets make up the network number and the two remaining octets make up the host ID.
- Class “C” addresses begin (starting from the left) with 1 1 0. In a class “C” address the first three octets make up the network number and the last octet is the host ID.
- Class “D” addresses begin with 1 1 1 0. Class “D” addresses are used for multicasting. (There is also a class “E” address. It is reserved for future use.)

**Table 254** Classes of IP Addresses

IP ADDRESS:		OCTET 1	OCTET 2	OCTET 3	OCTET 4
Class A	0	Network number	Host ID	Host ID	Host ID
Class B	10	Network number	Network number	Host ID	Host ID
Class C	110	Network number	Network number	Network number	Host ID

**Note:** Host IDs of all zeros or all ones are not allowed.

Therefore:

A class “C” network (8 host bits) can have  $2^8 - 2$  or 254 hosts.

A class “B” address (16 host bits) can have  $2^{16} - 2$  or 65534 hosts.

A class “A” address (24 host bits) can have  $2^{24} - 2$  hosts (approximately 16 million hosts).

Since the first octet of a class “A” IP address must contain a “0”, the first octet of a class “A” address can have a value of 0 to 127.

Similarly the first octet of a class “B” must begin with “10”, therefore the first octet of a class “B” address has a valid range of 128 to 191. The first octet of a class “C” address begins with “110”, and therefore has a range of 192 to 223.

**Table 255** Allowed IP Address Range By Class

CLASS	ALLOWED RANGE OF FIRST OCTET (BINARY)	ALLOWED RANGE OF FIRST OCTET (DECIMAL)
Class A	00000000 to 01111111	0 to 127
Class B	10000000 to 10111111	128 to 191
Class C	11000000 to 11011111	192 to 223
Class D	11100000 to 11101111	224 to 239

## Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). A subnet mask has 32 is a “1” then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is “0” then the corresponding bit in the IP address is part of the host ID.

Subnet masks are expressed in dotted decimal notation just as IP addresses are. The “natural” masks for class A, B and C IP addresses are as follows.

**Table 256** “Natural” Masks

CLASS	NATURAL MASK
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

## Subnetting

With subnetting, the class arrangement of an IP address is ignored. For example, a class C address no longer has to have 24 bits of network number and 8 bits of host ID. With subnetting, some of the host ID bits are converted into network number bits. By convention, subnet masks always consist of a continuous sequence of ones beginning from the left most bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a “/” followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with mask 255.255.255.128.

The following table shows all possible subnet masks for a class “C” address using both notations.

**Table 257** Alternative Subnet Mask Notation

SUBNET MASK IP ADDRESS	SUBNET MASK “1” BITS	LAST OCTET BIT VALUE
255.255.255.0	/24	0000 0000
255.255.255.128	/25	1000 0000
255.255.255.192	/26	1100 0000
255.255.255.224	/27	1110 0000
255.255.255.240	/28	1111 0000
255.255.255.248	/29	1111 1000
255.255.255.252	/30	1111 1100

The first mask shown is the class “C” natural mask. Normally if no mask is specified it is understood that the natural mask is being used.

## Example: Two Subnets

As an example, you have a class “C” address 192.168.1.0 with subnet mask of 255.255.255.0.

**Table 258** Two Subnets Example

	NETWORK NUMBER	HOST ID
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask	255.255.255.	0
Subnet Mask (Binary)	11111111.11111111.11111111.	00000000

The first three octets of the address make up the network number (class “C”). You want to have two separate networks.

Divide the network 192.168.1.0 into two separate subnets by converting one of the host ID bits of the IP address to a network number bit. The “borrowed” host ID bit can be either “0” or “1” thus giving two subnets; 192.168.1.0 with mask 255.255.255.128 and 192.168.1.128 with mask 255.255.255.128.

**Note:** In the following charts, shaded/bolded last octet bit values indicate host ID bits “borrowed” to form network ID bits. The number of “borrowed” host ID bits determines the number of subnets you can have. The remaining number of host ID bits (after “borrowing”) determines the number of hosts you can have on each subnet.

**Table 259** Subnet 1

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	<b>00000000</b>
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	<b>10000000</b>
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

**Table 260** Subnet 2

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	<b>10000000</b>
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	<b>10000000</b>
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

The remaining 7 bits determine the number of hosts each subnet can have. Host IDs of all zeros represent the subnet itself and host IDs of all ones are the broadcast address for that subnet, so the actual number of hosts available on each subnet in the example above is  $2^7 - 2$  or 126 hosts for each subnet.

192.168.1.0 with mask 255.255.255.128 is the subnet itself, and 192.168.1.127 with mask 255.255.255.128 is the directed broadcast address for the first subnet. Therefore, the lowest IP address that can be assigned to an actual host for the first subnet is 192.168.1.1 and the highest is 192.168.1.126. Similarly the host ID range for the second subnet is 192.168.1.129 to 192.168.1.254.

## Example: Four Subnets

The above example illustrated using a 25-bit subnet mask to divide a class “C” address space into two subnets. Similarly to divide a class “C” address into four subnets, you need to “borrow” two host ID bits to give four possible combinations of 00, 01, 10 and 11. The subnet mask is 26 bits (11111111.11111111.11111111.11000000) or 255.255.255.192. Each subnet contains 6 host ID bits, giving  $2^6-2$  or 62 hosts for each subnet (all 0’s is the subnet itself, all 1’s is the broadcast address on the subnet).

**Table 261** Subnet 1

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

**Table 262** Subnet 2

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	01000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

**Table 263** Subnet 3

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	10000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

**Table 264** Subnet 4

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	11000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

## Example Eight Subnets

Similarly use a 27-bit mask to create 8 subnets (001, 010, 011, 100, 101, 110).

The following table shows class C IP address last octet values for each subnet.

**Table 265** Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

The following table is a summary for class “C” subnet planning.

**Table 266** Class C Subnet Planning

NO. “BORROWED” HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

## Subnetting With Class A and Class B Networks.

For class “A” and class “B” addresses the subnet mask also determines which bits are part of the network number and which are part of the host ID.

A class “B” address has two host ID octets available for subnetting and a class “A” address has three host ID octets (see [Table 254 on page 694](#)) available for subnetting.

The following table is a summary for class “B” subnet planning.

**Table 267** Class B Subnet Planning

NO. “BORROWED” HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1





# APPENDIX F

## PPPoE

### PPPoE in Action

An ADSL modem bridges a PPP session over Ethernet (PPP over Ethernet, RFC 2516) from your computer to an ATM PVC (Permanent Virtual Circuit) which connects to a DSL Access Concentrator where the PPP session terminates (see [Figure 440 on page 703](#)). One PVC can support any number of PPP sessions from your LAN. PPPoE provides access control and billing functionality in a manner similar to dial-up services using PPP.

### Benefits of PPPoE

PPPoE offers the following benefits:

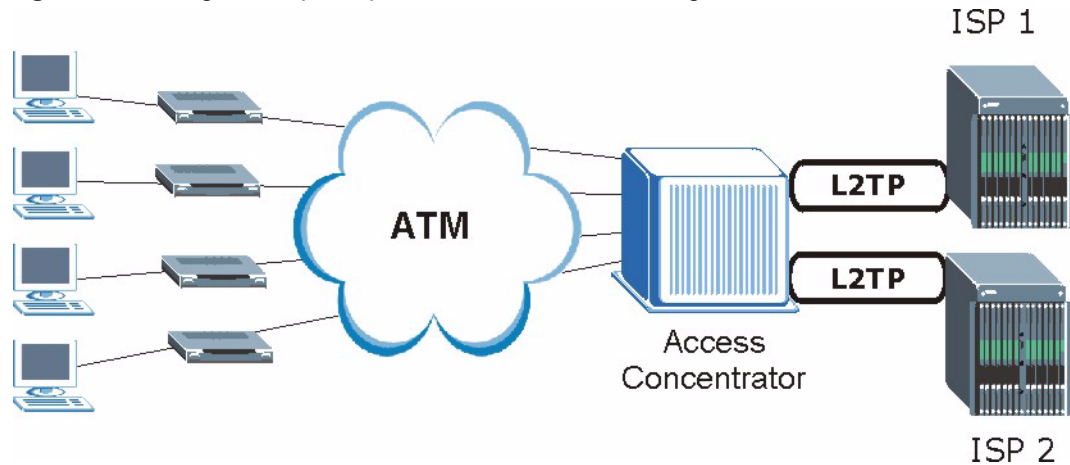
It provides you with a familiar dial-up networking (DUN) user interface.

It lessens the burden on the carriers of provisioning virtual circuits all the way to the ISP on multiple switches for thousands of users. For GSTN (PSTN and ISDN), the switching fabric is already in place.

It allows the ISP to use the existing dial-up model to authenticate and (optionally) to provide differentiated services.

### Traditional Dial-up Scenario

The following diagram depicts a typical hardware configuration where the computers use traditional dial-up networking.

**Figure 440** Single-Computer per Router Hardware Configuration

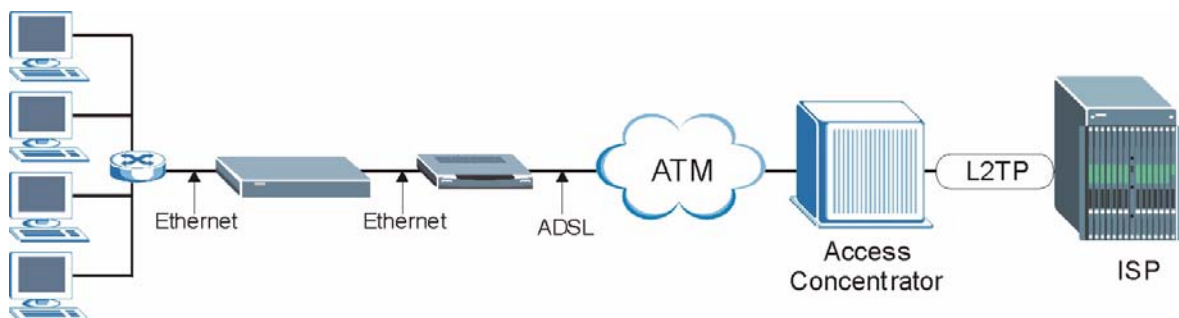
## How PPPoE Works

The PPPoE driver makes the Ethernet appear as a serial link to the computer and the computer runs PPP over it, while the modem bridges the Ethernet frames to the Access Concentrator (AC). Between the AC and an ISP, the AC is acting as a L2TP (Layer 2 Tunneling Protocol) LAC (L2TP Access Concentrator) and tunnels the PPP frames to the ISP. The L2TP tunnel is capable of carrying multiple PPP sessions.

With PPPoE, the VC (Virtual Circuit) is equivalent to the dial-up connection and is between the modem and the AC, as opposed to all the way to the ISP. However, the PPP negotiation is between the computer and the ISP.

## ZyWALL as a PPPoE Client

When using the ZyWALL as a PPPoE client, the computers on the LAN see only Ethernet and are not aware of PPPoE. This alleviates the administrator from having to manage the PPPoE clients on the individual computers.

**Figure 441** ZyWALL as a PPPoE Client

# APPENDIX G

## PPTP

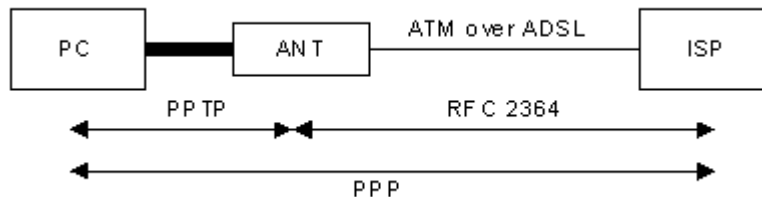
### What is PPTP?

PPTP (Point-to-Point Tunneling Protocol) is a Microsoft proprietary protocol (RFC 2637 for PPTP is informational only) to tunnel PPP frames.

### How can we transport PPP frames from a computer to a broadband modem over Ethernet?

A solution is to build PPTP into the ANT (ADSL Network Termination) where PPTP is used only over the short haul between the computer and the modem over Ethernet. For the rest of the connection, the PPP frames are transported with PPP over AAL5 (RFC 2364). The PPP connection, however, is still between the computer and the ISP. The various connections in this setup are depicted in the following diagram. The drawback of this solution is that it requires one separate ATM VC per destination.

**Figure 442** Transport PPP frames over Ethernet



### PPTP and the ZyWALL

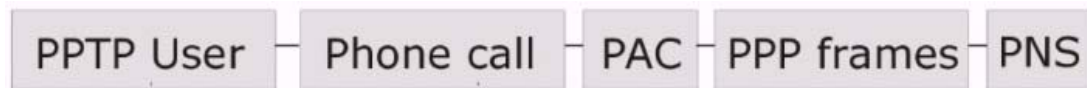
When the ZyWALL is deployed in such a setup, it appears as a computer to the ANT.

In Windows VPN or PPTP Pass-Through feature, the PPTP tunneling is created from Windows 95, 98 and NT clients to an NT server in a remote location. The pass-through feature allows users on the network to access a different remote server using the ZyWALL's Internet connection. In SUA/NAT mode, the ZyWALL is able to pass the PPTP packets to the internal PPTP server (i.e. NT server) behind the NAT. You need to configure port forwarding for port 1723 to have the ZyWALL forward PPTP packets to the server. In the case above as the remote PPTP Client initializes the PPTP connection, the user must configure the PPTP clients. The ZyWALL initializes the PPTP connection hence; there is no need to configure the remote PPTP clients.

## PPTP Protocol Overview

PPTP is very similar to L2TP, since L2TP is based on both PPTP and L2F (Cisco's Layer 2 Forwarding). Conceptually, there are three parties in PPTP, namely the PNS (PPTP Network Server), the PAC (PPTP Access Concentrator) and the PPTP user. The PNS is the box that hosts both the PPP and the PPTP stacks and forms one end of the PPTP tunnel. The PAC is the box that dials/answers the phone calls and relays the PPP frames to the PNS. The PPTP user is not necessarily a PPP client (can be a PPP server too). Both the PNS and the PAC must have IP connectivity; however, the PAC must in addition have dial-up capability. The phone call is between the user and the PAC and the PAC tunnels the PPP frames to the PNS. The PPTP user is unaware of the tunnel between the PAC and the PNS.

**Figure 443** PPTP Protocol Overview



Microsoft includes PPTP as a part of the Windows OS. In Microsoft's implementation, the computer, and hence the ZyWALL, is the PNS that requests the PAC (the ANT) to place an outgoing call over AAL5 to an RFC 2364 server.

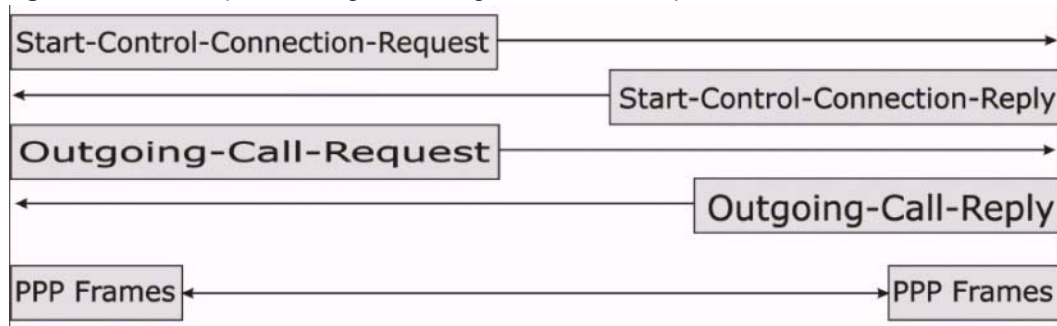
## Control & PPP Connections

Each PPTP session has distinct control connection and PPP data connection.

### Call Connection

The control connection runs over TCP. Similar to L2TP, a tunnel control connection is first established before call control messages can be exchanged. Please note that a tunnel control connection supports multiple call sessions.

The following diagram depicts the message exchange of a successful call setup between a computer and an ANT.

**Figure 444** Example Message Exchange between Computer and an ANT

## PPP Data Connection

The PPP frames are tunneled between the PNS and PAC over GRE (General Routing Encapsulation, RFC 1701, 1702). The individual calls within a tunnel are distinguished using the Call ID field in the GRE header.



# APPENDIX H

## Wireless LANs

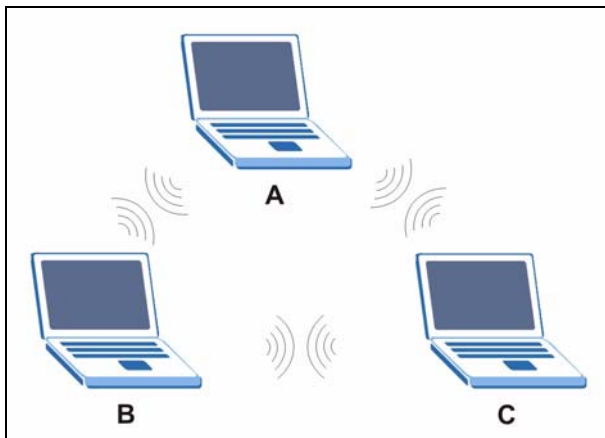
### Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

#### Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless stations (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an Ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an Ad-hoc wireless LAN.

**Figure 445** Peer-to-Peer Communication in an Ad-hoc Network

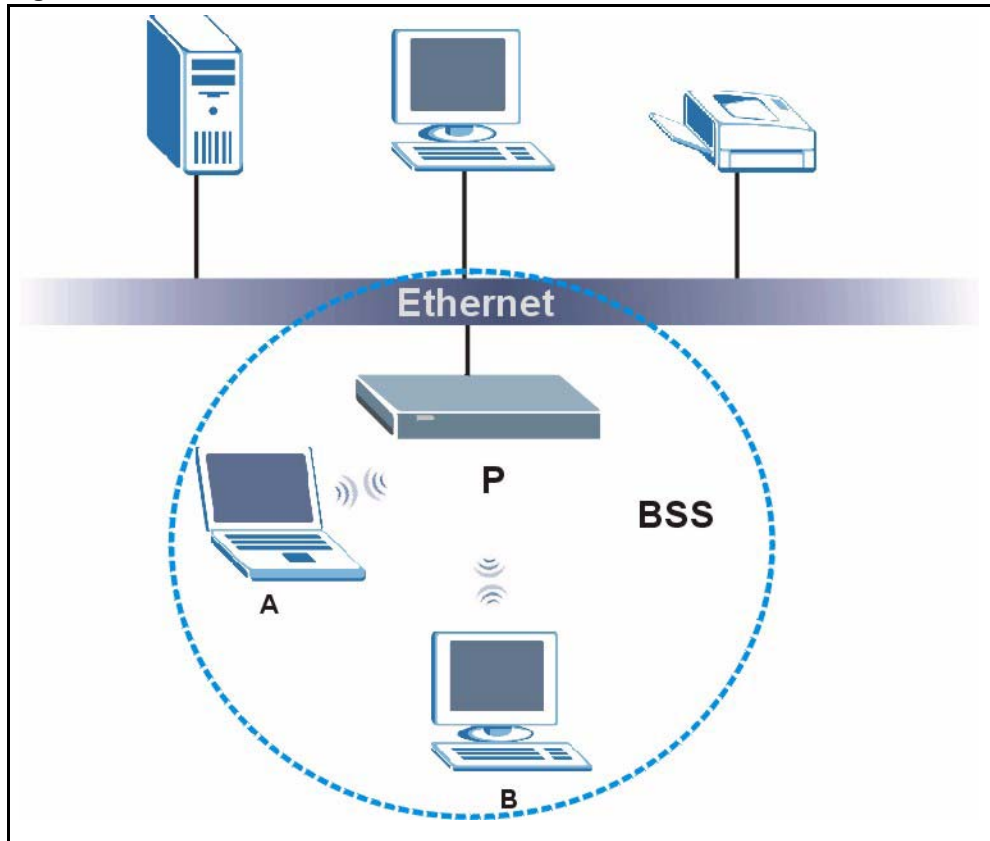


#### BSS

A Basic Service Set (BSS) exists when all communications between wireless stations or between a wireless station and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless stations in the BSS. When Intra-BSS is enabled, wireless station A and B can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless station A and B can still access the wired network but cannot communicate with each other.



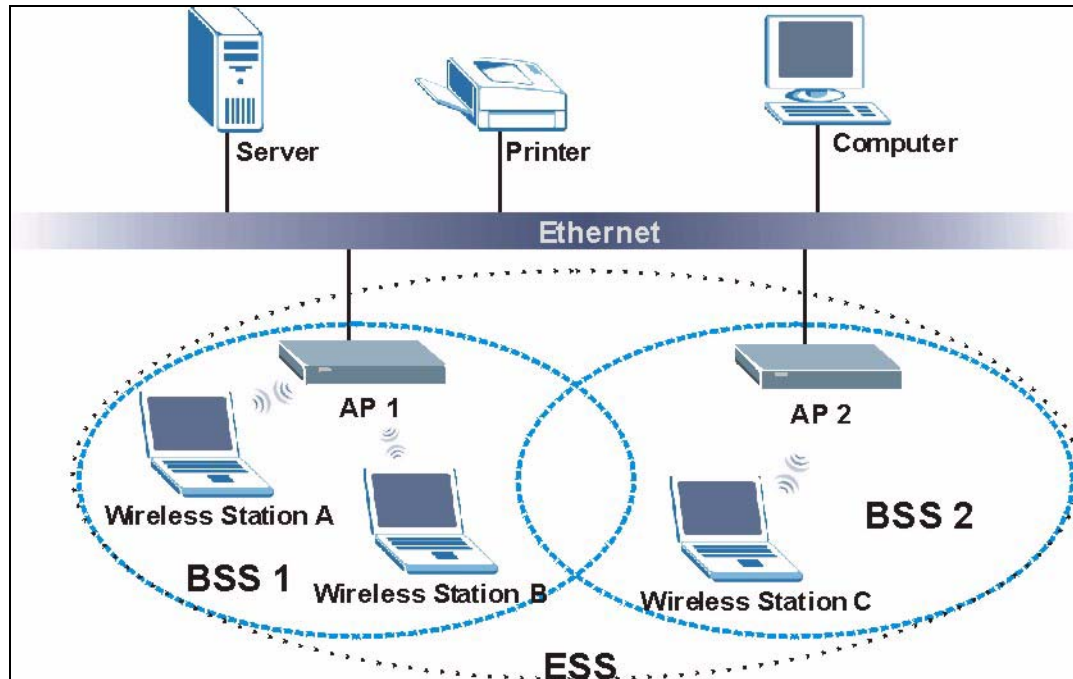
**Figure 446** Basic Service Set

## ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless stations within the same ESS must have the same ESSID in order to communicate.

**Figure 447** Infrastructure WLAN

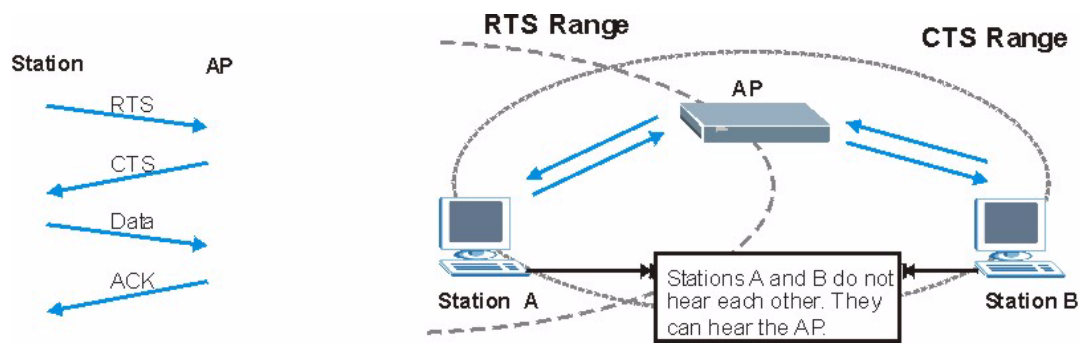
## Channel

A channel is the radio frequency(ies) used by IEEE 802.11a/b/g wireless devices. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a different channel than an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

## RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

**Figure 448** RTS/CTS

When station A sends data to the AP, it might not know that the station B is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

**RTS/CTS** is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

**Note:** Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

## Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the AP will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

## Preamble Type

A preamble is used to synchronize the transmission timing in your wireless network. There are two preamble modes: **Long** and **Short**.

Short preamble takes less time to process and minimizes overhead, so it should be used in a good wireless network environment when all wireless stations support it.

Select **Long** if you have a 'noisy' network or are unsure of what preamble mode your wireless stations support as all IEEE 802.11b compliant wireless adapters must support long preamble. However, not all wireless adapters support short preamble. Use long preamble if you are unsure what preamble mode the wireless adapters support, to ensure interpretability between the AP and the wireless stations and to provide more reliable communication in 'noisy' networks.

Select **Dynamic** to have the AP automatically use short preamble when all wireless stations support it, otherwise the AP uses long preamble.

**Note:** The AP and the wireless stations **MUST** use the same preamble mode in order to communicate.

## IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

**Table 268** IEEE802.11g

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing)

## IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are:

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless stations.

## RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- Authentication  
Determines the identity of the users.
- Authorization  
Determines the network services available to authenticated users once they are connected to the network.
- Accounting  
Keeps track of the client's network activity.

RADIUS is a simple package exchange in which your AP acts as a message relay between the wireless station and the network RADIUS server.

### Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- Access-Request  
Sent by an access point requesting authentication.
- Access-Reject  
Sent by a RADIUS server rejecting access.
- Access-Accept  
Sent by a RADIUS server allowing access.

- Access-Challenge

Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- Accounting-Request

Sent by the access point requesting accounting.

- Accounting-Response

Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

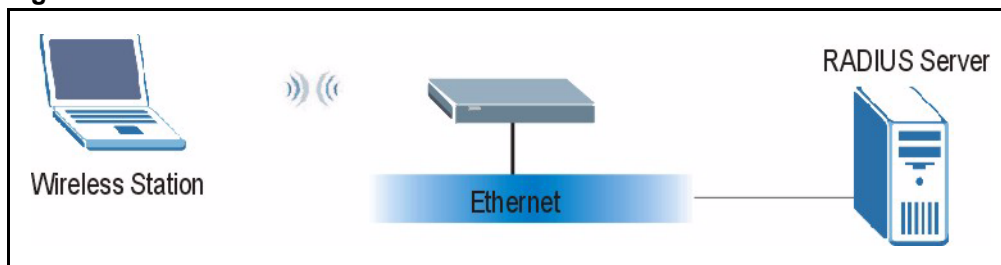
## EAP Authentication

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, the access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server or the AP.

The following figure shows an overview of authentication when you specify a RADIUS server on your access point.

**Figure 449** EAP Authentication



The details below provide a general description of how IEEE 802.1x EAP authentication works. For an example list of EAP-MD5 authentication steps, see the IEEE 802.1x appendix.

- 1 The wireless station sends a “start” message to the device.
- 2 The device sends a “request identity” message to the wireless station for identity information.

- 3 The wireless station replies with identity information, including username and password.
- 4 The RADIUS server checks the user information against its user profile database and determines whether or not to authenticate the wireless station.

## Types of Authentication

This section discusses some popular authentication types: **EAP-MD5**, **EAP-TLS**, **EAP-TTLS**, **PEAP** and **LEAP**.

The type of authentication you use depends on the RADIUS server or the AP. Consult your network administrator for more information.

### EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless station. The wireless station 'proves' that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

### EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless stations for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

### EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

## PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

## LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

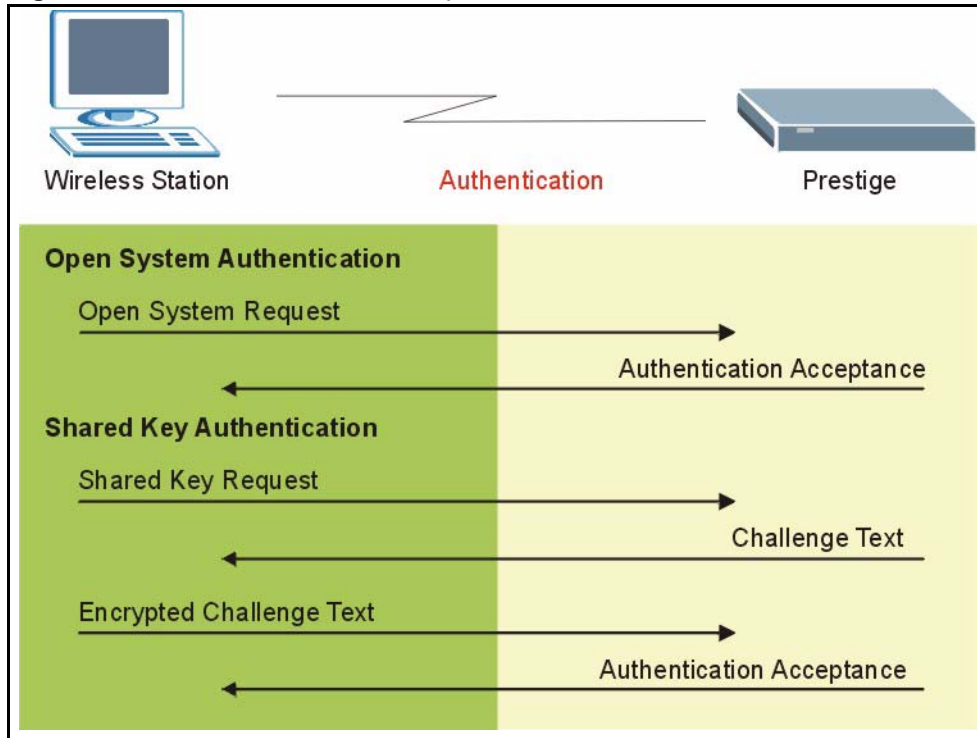
## WEP Encryption

WEP encryption scrambles the data transmitted between the wireless stations and the access points to keep network communications private. It encrypts unicast and multicast communications in a network. Both the wireless stations and the access points must use the same WEP key.

## WEP Authentication Steps

Three different methods can be used to authenticate wireless stations to the network: **Open System**, **Shared Key**, and **Auto**. The following figure illustrates the steps involved.



**Figure 450** WEP Authentication Steps

Open system authentication involves an unencrypted two-message procedure. A wireless station sends an open system authentication request to the AP, which will then automatically accept and connect the wireless station to the network. In effect, open system is not authentication at all as any station can gain access to the network.

Shared key authentication involves a four-message procedure. A wireless station sends a shared key authentication request to the AP, which will then reply with a challenge text message. The wireless station must then use the AP's default WEP key to encrypt the challenge text and return it to the AP, which attempts to decrypt the message using the AP's default WEP key. If the decrypted message matches the challenge text, the wireless station is authenticated.

When your device authentication method is set to open system, it will only accept open system authentication requests. The same is true for shared key authentication. However, when it is set to auto authentication, the device will accept either type of authentication request and the device will fall back to use open authentication if the shared key does not match.

## Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the Wireless screen. You may still configure and store keys here, but they will not be used while Dynamic WEP is enabled.

**Note:** EAP-MD5 cannot be used with Dynamic WEP Key Exchange

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

**Table 269** Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

## WPA

### User Authentication

WPA applies IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless stations using an external RADIUS database.

### Encryption

WPA improves data encryption by using Temporal Key Integrity Protocol (TKIP) or Advanced Encryption Standard (AES), Message Integrity Check (MIC) and IEEE 802.1x.

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. It includes a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

TKIP regularly changes and rotates the encryption keys so that the same encryption key is never used twice.

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless stations. This all happens in the background automatically.

AES (Advanced Encryption Standard) also uses a secret key. This implementation of AES applies a 128-bit key to 128-bit blocks of data.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), TKIP makes it much more difficult to decrypt data on a Wi-Fi network than WEP, making it difficult for an intruder to break into the network.

The encryption mechanisms used for WPA and WPA-PSK are the same. The only difference between the two is that WPA-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs an easier-to-use, consistent, single, alphanumeric password.

## Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each Authentication Method/ key management protocol type. MAC address filters are not dependent on how you configure these security features.

**Table 270** Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	ENABLE IEEE 802.1X
Open	None	No	No
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	WEP	No	Yes
WPA	TKIP	No	Yes
WPA-PSK	WEP	Yes	Yes
WPA-PSK	TKIP	Yes	Yes

## Roaming

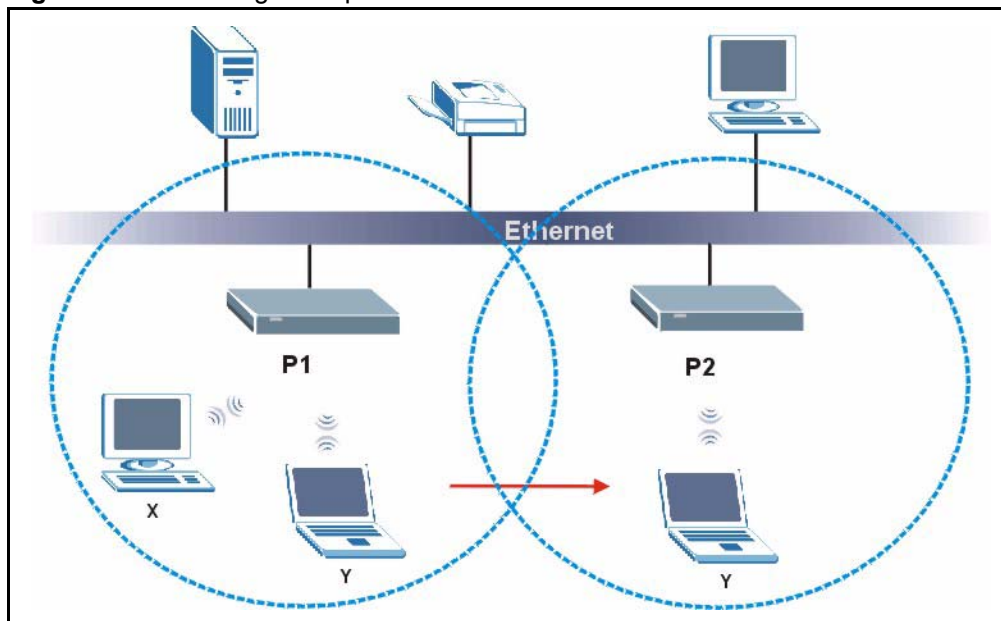
A wireless station is a device with an IEEE 802.11 mode compliant wireless adapter. An access point (AP) acts as a bridge between the wireless and wired networks. An AP creates its own wireless coverage area. A wireless station can associate with a particular access point only if it is within the access point's coverage area.

In a network environment with multiple access points, wireless stations are able to switch from one access point to another as they move between the coverage areas. This is roaming. As the wireless station moves from place to place, it is responsible for choosing the most appropriate access point depending on the signal strength, network utilization or other factors.

The roaming feature on the access points allows the access points to relay information about the wireless stations to each other. When a wireless station moves from a coverage area to another, it scans and uses the channel of a new access point, which then informs the access points on the LAN about the change. The new information is then propagated to the other access points on the LAN. An example is shown in [Figure 451](#).

If the roaming feature is not enabled on the access points, information is not communicated between the access points when a wireless station moves between coverage areas. The wireless station may not be able to communicate with other wireless stations on the network and vice versa.

**Figure 451** Roaming Example



The steps below describe the roaming process.

- 1** As wireless station **Y** moves from the coverage area of access point **P1** to that of access point
- 2** **P2**, it scans and uses the signal of access point **P2**.
- 3** Access point **P2** acknowledges the presence of wireless station **Y** and relays this information to access point **P1** through the wired LAN.
- 4** Access point **P1** updates the new position of wireless station.
- 5** Wireless station **Y** sends a request to access point **P2** for re-authentication.

## Requirements for Roaming

The following requirements must be met in order for wireless stations to roam between the coverage areas.

- 1** All the access points must be on the same subnet and configured with the same ESSID.
- 2** If IEEE 802.1x user authentication is enabled and to be done locally on the access point, the new access point must have the user profile for the wireless station.
- 3** The adjacent access points should use different radio channels when their coverage areas overlap.
- 4** All access points must use the same port number to relay roaming information.
- 5** The access points must be connected to the Ethernet and be able to get IP addresses from a DHCP server if using dynamic IP address assignment.

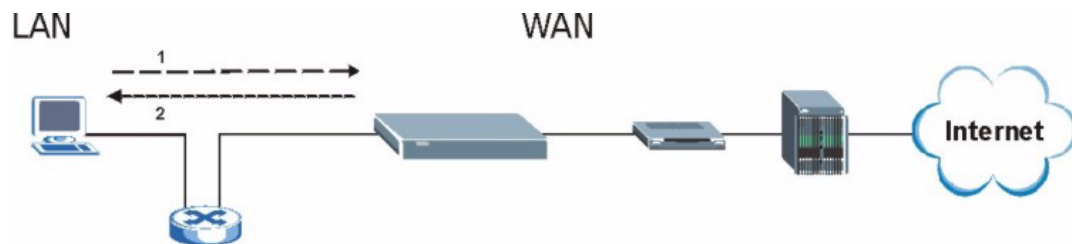
# APPENDIX I

## Triangle Route

### The Ideal Setup

When the firewall is on, your ZyWALL acts as a secure gateway between your LAN and the Internet. In an ideal network topology, all incoming and outgoing network traffic passes through the ZyWALL to protect your LAN against attacks.

**Figure 452** Ideal Setup

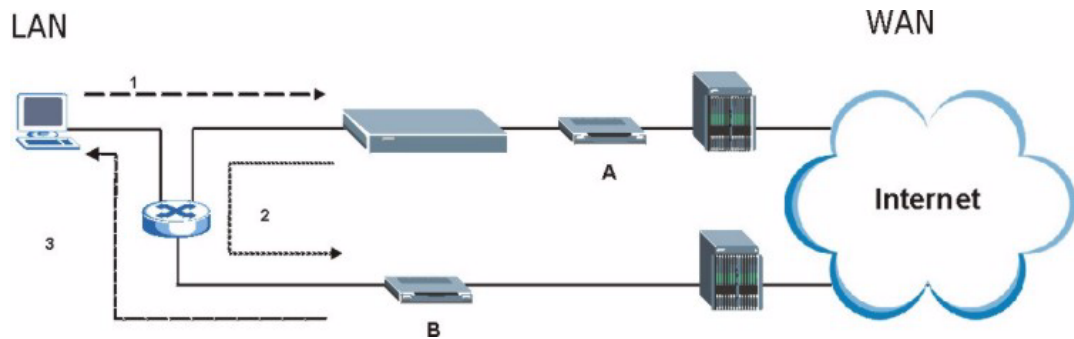


### The “Triangle Route” Problem

A traffic route is a path for sending or receiving data packets between two Ethernet devices. Some companies have more than one alternate route to one or more ISPs. If the LAN and ISP(s) are in the same subnet, the “triangle route” problem may occur. The steps below describe the “triangle route” problem.

- 1 A computer on the LAN initiates a connection by sending out a SYN packet to a receiving server on the WAN.
- 2 The ZyWALL reroutes the SYN packet through Gateway **B** on the LAN to the WAN.
- 3 The reply from the WAN goes directly to the computer on the LAN without going through the ZyWALL.

As a result, the ZyWALL resets the connection, as the connection has not been acknowledged.

**Figure 453** “Triangle Route” Problem

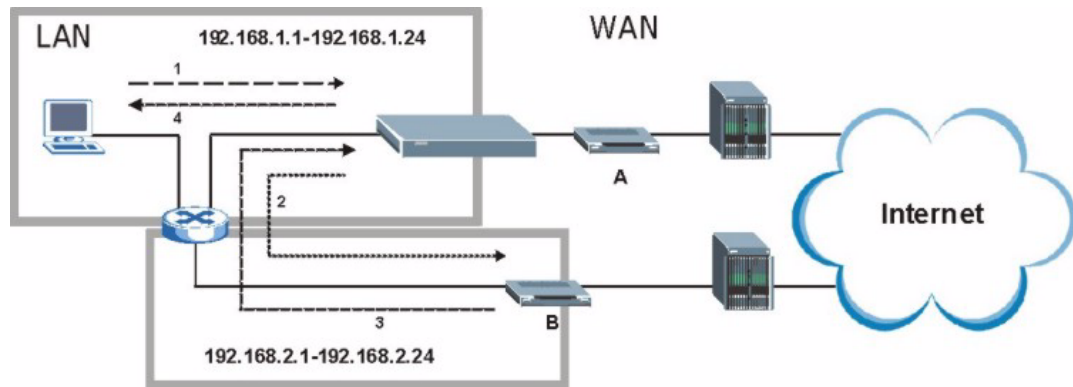
## The “Triangle Route” Solutions

This section presents you two solutions to the “triangle route” problem.

### IP Aliasing

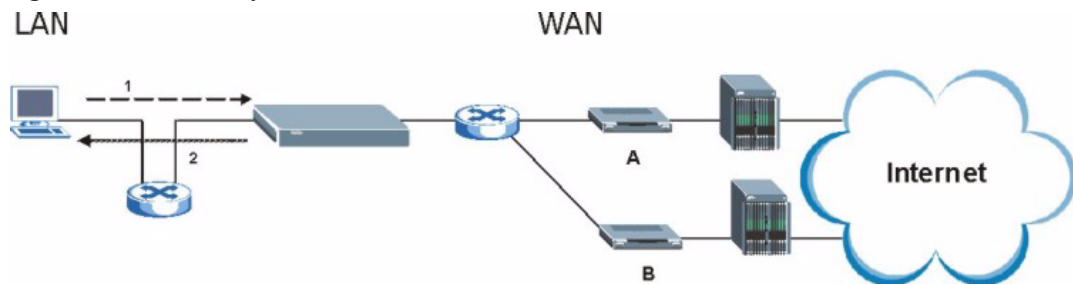
IP alias allows you to partition your network into logical sections over the same Ethernet interface. Your ZyWALL supports up to three logical LAN interfaces with the ZyWALL being the gateway for each logical network. By putting your LAN and Gateway **B** in different subnets, all returning network traffic must pass through the ZyWALL to your LAN. The following steps describe such a scenario.

- 1** A computer on the LAN initiates a connection by sending a SYN packet to a receiving server on the WAN.
- 2** The ZyWALL reroutes the packet to Gateway B, which is in the 192.168.2.1 to 192.168.2.24 subnet.
- 3** The reply from WAN goes through the ZyWALL to the computer on the LAN in the 192.168.1.1 to 192.168.1.24 subnet.

**Figure 454** IP Alias

## Gateways on the WAN Side

A second solution to the “triangle route” problem is to put all of your network gateways on the WAN side as the following figure shows. This ensures that all incoming network traffic passes through your ZyWALL to your LAN. Therefore your LAN is protected.

**Figure 455** Gateways on the WAN Side

## Configuring Triangle Route via Commands

- 1 From the SMT main menu, enter 24.
- 2 Enter “8” in menu 24 to enter CI command mode.
- 3 Use the following command to allow triangle route:

```
sys firewall ignore triangle all on
```

or this command to disallow triangle route:

```
sys firewall ignore triangle all off
```





# APPENDIX J

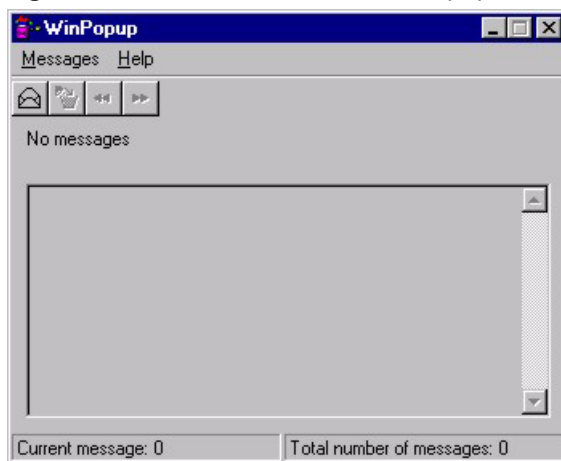
## Windows 98 SE/Me Requirements for Anti-Virus Message Display

With the anti-virus packet scan, when a virus is detected, an alert message is displayed on Microsoft Windows-based computers.

For Windows 98 SE/Me, you must open the **WinPopup** window in order to view real-time alert messages. For Windows 2000 and later versions, a message window automatically displays when an alert is received.

Click **Start, Run** and enter “winpopup” in the field provided and click **OK**. The **WinPopup** window displays as shown.

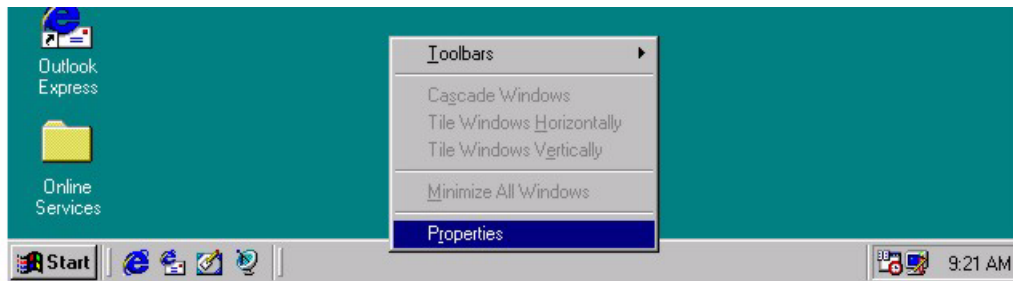
**Figure 456** Windows 98 SE: WinPopup



If you want to display the WinPopup window at startup, follow the steps below for Windows 98 SE (steps are similar for Windows Me).

- 1 Right-click on the program task bar and click **Properties**.

**Figure 457** Windows 98 SE: Program Task Bar



**2** Click the **Start Menu Programs** tab and click **Advanced ...**

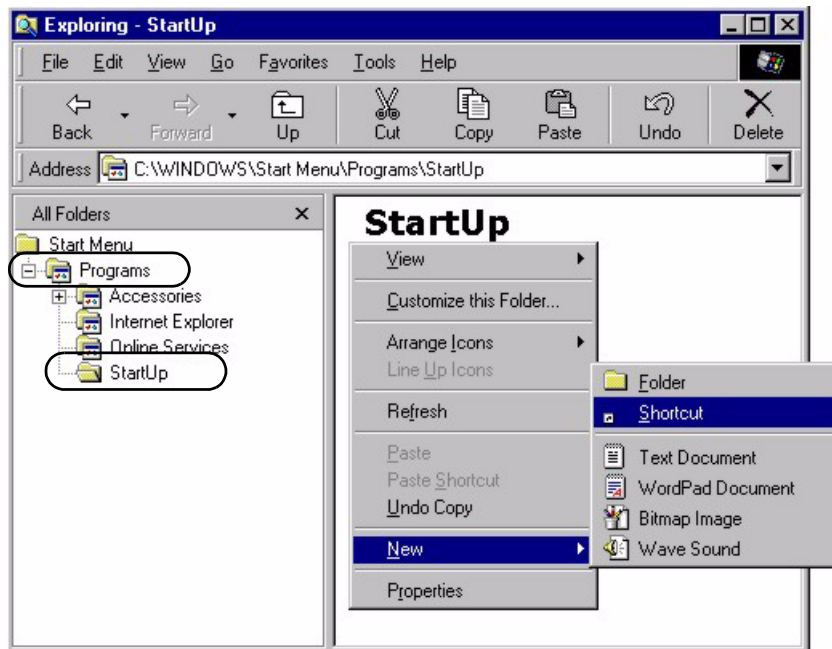
**Figure 458** Windows 98 SE: Task Bar Properties



**3** Double-click **Programs** and click **StartUp**.

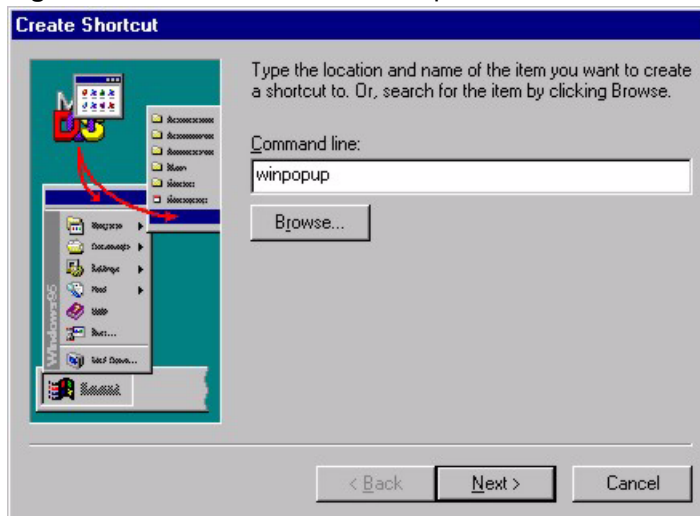
**4** Right-click in the **StartUp** pane and click **New, Shortcut**.

Figure 459 Windows 98 SE: StartUp



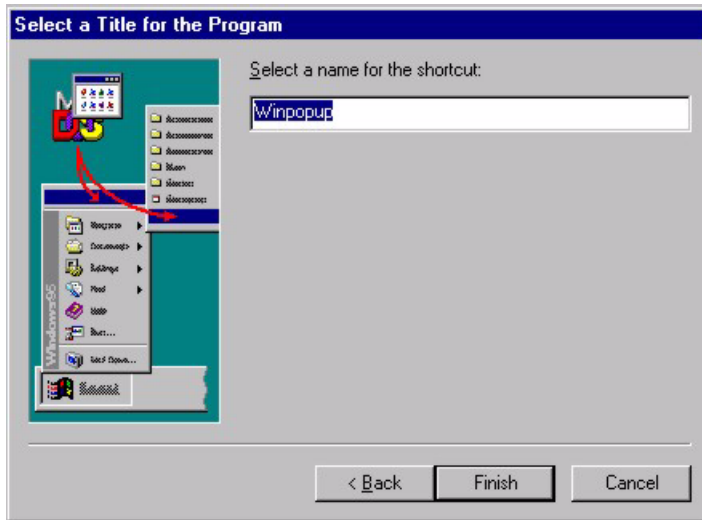
- 5 A Create Shortcut window displays. Enter "winpopup" in the **Command line** field and click **Next**.

Figure 460 Windows 98 SE: Startup: Create Shortcut



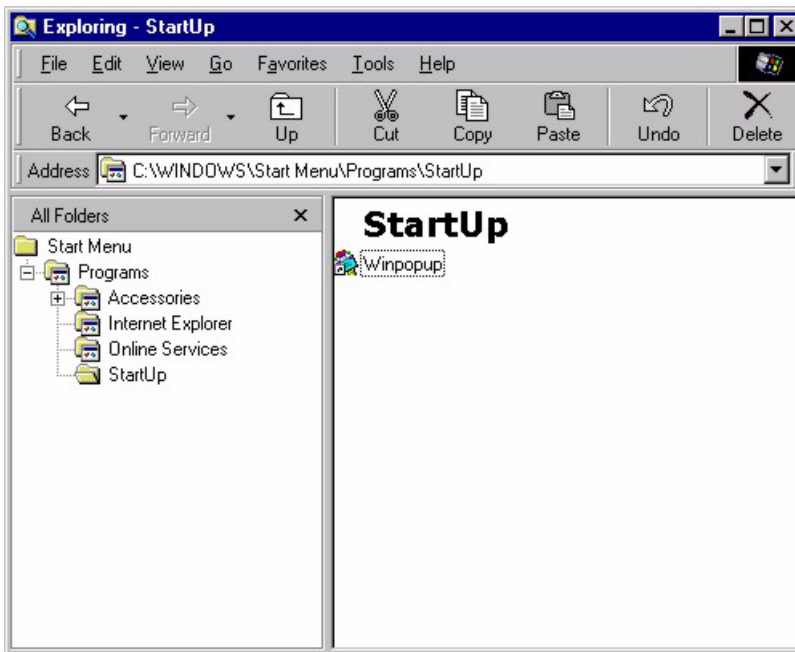
- 6 Specify a name for the shortcut or accept the default and click **Finish**.

**Figure 461** Windows 98 SE: Startup: Select a Title for the Program



7 A shortcut is created in the **StartUp** pane. Restart the computer when prompted.

**Figure 462** Windows 98 SE: Startup: Shortcut



**Note:** The WinPopup window displays after the computer finishes the startup process (see [Figure 456 on page 726](#)).

# APPENDIX K

## VPN Setup

This appendix will help you to quickly create a IPSec/VPN connection between two ZyXEL IPSec routers. It should be considered a quick reference for experienced users.

### General Notes

- The private networks behind the IPSec routers must be on different subnets. For example, 192.168.10.0/24 and 192.168.20.0/24.
- If the sites are/were previously connected using a leased line or ISDN router, physically disconnect these devices from the network before testing your new VPN connection. The old route may have been learnt by RIP and would take priority over the new VPN connection.
- To test whether or not a tunnel is working, ping from a computer at one site to a computer at the other. Before doing so, ensure that both computers have Internet access (via the IPSec routers).
- You can use the “E-MAIL” **Peer Type** and the “SUBNET” **Local and Remote Address Type** to simplify the configuration.
- Do not manually create any static IP routes for the remote VPN site. They are not required.

### Dynamic IPSec Rule

Create a dynamic rule by setting the **Remote Gateway Address** to ‘0.0.0.0’. A single dynamic rule can support multiple simultaneous incoming IPSec connections.

All users of a dynamic rule have the same pre-shared key. You may need to change the pre-shared key if one of the users leaves. See the support notes at <http://www.zyxel.com> for configuration examples for software VPN clients.

### Full Feature NAT Mode

With **Full Feature** NAT mode, you must map the intended VPN rule’s local policy addresses as the Inside Local Address (ILA) to a public IP address assigned by the ISP (an Inside Global Address or IGA) before you can configure the VPN rule. For example, you could create a One-to-One address mapping rule that maps the VPN rule’s local policy addresses as the ILA to the VPN rule’s my IP address as the IGA.

You may have to specify the public IP address in the **My ZyWALL** field of the local IPSec rule. If you have not configured the address mapping properly, a “SPD doesn’t match configuration of NAT” message displays when you try to save the IPSec rule.

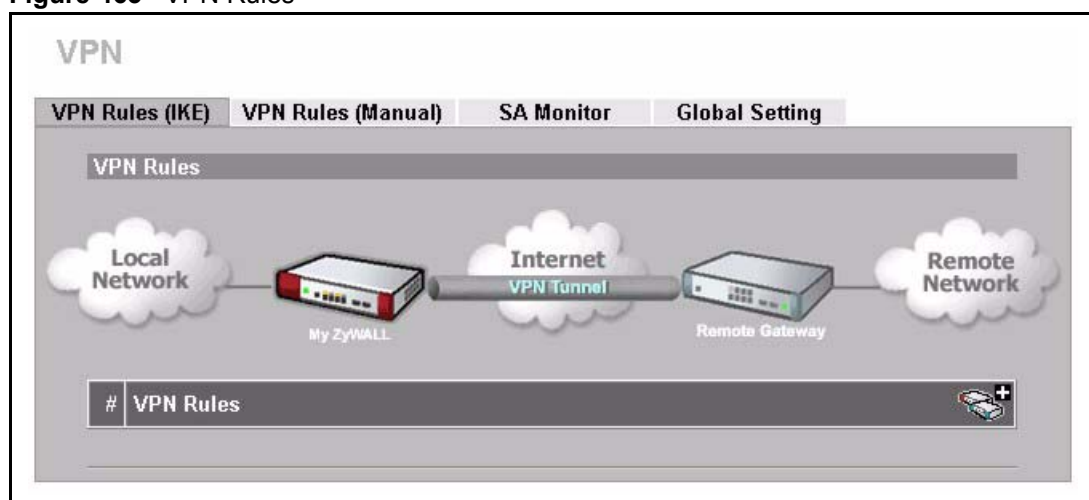
The following pages show a typical configuration that builds a tunnel between two private networks. One network is the headquarters (HQ) and the other is a branch office. Both sites have static (fixed) public addresses. Replace the **Remote Gateway Address** and **Local/Remote Starting IP Address** settings with your own values.

## VPN Configuration

This section gives a VPN rule configuration example using the web configurator.

- 1 Click **VPN** to display the following screen. Click the add gateway policy (🔑) icon to add an IPSec rule (or gateway policy).

**Figure 463** VPN Rules



- 2 Configure the screens in the headquarters and the branch office as follows and click **Apply**.

The pre-shared key must be exactly the same on both IPSec routers. Use a simple key and/or copy and paste the setting into the other IPSec router to avoid typos.

Figure 464 Headquarters Gateway Policy Edit

**VPN - GATEWAY POLICY - EDIT**

**Property**

Name:

NAT Traversal

**Gateway Policy Information**

**My ZyWALL**

My Address:  (Domain Name or IP Address)

My Domain Name:  (See [DDNS](#))

Remote Gateway Address:

**Authentication Key**

Pre-Shared Key:

Certificate:  (See [My Certificates](#))

Local ID Type:

Content:

Peer ID Type:

Content:

**Extended Authentication**

Enable Extended Authentication

Server Mode (Search [Local User](#) first then [RADIUS](#))

Client Mode

User Name:

Password:

**IKE Proposal**

Negotiation Mode:

Encryption Algorithm:

Authentication Algorithm:

SA Life Time (Seconds):

Key Group:

Enable Multiple Proposals

**Associated Network Policies**

#	Name	Local Network	Remote Network
ex-1		192.168.10.0 / 255.255.255.0	192.168.20.0 / 255.255.255.0

Apply Cancel

The IP address of the branch office IPSec router.



**Figure 465** Branch Office Gateway Policy Edit

VPN - GATEWAY POLICY - EDIT

**Property**

Name

NAT Traversal

**Gateway Policy Information**

**My ZyWALL**

My Address  (Domain Name or IP Address)

My Domain Name  (See [DDNS](#))

Remote Gateway Address

**Authentication Key**

Pre-Shared Key

Certificate  (See [My Certificates](#))

Local ID Type

Content

Peer ID Type

Content

**Extended Authentication**

Enable Extended Authentication

Server Mode (Search [Local User](#) first then [RADIUS](#))

Client Mode

User Name

Password

**IKE Proposal**

Negotiation Mode

Encryption Algorithm

Authentication Algorithm

SA Life Time (Seconds)


Key Group

Enable Multiple Proposals

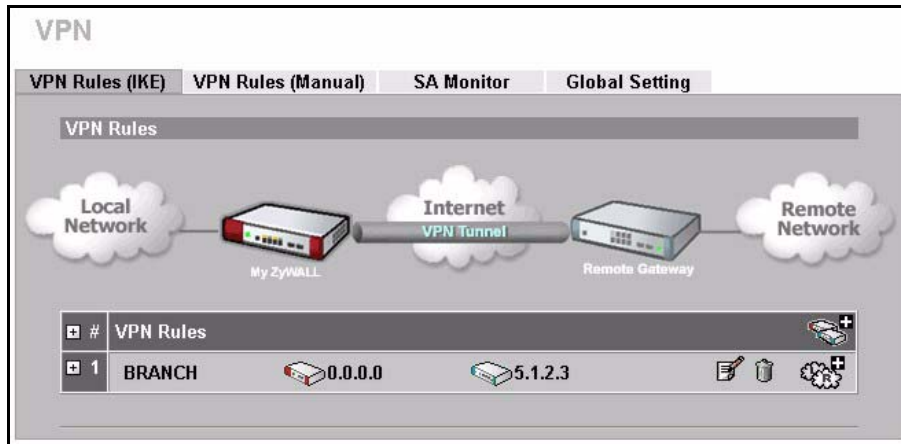
**Associated Network Policies**

#	Name	Local Network	Remote Network

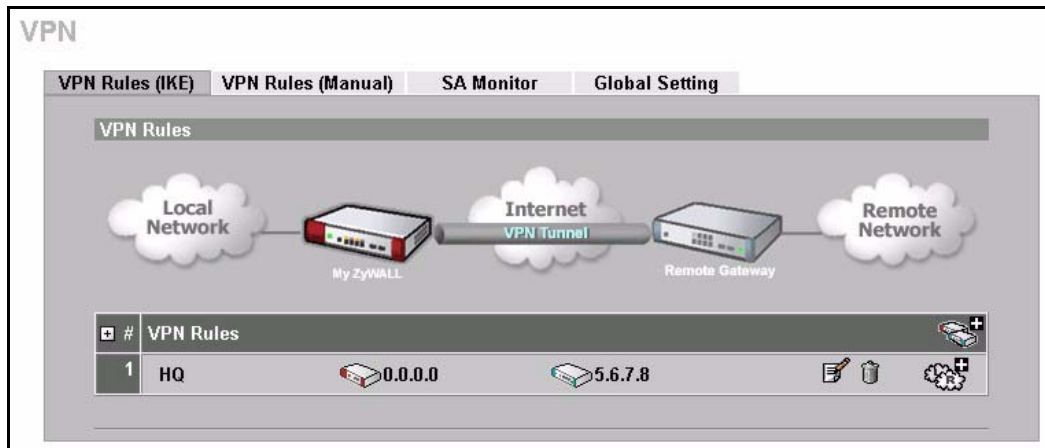
The IP address of the headquarters IPsec router.

3 Click the add network policy (  ) icon next to the **BRANCH** gateway policy to configure a VPN policy.

**Figure 466** Headquarters VPN Rule



**Figure 467** Branch Office VPN Rule



**4** Configure the screens in the headquarters and the branch office as follows and click **Apply**.

Figure 468 Headquarters Network Policy Edit

**VPN - NETWORK POLICY - EDIT**

**Property**

- Active
- Name: ex-1
- Protocol: 0
- Nailed-Up
- Allow NetBIOS Traffic Through IPSec Tunnel
- Check IPSec Tunnel Connectivity  Log
- Ping this Address: 0 . 0 . 0 . 0

**Gateway Policy Information**

Gateway Policy: BRANCH

**Local Network**

- Address Type: Subnet Address
- Starting IP Address: 192 . 168 . 10 . 0
- Ending IP Address / Subnet Mask: 255 . 255 . 255 . 0
- Local Port: Start 0 End 0

**Remote Network**

- Address Type: Subnet Address
- Starting IP Address: 192 . 168 . 20 . 0
- Ending IP Address / Subnet Mask: 255 . 255 . 255 . 0
- Remote Port: Start 0 End 0

**IPSec Proposal**

- Encapsulation Mode: Tunnel
- Active Protocol: ESP
- Encryption Algorithm: AES
- Authentication Algorithm: SHA1
- SA Life Time (Seconds): 28800
- Prefect Forward Secrecy (PFS): NONE
- Enable Replay Detection
- Enable Multiple Proposals

Apply Cancel

Figure 469 Branch Office Network Policy Edit

**VPN - NETWORK POLICY - EDIT**

**Property**

Active Activate the network policy.

Name: ex-1

Protocol: 0

Nailed-Up

Allow NetBIOS Traffic Through IPSec Tunnel

Check IPSec Tunnel Connectivity  Log

Ping this Address: 0 . 0 . 0 . 0

**Gateway Policy Information**

Gateway Policy: HQ

**Local Network**

Address Type: Subnet Address

Starting IP Address: 192 . 168 . 20 . 0

Ending IP Address / Subnet Mask: 255 . 255 . 255 . 0

Local Port: Start 0 End 0

**Remote Network**

Address Type: Subnet Address

Starting IP Address: 192 . 168 . 10 . 0

Ending IP Address / Subnet Mask: 255 . 255 . 255 . 0

Remote Port: Start 0 End 0

**IPSec Proposal**

Encapsulation Mode: Tunnel

Active Protocol: ESP

Encryption Algorithm: DES

Authentication Algorithm: SHA1

SA Life Time (Seconds): 28800

Perfect Forward Secrecy (PFS): NONE

Enable Replay Detection

Enable Multiple Proposals

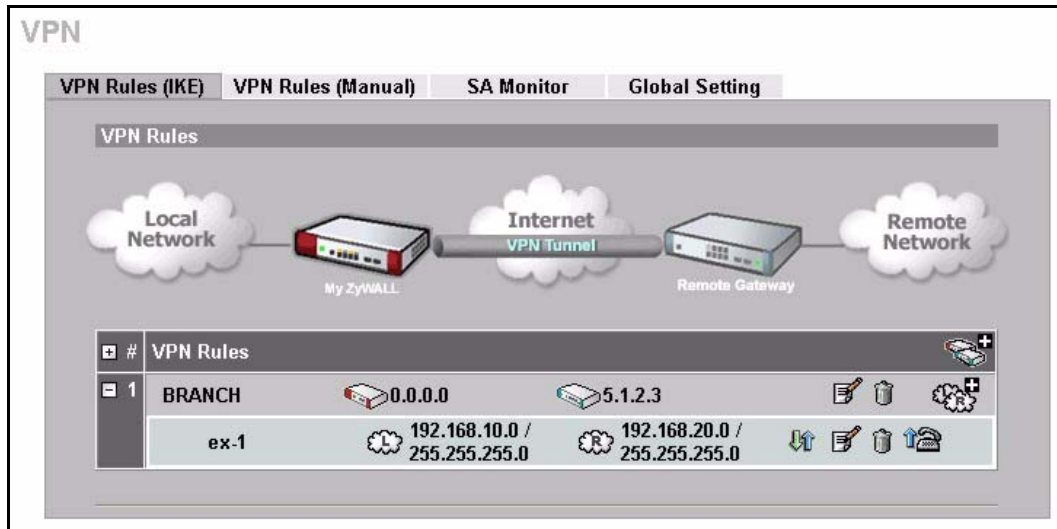
Apply Cancel

IP addresses on different subnets.

## Dialing the VPN Tunnel via Web Configurator

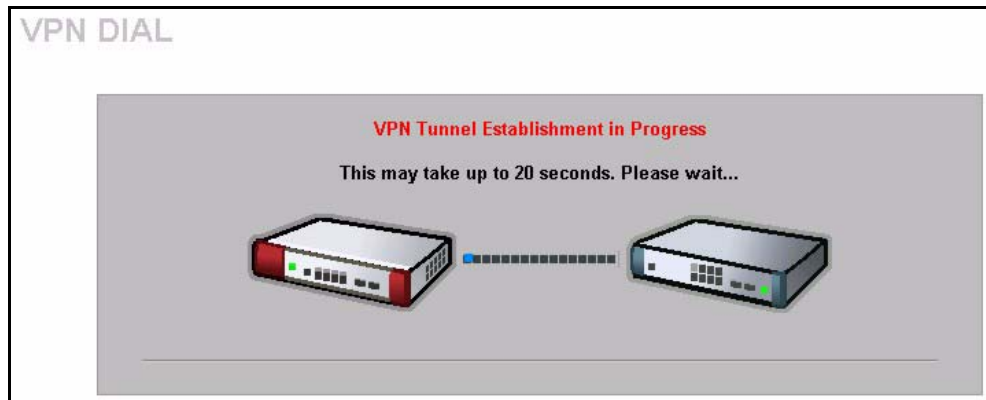
To test whether the IPSec routers can build the VPN tunnel, click the dial (📞) icon in the **VPN Rules (IKE)** screen to have the IPSec routers set up the tunnel.

**Figure 470** VPN Rule Configured



The following screen displays.

**Figure 471** VPN Dial



This screen displays later if the IPSec routers can build the VPN tunnel.

**Figure 472** VPN Tunnel Established



## VPN Troubleshooting

If the IPSec tunnel does not build properly, the problem is likely a configuration error at one of the IPSec routers. Log into the web configurators of both ZyXEL IPSec routers. Check the settings in each field methodically and slowly.

### VPN Log

The system log can often help to identify a configuration problem. Use the web configurator **LOGS Log Settings** screen to enable IKE and IPSec logging at both ends, clear the log and then build the tunnel.

View the log via the web configurator **LOGS View Log** screen or type `sys log disp` from **SMT Menu 24.8**. See [Appendix S on page 774](#) for information on the log messages.

**Figure 473** VPN Log Example

```

ras> sys log disp ike ipsec

# .time          source          destination      notes
  message
0|01/11/2001 18:47:22 |5.6.7.8          |5.1.2.3         |IKE
  Rule [ex-1] Tunnel built successfully
1|01/11/2001 18:47:22 |5.6.7.8          |5.1.2.3         |IKE
  The cookie pair is : 0xDAC0B43FBDE154F5 / 0xC5156C099C3F7DCA
2|01/11/2001 18:47:22 |5.6.7.8          |5.1.2.3         |IKE
  Send:[HASH]
3|01/11/2001 18:47:22 |5.6.7.8          |5.1.2.3         |IKE
  The cookie pair is : 0xDAC0B43FBDE154F5 / 0xC5156C099C3F7DCA
4|01/11/2001 18:47:22 |5.6.7.8          |5.1.2.3         |IKE
  Adjust TCP MSS to 1398
5|01/11/2001 18:47:22 |5.1.2.3          |5.6.7.8         |IKE
  Recv:[HASH][SA][NONCE][ID][ID]
6|01/11/2001 18:47:22 |5.1.2.3          |5.6.7.8         |IKE
  The cookie pair is : 0xDAC0B43FBDE154F5 / 0xC5156C099C3F7DCA
7|01/11/2001 18:47:21 |5.6.7.8          |5.1.2.3         |IKE
  IKE Packet Retransmit
8|01/11/2001 18:47:21 |5.6.7.8          |5.1.2.3         |IKE
  The cookie pair is : 0xDAC0B43FBDE154F5 / 0xC5156C099C3F7DCA
9|01/11/2001 18:47:17 |5.6.7.8          |5.1.2.3         |IKE
  Send:[HASH][SA][NONCE][ID][ID]
10|01/11/2001 18:47:17 |5.6.7.8          |5.1.2.3         |IKE
  The cookie pair is : 0xDAC0B43FBDE154F5 / 0xC5156C099C3F7DCA
11|01/11/2001 18:47:17 |5.6.7.8          |5.1.2.3         |IKE
  Start Phase 2: Quick Mode
12|01/11/2001 18:47:17 |5.6.7.8          |5.1.2.3         |IKE
  The cookie pair is : 0xDAC0B43FBDE154F5 / 0xC5156C099C3F7DCA
13|01/11/2001 18:47:17 |5.6.7.8          |5.1.2.3         |IKE
  Phase 1 IKE SA process done
14|01/11/2001 18:47:17 |5.6.7.8          |5.1.2.3         |IKE
  The cookie pair is : 0xDAC0B43FBDE154F5 / 0xC5156C099C3F7DCA
15|01/11/2001 18:47:17 |5.1.2.3          |5.6.7.8         |IKE
  Recv:[ID][HASH][NOTIFY:INIT_CONTACT]9C3F7DCA
16|01/11/2001 18:47:17 |5.1.2.3          |5.6.7.8         |IKE
  The cookie pair is : 0xDAC0B43FBDE154F5 / 0xC5156C099C3F7DCA
17|01/11/2001 18:47:15 |5.6.7.8          |5.1.2.3         |IKE
  Send:[ID][HASH][NOTIFY:INIT_CONTACT]9C3F7DCA
18|01/11/2001 18:47:15 |5.6.7.8          |5.1.2.3         |IKE
  The cookie pair is : 0xDAC0B43FBDE154F5 / 0xC5156C099C3F7DCA
19|01/11/2001 18:47:15 |5.1.2.3          |5.6.7.8         |IKE
  Recv:[KE][NONCE]
20|01/11/2001 18:47:15 |5.1.2.3          |5.6.7.8         |IKE
  The cookie pair is : 0xDAC0B43FBDE154F5 / 0xC5156C099C3F7DCA
21|01/11/2001 18:47:13 |5.6.7.8          |5.1.2.3         |IKE
  Send:[KE][NONCE]
22|01/11/2001 18:47:13 |5.6.7.8          |5.1.2.3         |IKE
  The cookie pair is : 0xDAC0B43FBDE154F5 / 0xC5156C099C3F7DCA
23|01/11/2001 18:47:13 |5.1.2.3          |5.6.7.8         |IKE
  Recv:[SA][VID][VID]

```

## IPSec Debug

If you are having difficulty building an IPSec tunnel to a non-ZyXEL IPSec router, advanced users may wish to examine the IPSec debug feature (**Menu 24.8**).

**Note:** If any of your VPN rules have an active network policy set to nailed-up, using the IPSec debug feature may cause the ZyWALL to continuously display new information. Type `ipsec debug level 0` and press [ENTER] to stop it.

**Figure 474** IKE/IPSec Debug Example

```

ras> ipsec debug
type          level          display
ras> ipsec debug type
<0:Disable | 1:Original on|off | 2:IKE on|off | 3: IPsec [SPI]|on|off |
4:XAUTH on|off | 5:CERT on|off | 6: All>
ras> ipsec debug level
<0:None | 1:User | 2:Low | 3:High>

ras> ipsec debug type 1 on
ras> ipsec debug type 2 on
ras> ipsec debug level 3

ras> ipsec dial 1
get_ipsec_sa_by_policyIndex():
Start dialing for tunnel <rule# 1>...
ikeStartNegotiate(): saIndex<0>
peerIp<5.1.2.3> protocol: <IPSEC_ESP>(3)

peer Ip <5.1.2.3> initiator(): type<IPSEC_ESP>, exch<Main>

initiator :
protocol: IPSEC_ESP, exchange mode: Main mode find_ipsec_sa():
find ipsec saNot found

Not found isadb_is_outstanding_req():
isakmp is outstanding req : SA not found
isadb_create_entry(): >> INITIATOR

isadb_get_entry_by_addr():
Get IKE entry by address: SA not found

SA not found ISAKMP SA created for peer <BRANCH> size<900>

ISAKMP SA created for peer <BRANCH> size<900> ISAKMP SA built,
ikePeer.s0

ISAKMP SA built, index = 0isadb_create_entry(): done

create IKE entry doneinitiator(): find myIpAddr = 0.0.0.0, use
<5.6.7.8> r

```



## Use a VPN Tunnel

A VPN tunnel gives you a secure connection to another computer or network. The **VPN Status** screen displays whether or not your VPN tunnel is connected. Example VPN tunnel uses are securely sending and retrieving files, and accessing corporate network drives, web servers and email. Services work as if you were at the office instead of connected through the Internet.

## FTP Example

The following example shows a text-based login from a branch office computer to an FTP server behind the remote IPSec router at headquarters. The server's IP address (192.168.10.33) is in the subnet configured in the **Local Policy** fields in [Figure 464 on page 732](#).

```
C:\Documents and Settings\Administrator>ftp 192.168.10.33
Connected to 192.168.109.33.
220 Serv-U FTP-Server v2.5b for WinSock ready...
User (192.168.109.33:(none)): test
331 User name okay, need password.
Password:
230 User logged in, proceed.
```

# APPENDIX L

## Importing Certificates

This appendix shows importing certificates examples using Internet Explorer 5.

### Import ZyWALL Certificates into Netscape Navigator

In Netscape Navigator, you can permanently trust the ZyWALL's server certificate by importing it into your operating system as a trusted certification authority.

Select **Accept This Certificate Permanently** in the following screen to do this.

**Figure 475** Security Certificate



### Importing the ZyWALL's Certificate into Internet Explorer

For Internet Explorer to trust a self-signed certificate from the ZyWALL, simply import the self-signed certificate into your operating system as a trusted certification authority.

To have Internet Explorer trust a ZyWALL certificate issued by a certificate authority, import the certificate authority's certificate into your operating system as a trusted certification authority.

The following example procedure shows how to import the ZyWALL's (self-signed) server certificate into your operating system as a trusted certification authority.

- 1 In Internet Explorer, double click the lock shown in the following screen.

**Figure 476** Login Screen



**2** Click **Install Certificate** to open the **Install Certificate** wizard.

**Figure 477** Certificate General Information before Import



**3** Click **Next** to begin the **Install Certificate** wizard.

**Figure 478** Certificate Import Wizard 1

- 4 Select where you would like to store the certificate and then click **Next**.

**Figure 479** Certificate Import Wizard 2

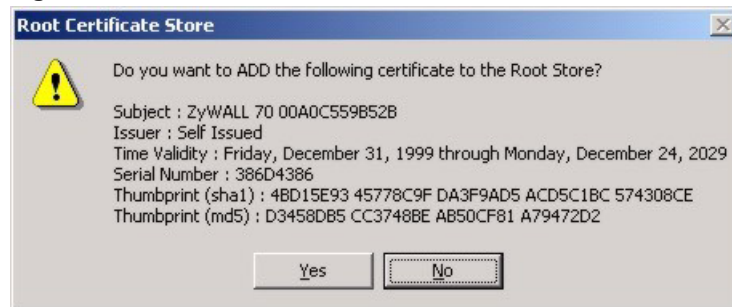
- 5 Click **Finish** to complete the **Import Certificate** wizard.

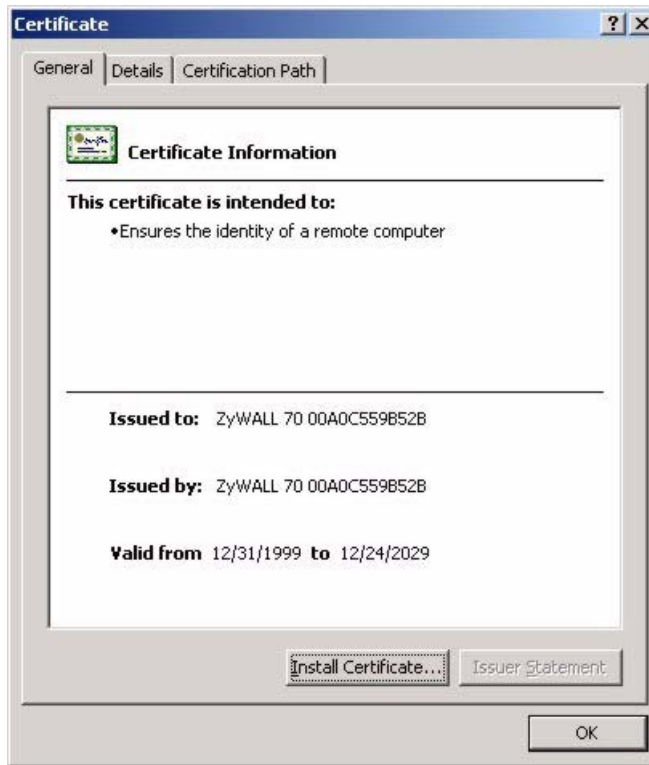
**Figure 480** Certificate Import Wizard 3



**6** Click **Yes** to add the ZyWALL certificate to the root store.

**Figure 481** Root Certificate Store



**Figure 482** Certificate General Information after Import

## Enrolling and Importing SSL Client Certificates

The SSL client needs a certificate if **Authenticate Client Certificates** is selected on the ZyWALL.

You must have imported at least one trusted CA to the ZyWALL in order for the **Authenticate Client Certificates** to be active (see the Certificates chapter for details).


Apply for a certificate from a Certification Authority (CA) that is trusted by the ZyWALL (see the ZyWALL's **Trusted CA** web configurator screen).

Figure 483 ZyWALL Trusted CA Screen





**CERTIFICATES**

My Certificates    Trusted CAs    Trusted Remote Hosts    Directory Servers

PKI Storage Space in Use

0%  100%

Trusted CA Setting

#	Name	Subject	Issuer	Valid From	Valid To	CRL Issuer	Modify
1	CHT-SubCA	OU=SSL CA for Test, O=Chunghwa Telecom Co., Ltd., C=TW	OU=eCA for Test, O=Chunghwa Telecom Co., Ltd., C=TW	2001 Nov 26th, 10:26:35 GMT	2021 Nov 26th, 10:26:35 GMT	No	 
2	SSH-CA	CN=SSH Test CA 1 No Liabilities, O=SSH Communications Security Corp, C=FI	CN=SSH Test CA 1 No Liabilities, O=SSH Communications Security Corp, C=FI	2001 Aug 1st, 07:08:32 GMT	2004 Aug 1st, 07:08:32 GMT	No	 

Import    Refresh

The CA sends you a package containing the CA's trusted certificate(s), your personal certificate(s) and a password to install the personal certificate(s).

## Installing the CA's Certificate

- 1 Double click the CA's trusted certificate to produce a screen similar to the one shown next.

**Figure 484** CA Certificate Example

**2** Click **Install Certificate** and follow the wizard as shown earlier in this appendix.

## Installing Your Personal Certificate(s)

You need a password in advance. The CA may issue the password or you may have to specify it during the enrollment. Double-click the personal certificate given to you by the CA to produce a screen similar to the one shown next

**1** Click **Next** to begin the wizard.



**Figure 485** Personal Certificate Import Wizard 1

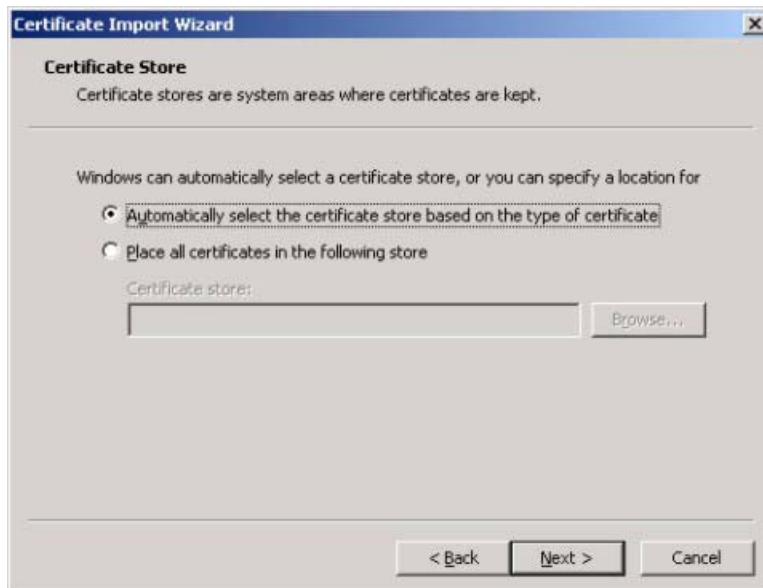
- 2 The file name and path of the certificate you double-clicked should automatically appear in the **File name** text box. Click **Browse** if you wish to import a different certificate.

**Figure 486** Personal Certificate Import Wizard 2

- 3 Enter the password given to you by the CA.

**Figure 487** Personal Certificate Import Wizard 3

- 4 Have the wizard determine where the certificate should be saved on your computer or select **Place all certificates in the following store** and choose a different location.

**Figure 488** Personal Certificate Import Wizard 4

- 5 Click **Finish** to complete the wizard and begin the import process.

**Figure 489** Personal Certificate Import Wizard 5

- 6 You should see the following screen when the certificate is correctly installed on your computer.

**Figure 490** Personal Certificate Import Wizard 6

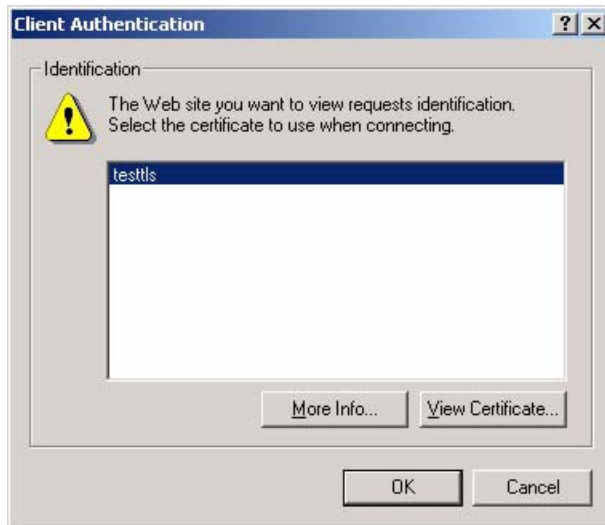
## Using a Certificate When Accessing the ZyWALL Example

Use the following procedure to access the ZyWALL via HTTPS.

- 1 Enter 'https://ZyWALL IP Address/' in your browser's web address field.

**Figure 491** Access the ZyWALL Via HTTPS

- 2 When **Authenticate Client Certificates** is selected on the ZyWALL, the following screen asks you to select a personal certificate to send to the ZyWALL. This screen displays even if you only have a single certificate as in the example.

**Figure 492** SSL Client Authentication

3 You next see the ZyWALL login screen.

**Figure 493** ZyWALL Secure Login Screen



# APPENDIX M

## Command Interpreter

The following describes how to use the command interpreter. Enter 24 in the main menu to bring up the system maintenance menu. Enter 8 to go to **Menu 24.8 - Command Interpreter Mode**. See the included disk or [zyxel.com](http://zyxel.com) for more detailed information on these commands.

**Note:** Use of undocumented commands or misconfiguration can damage the unit and possibly render it unusable.

### Command Syntax

- The command keywords are in `courier new` font.
- Enter the command keywords exactly as shown, do not abbreviate.
- The required fields in a command are enclosed in angle brackets `<>`.
- The optional fields in a command are enclosed in square brackets `[]`.
- The `|` symbol means or.

For example,

```
sys filter netbios config <type> <on|off>
```

means that you must specify the type of netbios filter and whether to turn it on or off.

### Command Usage

A list of valid commands can be found by typing `help` or `?` at the command prompt. Always type the full command. Type `exit` to return to the SMT main menu when finished.



# APPENDIX N

## Firewall Commands

The following describes the firewall commands. See [Appendix M on page 754](#) for information on the command structure.

**Table 271** Firewall Commands

FUNCTION	COMMAND	DESCRIPTION
Firewall Set-Up		
	<code>config edit firewall active &lt;yes   no&gt;</code>	This command turns the firewall on or off.
	<code>config retrieve firewall</code>	This command returns the previously saved firewall settings.
	<code>config save firewall</code>	This command saves the current firewall settings.
Display		
	<code>config display firewall</code>	This command shows the of all the firewall settings including e-mail, attack, and the sets/rules.
	<code>config display firewall set &lt;set #&gt;</code>	This command shows the current configuration of a set; including timeout values, name, default-permit, and etc.If you don't put use a number (#) after "set", information about all of the sets/rules appears.
	<code>config display firewall set &lt;set #&gt; rule &lt;rule #&gt;</code>	This command shows the current entries of a rule in a firewall rule set.
	<code>config display firewall attack</code>	This command shows all of the attack response settings.
	<code>config display firewall e-mail</code>	This command shows all of the e-mail settings.
	<code>config display firewall ?</code>	This command shows all of the available firewall sub commands.
Edit		



**Table 271** Firewall Commands (continued)

FUNCTION	COMMAND	DESCRIPTION
E-mail	<code>config edit firewall e-mail mail-server &lt;ip address of mail server&gt;</code>	This command sets the IP address to which the e-mail messages are sent.
	<code>config edit firewall e-mail return-addr &lt;e-mail address&gt;</code>	This command sets the source e-mail address of the firewall e-mails.
	<code>config edit firewall e-mail email-to &lt;e-mail address&gt;</code>	This command sets the e-mail address to which the firewall e-mails are sent.
	<code>config edit firewall e-mail policy &lt;full   hourly   daily   weekly&gt;</code>	This command sets how frequently the firewall log is sent via e-mail.
	<code>config edit firewall e-mail day &lt;sunday   monday   tuesday   wednesday   thursday   friday   saturday&gt;</code>	This command sets the day on which the current firewall log is sent through e-mail if the ZyWALL is set to send it on a weekly basis.
	<code>config edit firewall e-mail hour &lt;0-23&gt;</code>	This command sets the hour when the firewall log is sent through e-mail if the ZyWALL is set to send it on an hourly, daily or weekly basis.
	<code>config edit firewall e-mail minute &lt;0-59&gt;</code>	This command sets the minute of the hour for the firewall log to be sent via e-mail if the ZyWALL is set to send it on a hourly, daily or weekly basis.
Attack	<code>config edit firewall attack send-alert &lt;yes   no&gt;</code>	This command enables or disables the immediate sending of DOS attack notification e-mail messages.
	<code>config edit firewall attack block &lt;yes   no&gt;</code>	Set this command to yes to block new traffic after the tcp-max-incomplete threshold is exceeded. Set it to no to delete the oldest half-open session when traffic exceeds the tcp-max-incomplete threshold.
	<code>config edit firewall attack block-minute &lt;0-255&gt;</code>	This command sets the number of minutes for new sessions to be blocked when the tcp-max-incomplete threshold is reached. This command is only valid when block is set to yes.

**Table 271** Firewall Commands (continued)

FUNCTION	COMMAND	DESCRIPTION
	<code>config edit firewall attack minute-high &lt;0-255&gt;</code>	This command sets the threshold rate of new half-open sessions per minute where the ZyWALL starts deleting old half-opened sessions until it gets them down to the minute-low threshold.
	<code>config edit firewall attack minute-low &lt;0-255&gt;</code>	This command sets the threshold of half-open sessions where the ZyWALL stops deleting half-opened sessions.
	<code>config edit firewall attack max-incomplete-high &lt;0-255&gt;</code>	This command sets the threshold of half-open sessions where the ZyWALL starts deleting old half-opened sessions until it gets them down to the max incomplete low.
	<code>config edit firewall attack max-incomplete-low &lt;0-255&gt;</code>	This command sets the threshold where the ZyWALL stops deleting half-opened sessions.
	<code>config edit firewall attack tcp-max-incomplete &lt;0-255&gt;</code>	This command sets the threshold of half-open TCP sessions with the same destination where the ZyWALL starts dropping half-open sessions to that destination.
Sets	<code>config edit firewall set &lt;set #&gt; name &lt;desired name&gt;</code>	This command sets a name to identify a specified set.
	<code>Config edit firewall set &lt;set #&gt; default-permit &lt;forward   block&gt;</code>	This command sets 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>	This command sets the time period to allow an ICMP session to wait for the ICMP response.
	<code>Config edit firewall set &lt;set #&gt; udp-idle-timeout &lt;seconds&gt;</code>	This command sets how long a UDP connection is allowed to remain inactive before the ZyWALL considers the connection closed.
	<code>Config edit firewall set &lt;set #&gt; connection-timeout &lt;seconds&gt;</code>	This command sets how long ZyWALL waits for a TCP session to be established before dropping the session.
	<code>Config edit firewall set &lt;set #&gt; fin-wait-timeout &lt;seconds&gt;</code>	This command sets how long the ZyWALL leaves a TCP session open after the firewall detects a FIN-exchange (indicating the end of the TCP session).

**Table 271** Firewall Commands (continued)

FUNCTION	COMMAND	DESCRIPTION
	Config edit firewall set <set #> tcp-idle-timeout <seconds>	This command sets how long ZyWALL lets an inactive TCP connection remain open before considering it closed.
	Config edit firewall set <set #> log <yes   no>	This command sets whether or not the ZyWALL creates logs for packets that match the firewall's default rule set.
Rules	Config edit firewall set <set #> rule <rule #> permit <forward   block>	This command sets whether packets that match this rule are dropped or allowed through.
	Config edit firewall set <set #> rule <rule #> active <yes   no>	This command sets whether a rule is enabled or not.
	Config edit firewall set <set #> rule <rule #> protocol <integer protocol value >	This command sets the protocol specification number made in this rule for ICMP.
	Config edit firewall set <set #> rule <rule #> log <none   match   not-match   both>	This command sets the ZyWALL to log traffic that matches the rule, doesn't match, both or neither.
	Config edit firewall set <set #> rule <rule #> alert <yes   no>	This command sets whether or not the ZyWALL sends an alert e-mail when a DOS attack or a violation of a particular rule occurs.
	config edit firewall set <set #> rule <rule #> srcaddr-single <ip address>	This command sets the rule to have the ZyWALL check for traffic with this individual source address.
	config edit firewall set <set #> rule <rule #> srcaddr-subnet <ip address> <subnet mask>	This command sets a rule to have the ZyWALL check for traffic from a particular subnet (defined by IP address and subnet mask).
	config edit firewall set <set #> rule <rule #> srcaddr-range <start ip address> <end ip address>	This command sets a rule to have the ZyWALL check for traffic from this range of addresses.
	config edit firewall set <set #> rule <rule #> destaddr-single <ip address>	This command sets the rule to have the ZyWALL check for traffic with this individual destination address.

**Table 271** Firewall Commands (continued)

FUNCTION	COMMAND	DESCRIPTION
	<code>config edit firewall set &lt;set #&gt; rule &lt;rule #&gt; destaddr-subnet &lt;ip address&gt; &lt;subnet mask&gt;</code>	This command sets a rule to have the ZyWALL check for traffic with a particular subnet destination (defined by IP address and subnet mask).
	<code>config edit firewall set &lt;set #&gt; rule &lt;rule #&gt; destaddr-range &lt;start ip address&gt; &lt;end ip address&gt;</code>	This command sets a rule to have the ZyWALL check for traffic going to this range of addresses.
	<code>config edit firewall set &lt;set #&gt; rule &lt;rule #&gt; TCP destport-single &lt;port #&gt;</code>	This command sets a rule to have the ZyWALL check for TCP traffic with this destination address. You may repeat this command to enter various, non-consecutive port numbers.
	<code>config edit firewall set &lt;set #&gt; rule &lt;rule #&gt; TCP destport-range &lt;start port #&gt; &lt;end port #&gt;</code>	This command sets a rule to have the ZyWALL check for TCP traffic with a destination port in this range.
	<code>config edit firewall set &lt;set #&gt; rule &lt;rule #&gt; UDP destport-single &lt;port #&gt;</code>	This command sets a rule to have the ZyWALL check for UDP traffic with this destination address. You may repeat this command to enter various, non-consecutive port numbers.
	<code>config edit firewall set &lt;set #&gt; rule &lt;rule #&gt; UDP destport-range &lt;start port #&gt; &lt;end port #&gt;</code>	This command sets a rule to have the ZyWALL check for UDP traffic with a destination port in this range.
Delete		
	<code>config delete firewall e-mail</code>	This command removes all of the settings for e-mail alert.
	<code>config delete firewall attack</code>	This command resets all of the attack response settings to their defaults.
	<code>config delete firewall set &lt;set #&gt;</code>	This command removes the specified set from the firewall configuration.
	<code>config delete firewall set &lt;set #&gt; rule&lt;rule #&gt;</code>	This command removes the specified rule in a firewall configuration set.



# APPENDIX O

## NetBIOS Filter Commands

The following describes the NetBIOS packet filter commands. See [Appendix M on page 754](#) for information on the command structure.

### Introduction

NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to connect to and communicate with a LAN.

For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls.

You can configure NetBIOS filters to do the following:

- Allow or disallow the sending of NetBIOS packets from the LAN to the WAN and from the WAN to the LAN.
- Allow or disallow the sending of NetBIOS packets from the LAN to the DMZ and from the DMZ to the LAN.
- Allow or disallow the sending of NetBIOS packets from the WAN to the DMZ and from the DMZ to the WAN.
- Allow or disallow the sending of NetBIOS packets through VPN connections.
- Allow or disallow NetBIOS packets to initiate calls.

### Display NetBIOS Filter Settings

Syntax: `sys filter netbios disp`

This command gives a read-only list of the current NetBIOS filter modes for The ZyWALL.

#### NetBIOS Display Filter Settings Command Example

```
===== NetBIOS Filter Status =====  
Between LAN and WAN: Block  
Between LAN and DMZ: Block  
Between WAN and DMZ: Block  
IPSec Packets: Forward  
Trigger Dial: Disabled
```

The filter types and their default settings are as follows.

**Table 272** NetBIOS Filter Default Settings

NAME	DESCRIPTION	EXAMPLE
Between LAN and WAN	This field displays whether NetBIOS packets are blocked or forwarded between the LAN and the WAN.	Block
Between LAN and DMZ	This field displays whether NetBIOS packets are blocked or forwarded between the LAN and the DMZ.	Block
Between WAN and DMZ	This field displays whether NetBIOS packets are blocked or forwarded between the WAN and the DMZ.	Block
IPSec Packets	This field displays whether NetBIOS packets sent through a VPN connection are blocked or forwarded.	Forward
Trigger dial	This field displays whether NetBIOS packets are allowed to initiate calls. Disabled means that NetBIOS packets are blocked from initiating calls.	Disabled

## NetBIOS Filter Configuration

Syntax: `sys filter netbios config <type> <on|off>`

where

`<type>` = Identify which NetBIOS filter (numbered 0-3) to configure.

- 0 = Between LAN and WAN
- 1 = Between LAN and DMZ
- 2 = Between WAN and DMZ
- 3 = IPSec packet pass through
- 4 = Trigger Dial

`<on|off>` = For type 0 and 1, use on to enable the filter and block NetBIOS packets. Use off to disable the filter and forward NetBIOS packets. For type 3, use on to block NetBIOS packets from being sent through a VPN connection. Use off to allow NetBIOS packets to be sent through a VPN connection. For type 4, use on to allow NetBIOS packets to initiate dial backup calls. Use off to block NetBIOS packets from initiating dial backup calls.

### Example commands

`sys filter netbios config 0 on` This command blocks LAN to WAN and WAN to LAN NetBIOS packets.

`sys filter netbios config 1 off` This command forwards LAN to DMZ and DMZ to LAN NetBIOS packets.

`sys filter netbios` This command blocks IPSec NetBIOS packets.  
`config 3 on`

`sys filter netbios` This command stops NetBIOS commands from initiating calls.  
`config 4 off`





# APPENDIX P

## Certificates Commands

The following describes the certificate commands. See [Appendix M on page 754](#) for information on the command structure.

All of these commands start with certificates.

**Table 273** Certificates Commands

COMMAND	DESCRIPTION		
my_cert			
	create		
	create	selfsigned <name> <subject> [key size]	Create a self-signed local host certificate. <name> specifies a descriptive name for the generated certificate. <subject> specifies a subject name (required) and alternative name (required). The format is "subject-name-dn:{ip,dns,email}=value". If the name contains spaces, please put it in quotes. [key size] specifies the key size. It has to be an integer from 512 to 2048. The default is 1024 bits.
	create	request <name> <subject> [key size]	Create a certificate request and save it to the router for later manual enrollment. <name> specifies a descriptive name for the generated certification request. <subject> specifies a subject name (required) and alternative name (required). The format is "subject-name-dn:{ip,dns,email}=value". If the name contains spaces, please put it in quotes. [key size] specifies the key size. It has to be an integer from 512 to 2048. The default is 1024 bits.
	create	scep_enroll <name> <CA addr> <CA cert> <auth key> <subject> [key size]	Create a certificate request and enroll for a certificate immediately online using SCEP protocol. <name> specifies a descriptive name for the enrolled certificate. <CA addr> specifies the CA server address. <CA cert> specifies the name of the CA certificate. <auth key> specifies the key used for user authentication. If the key contains spaces, please put it in quotes. To leave it blank, type "". <subject> specifies a subject name (required) and alternative name (required). The format is "subject-name-dn:{ip,dns,email}=value". If the name contains spaces, please put it in quotes. [key size] specifies the key size. It has to be an integer from 512 to 2048. The default is 1024 bits.

**Table 273** Certificates Commands (continued)

COMMAND	DESCRIPTION		
	create	cmp_enroll <name> <CA addr> <CA cert> <auth key> <subject> [key size]	Create a certificate request and enroll for a certificate immediately online using CMP protocol. <name> specifies a descriptive name for the enrolled certificate. <CA addr> specifies the CA server address. <CA cert> specifies the name of the CA certificate. <auth key> specifies the id and key used for user authentication. The format is "id:key". To leave the id and key blank, type ".". <subject> specifies a subject name (required) and alternative name (required). The format is "subject-name-dn:{ip,dns,email}=value". If the name contains spaces, please put it in quotes. [key size] specifies the key size. It has to be an integer from 512 to 2048. The default is 1024 bits.
	import	[name]	Import the PEM-encoded certificate from stdin. [name] specifies the descriptive name (optional) as which the imported certificate is to be saved. For my certificate importation to be successful, a certification request corresponding to the imported certificate must already exist on ZyWALL. After the importation, the certification request will automatically be deleted. If a descriptive name is not specified for the imported certificate, the certificate will adopt the descriptive name of the certification request.
	export	<name>	Export the PEM-encoded certificate to stdout for user to copy and paste. <name> specifies the name of the certificate to be exported.
	view	<name>	View the information of the specified local host certificate. <name> specifies the name of the certificate to be viewed.
	verify	<name> [timeout]	Verify the certification path of the specified local host certificate. <name> specifies the name of the certificate to be verified. [timeout] specifies the timeout value in seconds (optional). The default timeout value is 20 seconds.
	delete	<name>	Delete the specified local host certificate. <name> specifies the name of the certificate to be deleted.
	list		List all my certificate names and basic information.
	rename	<old name> <new name>	Rename the specified my certificate. <old name> specifies the name of the certificate to be renamed. <new name> specifies the new name as which the certificate is to be saved.
	def_self_signed	[name]	Set the specified self-signed certificate as the default self-signed certificate. [name] specifies the name of the certificate to be set as the default self-signed certificate. If [name] is not specified, the name of the current self-signed certificate is displayed.

**Table 273** Certificates Commands (continued)

COMMAND	DESCRIPTION		
	replace_factory		Create a certificate using your device MAC address that will be specific to this device. The factory default certificate is a common default certificate for all ZyWALL models.
ca_trusted			
	import	<name>	Import the PEM-encoded certificate from stdin. <name> specifies the name as which the imported CA certificate is to be saved.
	export	<name>	Export the PEM-encoded certificate to stdout for user to copy and paste. <name> specifies the name of the certificate to be exported.
	view	<name>	View the information of the specified trusted CA certificate. <name> specifies the name of the certificate to be viewed.
	verify	<name> [timeout]	Verify the certification path of the specified trusted CA certificate. <name> specifies the name of the certificate to be verified. [timeout] specifies the timeout value in seconds (optional). The default timeout value is 20 seconds.
	delete	<name>	Delete the specified trusted CA certificate. <name> specifies the name of the certificate to be deleted.
	list		List all trusted CA certificate names and basic information.
	rename	<old name> <new name>	Rename the specified trusted CA certificate. <old name> specifies the name of the certificate to be renamed. <new name> specifies the new name as which the certificate is to be saved.
	crl_issuer	<name> [on off]	Specify whether or not the specified CA issues CRL. <name> specifies the name of the CA certificate. [on off] specifies whether or not the CA issues CRL. If [on off] is not specified, the current crl_issuer status of the CA.
remote_trusted			
	import	<name>	Import the PEM-encoded certificate from stdin. <name> specifies the name as which the imported remote host certificate is to be saved.
	export	<name>	Export the PEM-encoded certificate to stdout for user to copy and paste. <name> specifies the name of the certificate to be exported.
	view	<name>	View the information of the specified trusted remote host certificate. <name> specifies the name of the certificate to be viewed.
	verify	<name> [timeout]	Verify the certification path of the specified trusted remote host certificate. <name> specifies the name of the certificate to be verified. [timeout] specifies the timeout value in seconds (optional). The default timeout value is 20 seconds.

**Table 273** Certificates Commands (continued)

COMMAND	DESCRIPTION		
	delete	<name>	Delete the specified trusted remote host certificate. <name> specifies the name of the certificate to be deleted.
	list		List all trusted remote host certificate names and basic information.
	rename	<old name> <new name>	Rename the specified trusted remote host certificate. <old name> specifies the name of the certificate to be renamed. <new name> specifies the new name as which the certificate is to be saved.
dir_server			
	add	<name> <addr[:port]> > [login:pswd]	Add a new directory service. <name> specifies a descriptive name as which the added directory server is to be saved. <addr[:port]> specifies the server address (required) and port (optional). The format is "server-address[:port]". The default port is 389. [login:pswd] specifies the login name and password, if required. The format is "[login:password]".
	delete	<name>	Delete the specified directory service. <name> specifies the name of the directory server to be deleted.
	view	<name>	View the specified directory service. <name> specifies the name of the directory server to be viewed.
	edit	<name> <addr[:port]> > [login:pswd]	Edit the specified directory service. <name> specifies the name of the directory server to be edited. <addr[:port]> specifies the server address (required) and port (optional). The format is "server-address[:port]". The default port is 389. [login:pswd] specifies the login name and password, if required. The format is "[login:password]".
	list		List all directory service names and basic information.
	rename	<old name> <new name>	Rename the specified directory service. <old name> specifies the name of the directory server to be renamed. <new name> specifies the new name as which the directory server is to be saved.
cert_manager			
	reinit		Reinitialize the certificate manager.

# APPENDIX Q

## Brute-Force Password Guessing Protection

Brute-force password guessing protection allows you to specify a wait-time that must expire before entering a fourth password after three incorrect passwords have been entered.

The following describes the commands for enabling, disabling and configuring the brute-force password guessing protection mechanism for the password. See [Appendix M on page 754](#) for information on the command structure.

**Table 274** Brute-Force Password Guessing Protection Commands

COMMAND	DESCRIPTION
sys pwderrtm	This command displays the brute-force guessing password protection settings.
sys pwderrtm 0	This command turns off the password's protection from brute-force guessing. The brute-force password guessing protection is turned off by default.
sys pwderrtm N	This command sets the password protection to block all access attempts for N (a number from 1 to 60) minutes after the third time an incorrect password is entered.

### Example

```
sys pwderrtm 5
```

This command sets the password protection to block all access attempts for five minutes after the third time an incorrect password is entered.



# APPENDIX R

## Boot Commands

The BootModule AT commands execute from within the router's bootup software, when debug mode is selected before the main router firmware is started. When you start up your ZyWALL, you are given a choice to go into debug mode by pressing a key at the prompt shown in the following screen. In debug mode you have access to a series of boot module commands, for example ATUR (for uploading firmware) and ATLC (for uploading the configuration file). These are already discussed in the **Firmware and Configuration File Maintenance** chapter.

**Figure 494** Option to Enter Debug Mode

```
Bootbase Version: V1.02 | 08/08/2001 15:40:50
RAM: Size = 16384 Kbytes
DRAM Post: Testing: 16384K OK
FLASH: Intel 16M
RAS Version: V3.50(WB.0)b3 | 08/08/2001 16:21:27
Press any key to enter debug mode within 3
seconds.
.....
```

Enter ATHE to view all available ZyWALL boot module commands as shown in the next screen. ATBAx allows you to change the console port speed. The x denotes the number preceding the colon to give the console port speed following the colon in the list of numbers that follows; for example ATBA3 will give a console port speed of 9.6 Kbps. ATSE displays the seed that is used to generate a password to turn on the debug flag in the firmware. The ATSH command shows product related information such as boot module version, vendor name, product model, RAS code revision, etc. ATGO allows you to continue booting the system. Most other commands aid in advanced troubleshooting and should only be used by qualified engineers.



**Figure 495** Boot Module Commands

AT	just answer OK
ATHE	print help
ATBAx	change baudrate. 1:38.4k, 2:19.2k, 3:9.6k 4:57.6k 5:115.2k
ATENx,(y)	set BootExtension Debug Flag (y=password)
ATSE	show the seed of password generator
ATTI(h,m,s)	change system time to hour:min:sec or show current time
ATDA(y,m,d)	change system date to year/month/day or show current date
ATDS	dump RAS stack
ATDT	dump Boot Module Common Area
ATDUx,y	dump memory contents from address x for length y
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
ATRTw,x,y(,z)	RAM test level w, from address x to y (z iterations)
ATSH	dump manufacturer related data in ROM
ATDOx,y	download from address x for length y to PC via XMODEM
ATTD	download router configuration to PC via XMODEM
ATUR	upload router firmware to flash ROM
ATLC	upload router configuration file to flash ROM
ATXSx	xmodem select: x=0: CRC mode(default); x=1: checksum mode
ATSR	system reboot

# APPENDIX S

## Log Descriptions

This appendix provides descriptions of example log messages.

**Table 275** System Maintenance Logs

LOG MESSAGE	DESCRIPTION
Time calibration is successful	The router has adjusted its time based on information from the time server.
Time calibration failed	The router failed to get information from the time server.
WAN interface gets IP: %s	A WAN interface got a new IP address from the DHCP, PPPoE, PPTP or dial-up server.
DHCP client IP expired	A DHCP client's IP address has expired.
DHCP server assigns %s	The DHCP server assigned an IP address to a client.
Successful SMT login	Someone has logged on to the router's SMT interface.
SMT login failed	Someone has failed to log on to the router's SMT interface.
Successful WEB login	Someone has logged on to the router's web configurator interface.
WEB login failed	Someone has failed to log on to the router's web configurator interface.
Successful TELNET login	Someone has logged on to the router via telnet.
TELNET login failed	Someone has failed to log on to the router via telnet.
Successful FTP login	Someone has logged on to the router via ftp.
FTP login failed	Someone has failed to log on to the router via ftp.
NAT Session Table is Full!	The maximum number of NAT session table entries has been exceeded and the table is full.
Starting Connectivity Monitor	Starting Connectivity Monitor.
Time initialized by Daytime Server	The router got the time and date from the Daytime server.
Time initialized by Time server	The router got the time and date from the time server.
Time initialized by NTP server	The router got the time and date from the NTP server.
Connect to Daytime server fail	The router was not able to connect to the Daytime server.
Connect to Time server fail	The router was not able to connect to the Time server.
Connect to NTP server fail	The router was not able to connect to the NTP server.
Too large ICMP packet has been dropped	The router dropped an ICMP packet that was too large.
SMT Session Begin	An SMT management session has started.
SMT Session End	An SMT management session has ended.

**Table 275** System Maintenance Logs (continued)

LOG MESSAGE	DESCRIPTION
Configuration Change: PC = 0x%x, Task ID = 0x%x	The router is saving configuration changes.
Successful SSH login	Someone has logged on to the router's SSH server.
SSH login failed	Someone has failed to log on to the router's SSH server.
Successful HTTPS login	Someone has logged on to the router's web configurator interface using HTTPS protocol.
HTTPS login failed	Someone has failed to log on to the router's web configurator interface using HTTPS protocol.
DNS server %s was not responding to last 32 consecutive queries...	The specified DNS server did not respond to the last 32 consecutive queries.
DDNS update IP:%s (host %d) successfully	The device updated the IP address of the specified DDNS host name.
SMTP successfully	The device sent an e-mail.
myZyXEL.com registration successful	Registration of the device with myZyXEL.com was successful.
Trial service registration successful	Registration for a trial service was successful.
Service upgrade successful	Registration for a service upgrade was successful.
Service refresh successful.	The device successfully refreshed service information from myZyXEL.com.
Content Filter trial service activation successfully	The content filtering trial service was successfully activated for this device.
Anti-Spam trial service activation successfully	The anti-spam trial service was successfully activated for this device.
IDP/Anti-Virus trial service activation successfully	The IDP and anti-virus trial service was successfully activated for this device.
%s	The myZyXEL.com service registration failed due to the error listed. If you are unable to register for services at myZYXEL.com, the error message displayed in this log may be useful when contacting customer support.

**Table 276** System Error Logs

LOG MESSAGE	DESCRIPTION
%s exceeds the max. number of session per host!	This attempt to create a NAT session exceeds the maximum number of NAT session table entries allowed to be created per host.
setNetBIOSFilter: calloc error	The router failed to allocate memory for the NetBIOS filter settings.
readNetBIOSFilter: calloc error	The router failed to allocate memory for the NetBIOS filter settings.

**Table 276** System Error Logs (continued)

LOG MESSAGE	DESCRIPTION
WAN connection is down.	A WAN connection is down. You cannot access the network through this interface.
Dial Backup starts	Dial backup started working.
Dial Backup ends	Dial backup stopped working.
DHCP Server cannot assign the static IP %S (out of range).	The LAN subnet, LAN alias 1, or LAN alias 2 was changed and the specified static DHCP IP addresses are no longer valid.
The DHCP static IP %s is conflict.	The static DHCP IP address conflicts with another host.
SMTP fail (%s)	The device failed to send an e-mail (error message included).
SMTP authentication fail (%s)	The device failed to authenticate with the SMTP server (error message included).

**Table 277** Access Control Logs

LOG MESSAGE	DESCRIPTION
Firewall default policy: [ TCP   UDP   IGMP   ESP   GRE   OSPF ] <Packet Direction>	Attempted TCP/UDP/IGMP/ESP/GRE/OSPF access matched the default policy and was blocked or forwarded according to the default policy's setting.
Firewall rule [NOT] match:[ TCP   UDP   IGMP   ESP   GRE   OSPF ] <Packet Direction>, <rule:%d>	Attempted TCP/UDP/IGMP/ESP/GRE/OSPF access matched (or did not match) a configured firewall rule (denoted by its number) and was blocked or forwarded according to the rule.
Triangle route packet forwarded: [ TCP   UDP   IGMP   ESP   GRE   OSPF ]	The firewall allowed a triangle route session to pass through.
Packet without a NAT table entry blocked: [ TCP   UDP   IGMP   ESP   GRE   OSPF ]	The router blocked a packet that didn't have a corresponding NAT table entry.
Router sent blocked web site message: TCP	The router sent a message to notify a user that the router blocked access to a web site that the user requested.
Exceed maximum sessions per host (%d).	The device blocked a session because the host's connections exceeded the maximum sessions per host.
Firewall allowed a packet that matched a NAT session: [ TCP   UDP ]	A packet from the WAN (TCP or UDP) matched a cone NAT session and the device forwarded it to the LAN.

**Table 278** TCP Reset Logs

LOG MESSAGE	DESCRIPTION
Under SYN flood attack, sent TCP RST	The router sent a TCP reset packet when a host was under a SYN flood attack (the TCP incomplete count is per destination host.)
Exceed TCP MAX incomplete, sent TCP RST	The router sent a TCP reset packet when the number of TCP incomplete connections exceeded the user configured threshold. (the TCP incomplete count is per destination host.) Note: Refer to <b>TCP Maximum Incomplete</b> in the <b>Firewall Attack Alerts</b> screen.
Peer TCP state out of order, sent TCP RST	The router sent a TCP reset packet when a TCP connection state was out of order. Note: The firewall refers to RFC793 Figure 6 to check the TCP state.
Firewall session time out, sent TCP RST	The router sent a TCP reset packet when a dynamic firewall session timed out.  The default timeout values are as follows: ICMP idle timeout: 3 minutes UDP idle timeout: 3 minutes TCP connection (three way handshaking) timeout: 270 seconds TCP FIN-wait timeout: 2 MSL (Maximum Segment Lifetime set in the TCP header). TCP idle (established) timeout (s): 150 minutes TCP reset timeout: 10 seconds
Exceed MAX incomplete, sent TCP RST	The router sent a TCP reset packet when the number of incomplete connections (TCP and UDP) exceeded the user-configured threshold. (Incomplete count is for all TCP and UDP connections through the firewall.) Note: When the number of incomplete connections (TCP + UDP) > "Maximum Incomplete High", the router sends TCP RST packets for TCP connections and destroys TOS (firewall dynamic sessions) until incomplete connections < "Maximum Incomplete Low".
Access block, sent TCP RST	The router sends a TCP RST packet and generates this log if you turn on the firewall TCP reset mechanism (via CLI command: "sys firewall tcprst").

**Table 279** Packet Filter Logs

LOG MESSAGE	DESCRIPTION
[ TCP   UDP   ICMP   IGMP   Generic ] packet filter matched (set: %d, rule: %d)	Attempted access matched a configured filter rule (denoted by its set and rule number) and was blocked or forwarded according to the rule.

For type and code details, see [Table 294 on page 789](#).

**Table 280** ICMP Logs

LOG MESSAGE	DESCRIPTION
Firewall default policy: ICMP <Packet Direction>, <type:%d>, <code:%d>	ICMP access matched the default policy and was blocked or forwarded according to the user's setting.
Firewall rule [NOT] match: ICMP <Packet Direction>, <rule:%d>, <type:%d>, <code:%d>	ICMP access matched (or didn't match) a firewall rule (denoted by its number) and was blocked or forwarded according to the rule.
Triangle route packet forwarded: ICMP	The firewall allowed a triangle route session to pass through.
Packet without a NAT table entry blocked: ICMP	The router blocked a packet that didn't have a corresponding NAT table entry.
Unsupported/out-of-order ICMP: ICMP	The firewall does not support this kind of ICMP packets or the ICMP packets are out of order.
Router reply ICMP packet: ICMP	The router sent an ICMP reply packet to the sender.

**Table 281** CDR Logs

LOG MESSAGE	DESCRIPTION
board %d line %d channel %d, call %d, %s C01 Outgoing Call dev=%x ch=%x %s	The router received the setup requirements for a call. "call" is the reference (count) number of the call. "dev" is the device type (3 is for dial-up, 6 is for PPPoE, 10 is for PPTP). "channel" or "ch" is the call channel ID. For example, "board 0 line 0 channel 0, call 3, C01 Outgoing Call dev=6 ch=0" Means the router has dialed to the PPPoE server 3 times.
board %d line %d channel %d, call %d, %s C02 OutCall Connected %d %s	The PPPoE, PPTP or dial-up call is connected.
board %d line %d channel %d, call %d, %s C02 Call Terminated	The PPPoE, PPTP or dial-up call was disconnected.

**Table 282** PPP Logs

LOG MESSAGE	DESCRIPTION
ppp:LCP Starting	The PPP connection's Link Control Protocol stage has started.
ppp:LCP Opening	The PPP connection's Link Control Protocol stage is opening.
ppp:CHAP Opening	The PPP connection's Challenge Handshake Authentication Protocol stage is opening.
ppp:IPCP Starting	The PPP connection's Internet Protocol Control Protocol stage is starting.
ppp:IPCP Opening	The PPP connection's Internet Protocol Control Protocol stage is opening.

**Table 282** PPP Logs (continued)

LOG MESSAGE	DESCRIPTION
ppp:LCP Closing	The PPP connection's Link Control Protocol stage is closing.
ppp:IPCP Closing	The PPP connection's Internet Protocol Control Protocol stage is closing.

**Table 283** UPnP Logs

LOG MESSAGE	DESCRIPTION
UPnP pass through Firewall	UPnP packets can pass through the firewall.

**Table 284** Content Filtering Logs

LOG MESSAGE	DESCRIPTION
%s: Keyword blocking	The content of a requested web page matched a user defined keyword.
%s: Not in trusted web list	The web site is not in a trusted domain, and the router blocks all traffic except trusted domain sites.
%s: Forbidden Web site	The web site is in the forbidden web site list.
%s: Contains ActiveX	The web site contains ActiveX.
%s: Contains Java applet	The web site contains a Java applet.
%s: Contains cookie	The web site contains a cookie.
%s: Proxy mode detected	The router detected proxy mode in the packet.
%s	The content filter server responded that the web site is in the blocked category list, but it did not return the category type.
%s: %s	The content filter server responded that the web site is in the blocked category list, and returned the category type.
%s(cache hit)	The system detected that the web site is in the blocked list from the local cache, but does not know the category type.
%s :%s(cache hit)	The system detected that the web site is in blocked list from the local cache, and knows the category type.
%s: Trusted Web site	The web site is in a trusted domain.
%s	When the content filter is not on according to the time schedule or you didn't select the "Block Matched Web Site" checkbox, the system forwards the web content.
Waiting content filter server timeout	The external content filtering server did not respond within the timeout period.
DNS resolving failed	The ZyWALL cannot get the IP address of the external content filtering via DNS query.
Creating socket failed	The ZyWALL cannot issue a query because TCP/IP socket creation failed, port:port number.

**Table 284** Content Filtering Logs (continued)

LOG MESSAGE	DESCRIPTION
Connecting to content filter server fail	The connection to the external content filtering server failed.
License key is invalid	The external content filtering license key is invalid.

For type and code details, see [Table 294 on page 789](#).

**Table 285** Attack Logs

LOG MESSAGE	DESCRIPTION
attack [ TCP   UDP   IGMP   ESP   GRE   OSPF ]	The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF attack.
attack ICMP (type:%d, code:%d)	The firewall detected an ICMP attack.
land [ TCP   UDP   IGMP   ESP   GRE   OSPF ]	The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF land attack.
land ICMP (type:%d, code:%d)	The firewall detected an ICMP land attack.
ip spoofing - WAN [ TCP   UDP   IGMP   ESP   GRE   OSPF ]	The firewall detected an IP spoofing attack on the WAN port.
ip spoofing - WAN ICMP (type:%d, code:%d)	The firewall detected an ICMP IP spoofing attack on the WAN port.
icmp echo : ICMP (type:%d, code:%d)	The firewall detected an ICMP echo attack.
syn flood TCP	The firewall detected a TCP syn flood attack.
ports scan TCP	The firewall detected a TCP port scan attack.
teardrop TCP	The firewall detected a TCP teardrop attack.
teardrop UDP	The firewall detected an UDP teardrop attack.
teardrop ICMP (type:%d, code:%d)	The firewall detected an ICMP teardrop attack.
illegal command TCP	The firewall detected a TCP illegal command attack.
NetBIOS TCP	The firewall detected a TCP NetBIOS attack.
ip spoofing - no routing entry [ TCP   UDP   IGMP   ESP   GRE   OSPF ]	The firewall classified a packet with no source routing entry as an IP spoofing attack.
ip spoofing - no routing entry ICMP (type:%d, code:%d)	The firewall classified an ICMP packet with no source routing entry as an IP spoofing attack.
vulnerability ICMP (type:%d, code:%d)	The firewall detected an ICMP vulnerability attack.
traceroute ICMP (type:%d, code:%d)	The firewall detected an ICMP traceroute attack.
ports scan UDP	The firewall detected a UDP port scan attack.



**Table 285** Attack Logs (continued)

LOG MESSAGE	DESCRIPTION
Firewall sent TCP packet in response to DoS attack TCP	The firewall sent TCP packet in response to a DoS attack
ICMP Source Quench ICMP	The firewall detected an ICMP Source Quench attack.
ICMP Time Exceed ICMP	The firewall detected an ICMP Time Exceed attack.
ICMP Destination Unreachable ICMP	The firewall detected an ICMP Destination Unreachable attack.
ping of death. ICMP	The firewall detected an ICMP ping of death attack.
smurf ICMP	The firewall detected an ICMP smurf attack.
IP address in FTP port command is different from the client IP address. It maybe a bounce attack.	The IP address in an FTP port command is different from the client IP address. It may be a bounce attack.
Fragment packet size is smaller than the MTU size of output interface.	The fragment packet size is smaller than the MTU size of output interface.

**Table 286** Remote Management Logs

LOG MESSAGE	DESCRIPTION
Remote Management: FTP denied	Attempted use of FTP service was blocked according to remote management settings.
Remote Management: TELNET denied	Attempted use of TELNET service was blocked according to remote management settings.
Remote Management: HTTP or UPnP denied	Attempted use of HTTP or UPnP service was blocked according to remote management settings.
Remote Management: WWW denied	Attempted use of WWW service was blocked according to remote management settings.
Remote Management: HTTPS denied	Attempted use of HTTPS service was blocked according to remote management settings.
Remote Management: SSH denied	Attempted use of SSH service was blocked according to remote management settings.
Remote Management: ICMP Ping response denied	Attempted use of ICMP service was blocked according to remote management settings.
Remote Management: SNMP denied	Attempted use of SNMP service was blocked according to remote management settings.
Remote Management: DNS denied	Attempted use of DNS service was blocked according to remote management settings.

**Table 287** Wireless Logs

LOG MESSAGE	DESCRIPTION
WLAN MAC Filter Fail	The MAC filter blocked a wireless station from connecting to the device.
WLAN MAC Filter Success	The MAC filter allowed a wireless station to connect to the device.
WLAN STA Association	A wireless station associated with the device.
WLAN STA Association List Full	The maximum number of associated wireless clients has been reached.
WLAN STA Association Again	The SSID and time of association were updated for an wireless station that was already associated.

**Table 288** IPsec Logs

LOG MESSAGE	DESCRIPTION
Discard REPLAY packet	The router received and discarded a packet with an incorrect sequence number.
Inbound packet authentication failed	The router received a packet that has been altered. A third party may have altered or tampered with the packet.
Receive IPsec packet, but no corresponding tunnel exists	The router dropped an inbound packet for which SPI could not find a corresponding phase 2 SA.
Rule <%d> idle time out, disconnect	The router dropped a connection that had outbound traffic and no inbound traffic for a certain time period. You can use the "ipsec timer chk_conn" CLI command to set the time period. The default value is 2 minutes.
WAN IP changed to <IP>	The router dropped all connections with the "MyIP" configured as "0.0.0.0" when the WAN IP address changed.
Inbound packet decryption failed	Please check the algorithm configuration.
Cannot find outbound SA for rule <%d>	A packet matches a rule, but there is no phase 2 SA for outbound traffic.
Rule [%s] sends an echo request to peer	The device sent a ping packet to check the specified VPN tunnel's connectivity.
Rule [%s] receives an echo reply from peer	The device received a ping response when checking the specified VPN tunnel's connectivity.

**Table 289** IKE Logs

LOG MESSAGE	DESCRIPTION
Active connection allowed exceeded	The IKE process for a new connection failed because the limit of simultaneous phase 2 SAs has been reached.
Start Phase 2: Quick Mode	Phase 2 Quick Mode has started.
Verifying Remote ID failed:	The connection failed during IKE phase 2 because the router and the peer's Local/Remote Addresses don't match.
Verifying Local ID failed:	The connection failed during IKE phase 2 because the router and the peer's Local/Remote Addresses don't match.
IKE Packet Retransmit	The router retransmitted the last packet sent because there was no response from the peer.
Failed to send IKE Packet	An Ethernet error stopped the router from sending IKE packets.
Too many errors! Deleting SA	An SA was deleted because there were too many errors.
Phase 1 IKE SA process done	The phase 1 IKE SA process has been completed.
Duplicate requests with the same cookie	The router received multiple requests from the same peer while still processing the first IKE packet from the peer.
IKE Negotiation is in process	The router has already started negotiating with the peer for the connection, but the IKE process has not finished yet.
No proposal chosen	Phase 1 or phase 2 parameters don't match. Please check all protocols / settings. Ex. One device being configured for 3DES and the other being configured for DES causes the connection to fail.
Local / remote IPs of incoming request conflict with rule <%d>	The security gateway is set to "0.0.0.0" and the router used the peer's "Local Address" as the router's "Remote Address". This information conflicted with static rule #d; thus the connection is not allowed.
Cannot resolve Secure Gateway Addr for rule <%d>	The router couldn't resolve the IP address from the domain name that was used for the secure gateway address.
Peer ID: <peer id> <My remote type> -<My local type>	The displayed ID information did not match between the two ends of the connection.
vs. My Remote <My remote> -<My remote>	The displayed ID information did not match between the two ends of the connection.
vs. My Local <My local>-<My local>	The displayed ID information did not match between the two ends of the connection.
Send <packet>	A packet was sent.
Recv <packet>	IKE uses ISAKMP to transmit data. Each ISAKMP packet contains many different types of payloads. All of them show in the LOG. Refer to RFC2408 – ISAKMP for a list of all ISAKMP payload types.
Recv <Main or Aggressive> Mode request from <IP>	The router received an IKE negotiation request from the peer address specified.
Send <Main or Aggressive> Mode request to <IP>	The router started negotiation with the peer.
Invalid IP <Peer local> / <Peer local>	The peer's "Local IP Address" is invalid.

**Table 289** IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
Remote IP <Remote IP> / <Remote IP> conflicts	The security gateway is set to "0.0.0.0" and the router used the peer's "Local Address" as the router's "Remote Address". This information conflicted with static rule #d; thus the connection is not allowed.
Phase 1 ID type mismatch	This router's "Peer ID Type" is different from the peer IPsec router's "Local ID Type".
Phase 1 ID content mismatch	This router's "Peer ID Content" is different from the peer IPsec router's "Local ID Content".
No known phase 1 ID type found	The router could not find a known phase 1 ID in the connection attempt.
ID type mismatch. Local / Peer: <Local ID type/Peer ID type>	The phase 1 ID types do not match.
ID content mismatch	The phase 1 ID contents do not match.
Configured Peer ID Content: <Configured Peer ID Content>	The phase 1 ID contents do not match and the configured "Peer ID Content" is displayed.
Incoming ID Content: <Incoming Peer ID Content>	The phase 1 ID contents do not match and the incoming packet's ID content is displayed.
Unsupported local ID Type: <%d>	The phase 1 ID type is not supported by the router.
Build Phase 1 ID	The router has started to build the phase 1 ID.
Adjust TCP MSS to %d	The router automatically changed the TCP Maximum Segment Size value after establishing a tunnel.
Rule <%d> input idle time out, disconnect	The tunnel for the listed rule was dropped because there was no inbound traffic within the idle timeout period.
XAUTH succeed! Username: <Username>	The router used extended authentication to authenticate the listed username.
XAUTH fail! Username: <Username>	The router was not able to use extended authentication to authenticate the listed username.
Rule[%d] Phase 1 negotiation mode mismatch	The listed rule's IKE phase 1 negotiation mode did not match between the router and the peer.
Rule [%d] Phase 1 encryption algorithm mismatch	The listed rule's IKE phase 1 encryption algorithm did not match between the router and the peer.
Rule [%d] Phase 1 authentication algorithm mismatch	The listed rule's IKE phase 1 authentication algorithm did not match between the router and the peer.
Rule [%d] Phase 1 authentication method mismatch	The listed rule's IKE phase 1 authentication method did not match between the router and the peer.
Rule [%d] Phase 1 key group mismatch	The listed rule's IKE phase 1 key group did not match between the router and the peer.
Rule [%d] Phase 2 protocol mismatch	The listed rule's IKE phase 2 protocol did not match between the router and the peer.
Rule [%d] Phase 2 encryption algorithm mismatch	The listed rule's IKE phase 2 encryption algorithm did not match between the router and the peer.

**Table 289** IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
Rule [%d] Phase 2 authentication algorithm mismatch	The listed rule's IKE phase 2 authentication algorithm did not match between the router and the peer.
Rule [%d] Phase 2 encapsulation mismatch	The listed rule's IKE phase 2 encapsulation did not match between the router and the peer.
Rule [%d]> Phase 2 pfs mismatch	The listed rule's IKE phase 2 perfect forward secret (pfs) setting did not match between the router and the peer.
Rule [%d] Phase 1 ID mismatch	The listed rule's IKE phase 1 ID did not match between the router and the peer.
Rule [%d] Phase 1 hash mismatch	The listed rule's IKE phase 1 hash did not match between the router and the peer.
Rule [%d] Phase 1 preshared key mismatch	The listed rule's IKE phase 1 pre-shared key did not match between the router and the peer.
Rule [%d] Tunnel built successfully	The listed rule's IPSec tunnel has been built successfully.
Rule [%d] Peer's public key not found	The listed rule's IKE phase 1 peer's public key was not found.
Rule [%d] Verify peer's signature failed	The listed rule's IKE phase 1 verification of the peer's signature failed.
Rule [%d] Sending IKE request	IKE sent an IKE request for the listed rule.
Rule [%d] Receiving IKE request	IKE received an IKE request for the listed rule.
Swap rule to rule [%d]	The router changed to using the listed rule.
Rule [%d] Phase 1 key length mismatch	The listed rule's IKE phase 1 key length (with the AES encryption algorithm) did not match between the router and the peer.
Rule [%d] phase 1 mismatch	The listed rule's IKE phase 1 did not match between the router and the peer.
Rule [%d] phase 2 mismatch	The listed rule's IKE phase 2 did not match between the router and the peer.
Rule [%d] Phase 2 key length mismatch	The listed rule's IKE phase 2 key lengths (with the AES encryption algorithm) did not match between the router and the peer.
Remote Gateway Addr in rule [%s] is changed to %s"	The IP address for the domain name of the peer gateway in the listed rule changed to the listed IP address.
New My ZyWALL Addr in rule [%s] is changed to %s	The IP address for the domain name of the ZyWALL in the listed rule changed to the listed IP address.
Remote Gateway Addr has changed, tunnel [%s] will be deleted	The listed tunnel will be deleted because the remote gateway's IP address changed.
My ZyWALL Addr has changed, tunnel [%s] will be deleted	The listed tunnel will be deleted because the ZyWALL's IP address changed.

**Table 290** PKI Logs

LOG MESSAGE	DESCRIPTION
Enrollment successful	The SCEP online certificate enrollment was successful. The Destination field records the certification authority server IP address and port.
Enrollment failed	The SCEP online certificate enrollment failed. The Destination field records the certification authority server's IP address and port.
Failed to resolve <SCEP CA server url>	The SCEP online certificate enrollment failed because the certification authority server's address cannot be resolved.
Enrollment successful	The CMP online certificate enrollment was successful. The Destination field records the certification authority server's IP address and port.
Enrollment failed	The CMP online certificate enrollment failed. The Destination field records the certification authority server's IP address and port.
Failed to resolve <CMP CA server url>	The CMP online certificate enrollment failed because the certification authority server's IP address cannot be resolved.
Rcvd ca cert: <subject name>	The router received a certification authority certificate, with subject name as recorded, from the LDAP server whose IP address and port are recorded in the Source field.
Rcvd user cert: <subject name>	The router received a user certificate, with subject name as recorded, from the LDAP server whose IP address and port are recorded in the Source field.
Rcvd CRL <size>: <issuer name>	The router received a CRL (Certificate Revocation List), with size and issuer name as recorded, from the LDAP server whose IP address and port are recorded in the Source field.
Rcvd ARL <size>: <issuer name>	The router received an ARL (Authority Revocation List), with size and issuer name as recorded, from the LDAP server whose address and port are recorded in the Source field.
Failed to decode the received ca cert	The router received a corrupted certification authority certificate from the LDAP server whose address and port are recorded in the Source field.
Failed to decode the received user cert	The router received a corrupted user certificate from the LDAP server whose address and port are recorded in the Source field.
Failed to decode the received CRL	The router received a corrupted CRL (Certificate Revocation List) from the LDAP server whose address and port are recorded in the Source field.
Failed to decode the received ARL	The router received a corrupted ARL (Authority Revocation List) from the LDAP server whose address and port are recorded in the Source field.
Rcvd data <size> too large! Max size allowed: <max size>	The router received directory data that was too large (the size is listed) from the LDAP server whose address and port are recorded in the Source field. The maximum size of directory data that the router allows is also recorded.
Cert trusted: <subject name>	The router has verified the path of the certificate with the listed subject name.
Due to <reason codes>, cert not trusted: <subject name>	Due to the reasons listed, the certificate with the listed subject name has not passed the path verification. The recorded reason codes are only approximate reasons for not trusting the certificate. Please see <a href="#">Table 291 on page 787</a> for the corresponding descriptions of the codes.

**Table 291** Certificate Path Verification Failure Reason Codes

CODE	DESCRIPTION
1	Algorithm mismatch between the certificate and the search constraints.
2	Key usage mismatch between the certificate and the search constraints.
3	Certificate was not valid in the time interval.
4	(Not used)
5	Certificate is not valid.
6	Certificate signature was not verified correctly.
7	Certificate was revoked by a CRL.
8	Certificate was not added to the cache.
9	Certificate decoding failed.
10	Certificate was not found (anywhere).
11	Certificate chain looped (did not find trusted root).
12	Certificate contains critical extension that was not handled.
13	Certificate issuer was not valid (CA specific information missing).
14	(Not used)
15	CRL is too old.
16	CRL is not valid.
17	CRL signature was not verified correctly.
18	CRL was not found (anywhere).
19	CRL was not added to the cache.
20	CRL decoding failed.
21	CRL is not currently valid, but in the future.
22	CRL contains duplicate serial numbers.
23	Time interval is not continuous.
24	Time information not available.
25	Database method failed due to timeout.
26	Database method failed.
27	Path was not verified.
28	Maximum path length reached.

**Table 292** 802.1X Logs

LOG MESSAGE	DESCRIPTION
Local User Database accepts user.	A user was authenticated by the local user database.
Local User Database reports user credential error.	A user was not authenticated by the local user database because of an incorrect user password.

**Table 292** 802.1X Logs (continued)

LOG MESSAGE	DESCRIPTION
Local User Database does not find user`s credential.	A user was not authenticated by the local user database because the user is not listed in the local user database.
RADIUS accepts user.	A user was authenticated by the RADIUS Server.
RADIUS rejects user. Pls check RADIUS Server.	A user was not authenticated by the RADIUS Server. Please check the RADIUS Server.
Local User Database does not support authentication method.	The local user database only supports the EAP-MD5 method. A user tried to use another authentication method and was not authenticated.
User logout because of session timeout expired.	The router logged out a user whose session expired.
User logout because of user deassociation.	The router logged out a user who ended the session.
User logout because of no authentication response from user.	The router logged out a user from which there was no authentication response.
User logout because of idle timeout expired.	The router logged out a user whose idle timeout period expired.
User logout because of user request.	A user logged out.
Local User Database does not support authentication method.	A user tried to use an authentication method that the local user database does not support (it only supports EAP-MD5).
No response from RADIUS. Pls check RADIUS Server.	There is no response message from the RADIUS server, please check the RADIUS server.
Use Local User Database to authenticate user.	The local user database is operating as the authentication server.
Use RADIUS to authenticate user.	The RADIUS server is operating as the authentication server.
No Server to authenticate user.	There is no authentication server to authenticate a user.
Local User Database does not find user`s credential.	A user was not authenticated by the local user database because the user is not listed in the local user database.

**Table 293** ACL Setting Notes

PACKET DIRECTION	DIRECTION	DESCRIPTION
(L to W)	LAN to WAN	ACL set for packets traveling from the LAN to the WAN.
(W to L)	WAN to LAN	ACL set for packets traveling from the WAN to the LAN.
(D to L)	DMZ to LAN	ACL set for packets traveling from the DMZ to the LAN.
(D to W)	DMZ to WAN	ACL set for packets traveling from the DMZ to the WAN.
(W to D)	WAN to DMZ	ACL set for packets traveling from the WAN to the DMZ.
(L to D)	LAN to DMZ	ACL set for packets traveling from the LAN to the DMZ.



**Table 293** ACL Setting Notes (continued)

PACKET DIRECTION	DIRECTION	DESCRIPTION
(L to L/ZW)	LAN to LAN/ ZyWALL	ACL set for packets traveling from the LAN to the LAN or the ZyWALL.
(W to W/ZW)	WAN to WAN/ ZyWALL	ACL set for packets traveling from the WAN to the WAN or the ZyWALL.
(D to D/ZW)	DMZ to DMZ/ ZyWALL	ACL set for packets traveling from the DMZ to the DM or the ZyWALL.
(L to WL)	LAN to WLAN	ACL set for packets traveling from the LAN to the WLAN.
(WL to L)	WLAN to LAN	ACL set for packets traveling from the WLAN to the LAN.
(W to WL)	WAN to WLAN	ACL set for packets traveling from the WAN to the WLAN.
(WL to W)	WLAN to WAN	ACL set for packets traveling from the WLAN to the WAN.
(D to WL)	DMZ to WLAN	ACL set for packets traveling from the DMZ to the WLAN.
(WL to D)	WLAN to DMZ	ACL set for packets traveling from the WLAN to the DMZ.
(WL to WL)	WLAN to WLAN/ ZyWALL	ACL set for packets traveling from the WLAN to the WLAN or the ZyWALL.

**Table 294** ICMP Notes

TYPE	CODE	DESCRIPTION
0		Echo Reply
	0	Echo reply message
3		Destination Unreachable
	0	Net unreachable
	1	Host unreachable
	2	Protocol unreachable
	3	Port unreachable
	4	A packet that needed fragmentation was dropped because it was set to Don't Fragment (DF)
	5	Source route failed
4		Source Quench
	0	A gateway may discard internet datagrams if it does not have the buffer space needed to queue the datagrams for output to the next network on the route to the destination network.
5		Redirect
	0	Redirect datagrams for the Network
	1	Redirect datagrams for the Host
	2	Redirect datagrams for the Type of Service and Network
	3	Redirect datagrams for the Type of Service and Host
8		Echo
	0	Echo message

**Table 294** ICMP Notes (continued)

TYPE	CODE	DESCRIPTION
11		Time Exceeded
	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded
12		Parameter Problem
	0	Pointer indicates the error
13		Timestamp
	0	Timestamp request message
14		Timestamp Reply
	0	Timestamp reply message
15		Information Request
	0	Information request message
16		Information Reply
	0	Information reply message

**Table 295** IDP Logs

LOG MESSAGE	DESCRIPTION
The buffer size is too small!	The buffer for holding IDP information such as the signature file version was too small to hold any more information.
The format of the user config file is incorrect!	There was a format error in the configuration backup file that someone attempted to load into the system.
The system is doing signature update now , please wait!	The device is updating the signature file.
No data!	The system could not find any IDP signatures that matched a search.
IDP %s!	The device detected an intrusion event in a connection. The format of %s is "ID" followed by the IDP ID signature number and the IDP signature name. For example, ID:10001,Window Ping.
Can not find the signature , please update the signature!	The device does not have a signature file loaded.
Failed in signature update - %s!	The device failed to update the signature file through the Internet. %s describes the reason for the error. You may need to provide the error message when contacting customer support if you are repeatedly unable to download the signature file from the update server.
Check signature version - %s.	The device attempted to check for the latest available signature version. %s gives details. Either the check was unsuccessful due to the server being busy or the device is already using the latest available firmware.

**Table 295** IDP Logs (continued)

LOG MESSAGE	DESCRIPTION
Signature update OK - New signature version: <Signature version> Release Date: <Release date>!	The device updated the signature file successfully. The signature file's version and release date are included.
The turbo card is not ready , please insert the card and reboot!	The turbo card is not installed.

**Table 296** AV Logs

LOG MESSAGE	DESCRIPTION
HTTP Virus infected - %s!	The device detected a virus in an HTTP connection. The format of %s is "ID" Vireus ID number, virus name, filename. For example , ID:30001,CIH.Win95,/game.exe.
FTPDATA Virus infected - %s!	The device detected a virus in a FTPDATA connection. The format of %s is "ID" Vireus ID number, virus name, filename. For example , ID:30001,CIH.Win95,/game.exe.
SMTP Virus infected - %s!	The device detected a virus in a SMTP connection. The format of %s is "ID" Vireus ID number, virus name, filename. For example , ID:30001,CIH.Win95,/game.exe.
POP3 Virus infected - %s!	The device detected a virus in a POP3 connection. The format of %s is "ID" Vireus ID number, virus name, filename. For example , ID:30001,CIH.Win95,/game.exe.
HTTP Bypass - %s!	The device bypassed the scanning of files in HTTP connections. %s is the filename. For example, game.zip.
FTPDATA Bypass - %s!	The device bypassed the scanning of files in FTP data connections. %s is the filename. For example, game.zip.
SMTP Bypass - %s!	The device bypassed the scanning of files in SMTP connections. %s is the filename. For example, game.zip.
POP3 Bypass - %s!	The device bypassed the scanning of files in POP3 connections. %s is the filename. For example, game.zip.
Can not find the signature , please update the signature!	The device does not have a signature file loaded.
Failed in signature update - %s!	The device failed to update the signature file through the Internet. %s describes the reason for the error. You may need to provide the error message when contacting customer support if you are repeatedly unable to download the signature file from the update server.
Check signature version - %s.	The device attempted to check for the latest available signature version. %s gives details. Either the check was unsuccessful due to the server being busy or the device is already using the latest available firmware.
Update the signature file successfully.	The device updated the signature file successfully.

**Table 296** AV Logs (continued)

LOG MESSAGE	DESCRIPTION
The turbo card is not ready , please insert the card and reboot!	The turbo card is not installed.
The system is doing signature update now , please wait!	The device is updating the signature file.

**Table 297** AS Logs

LOG MESSAGE	DESCRIPTION
Mail is in the Black List - Mail From:%EMAIL_ADDRESS% Subject:%MAIL_SUBJECT%!	An e-mail with the listed source and subject matched an anti-spam blacklist entry.
Mail score is higher than threshold - Spam Score:%d Mail From:%EMAIL_ADDRESS% Subject:%MAIL_SUBJECT%!	The spam score (listed) for the e-mail with the listed source and subject was higher than the spam score threshold.
Query external database timeout - [%Rating Server IP Address%]	The anti-spam external database query timed out. The following log identifies the e-mail that was being checked.
Mail From:Email address Subject:Mail Subject!	This is the source and subject of an e-mail for which the anti-spam external database query failed.
External database query failed - [%Rating Server IP Address%] %s!	An anti-spam external database query failed due to an error, such as Http Error 404, Http conection can't be built. Please refer to "reason" field. The following log identifies the e-mail that was being checked.
Mail From:Email address Subject:Mail Subject!	This is the source and subject of an e-mail for which the anti-spam external database query failed.
Exceed maximum mail sessions (%d).	The number of concurrent mail sessions went over the limit (%d).
Error code from anti-spam server - [%Rating Server IP Address%] %s!	The device received an error code from the anti-spam external database server. Please refer to "reason" field. The following log identifies the e-mail that was being checked.
Mail From:Email address Subject:Mail Subject!	This is the source and subject of an e-mail for which the anti-spam external database query failed.
Unknown anti-spam query response - [%Rating Server IP Address%]!	The device received a response with an unknown format from the anti-spam external database server. The following log identifies the e-mail that was being checked.
Mail From:Email address Subject:Mail Subject!	This is the source and subject of an e-mail for which the anti-spam external database query failed.

**Table 297** AS Logs (continued)

LOG MESSAGE	DESCRIPTION
Remove rating server [%Rating Server IP Address%] from server list!	The listed server IP address has been removed from the list of anti-spam external database servers.
"This is a phishing mail - Spam Score:%d Mail From:%EMAIL_ADDRESS% Subject:%MAIL_SUBJECT%!"	The spam score (listed) for the e-mail with the listed source and subject was higher than the spam score threshold. The anti-spam external database identified the e-mail as a phishing mail.
Invalid parameter for AsEngine!	There was an internal AS system error. This type of error causes the device to restart.
Mail Parser buffer is overflow!	There were too many characters in a single line of an e-mail header that the device was attempting to parse.
There is no available HTTP session for external database!	There was not an HTTP session available to query the external database.
Mail From:Email address Subject:Mail Subject!	This is the source and subject of an e-mail for which there was not an HTTP session available for querying the external database.
Mail Digest creating failed!	The device was not able to create a digest of an e-mail.
Mail From:Email address Subject:Mail Subject!	This is the source and subject of an e-mail for which the device was not able to create a digest.
There is no available timer for external database!	There was not an internal timer mechanism free for the anti-spam feature to use when sending a query to the external database.
Mail From:Email address Subject:Mail Subject!	This is the source and subject of an e-mail for which there was not an internal timer mechanism available for querying the external database.
There is no available HTTP session and timer for external database!	There was not an HTTP session available to query the external database. There also was not an internal timer mechanism free for the anti-spam feature to use when sending a query to the external database.
Mail From:Email address Subject:Mail Subject!	This is the source and subject of an e-mail for which there was no HTTP session and no internal timer mechanism available for querying the external database.

## Syslog Logs

There are two types of syslog: event logs and traffic logs. The device generates an event log when a system event occurs, for example, when a user logs in or the device is under attack. The device generates a traffic log when a "session" is terminated. A traffic log summarizes the session's type, when it started and stopped the amount of traffic that was sent and received and so on. An external log analyzer can reconstruct and analyze the traffic flowing through the device after collecting the traffic logs.

**Table 298** Syslog Logs

LOG MESSAGE	DESCRIPTION
Event Log: <Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="<msg>" note="<note>" devID="<mac address>" cat="<category>"	This message is sent by the system ("RAS" displays as the system name if you haven't configured one) when the router generates a syslog. The facility is defined in the web <b>MAIN MENU, LOGS, Log Settings</b> page. The severity is the log's syslog class. The definition of messages and notes are defined in the other log tables. The "devID" is the MAC address of the router's LAN port. The "cat" is the same as the category in the router's logs.
Traffic Log: <Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="Traffic Log" note="Traffic Log" devID="<mac address>" cat="Traffic Log" duration=seconds sent=sentBytes rcvd=receiveBytes dir="<from:to>" protoID=IPProtocolID proto="serviceName" trans="IPSec/Normal"	This message is sent by the device when the connection (session) is closed. The facility is defined in the Log Settings screen. The severity is the traffic log type. The message and note always display "Traffic Log". The "proto" field lists the service name. The "dir" field lists the incoming and outgoing interfaces ("LAN:LAN", "LAN:WAN", "LAN:DMZ", "LAN:DEV" for example).
Event Log: <Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" ob="<0 1>" ob_mac="<mac address>" msg="<msg>" note="<note>" devID="<mac address>" cat="<category>"	This message is sent by the device ("RAS" displays as the system name if you haven't configured one) at the time when this syslog is generated. The facility is defined in the web <b>MAIN MENU, LOGS, Log Settings</b> page. The severity is the log's syslog class. The definition of messages and notes are defined in the other log tables. OB is the Out Break flag and the mac address of the Out Break PC .
Event Log: <Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" ob="0 1" ob_mac="<mac address>" msg="<msg>" note="<note>" devID="<mac address>" cat="Anti Virus" encode="< uu   b64 >"	This message is sent by the device ("RAS" displays as the system name if you haven't configured one) at the time when this syslog is generated. The facility is defined in the web <b>MAIN MENU, LOGS, Log Settings</b> page. The severity is the log's syslog class. The "encode" message indicates the mail attachments encoding method. The definition of messages and notes are defined in the Anti-Virus log descriptions.

**Table 298** Syslog Logs (continued)

LOG MESSAGE	DESCRIPTION
Event Log: <Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" ob="<0 1>" ob_mac="<mac address>" msg="<msg>" note="<note>" devID="<mac address>" cat="IDP" class="<idp class>" sid="<idp sid>" act="<idp action>" count="1"	This message is sent by the device ("RAS" displays as the system name if you haven't configured one) at the time when this syslog is generated. The facility is defined in the web <b>MAIN MENU, LOGS, Log Settings</b> page. The severity is the log's syslog class. The definition of messages and notes are defined in the IDP log descriptions.
Event Log: <Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" ob="<0 1>" ob_mac="<mac address>" msg="<msg>" note="<note>" devID="<mac address>" cat="Anti Spam" 1stReIP="<IP>"	This message is sent by the device ("RAS" displays as the system name if you haven't configured one) at the time when this syslog is generated. The facility is defined in the web <b>MAIN MENU, LOGS, Log Settings</b> page. The severity is the log's syslog class. 1stReIP is the IP address of the first mail relay server. The definition of messages and notes are defined in the Anti-Spam log descriptions.

The following table shows RFC-2408 ISAKMP payload types that the log displays. Please refer to the RFC for detailed information on each type.

**Table 299** RFC-2408 ISAKMP Payload Types

LOG DISPLAY	PAYLOAD TYPE
SA	Security Association
PROP	Proposal
TRANS	Transform
KE	Key Exchange
ID	Identification
CER	Certificate
CER_REQ	Certificate Request
HASH	Hash
SIG	Signature
NONCE	Nonce
NOTFY	Notification
DEL	Delete
VID	Vendor ID

## Log Commands

Go to the command interpreter interface. [Appendix M on page 754](#) explains how to access and use the commands.

### Configuring What You Want the ZyWALL to Log

- 1 Use the `sys logs load` command to load the log setting buffer that allows you to configure which logs the ZyWALL is to record.
- 2 Use `sys logs category` to view a list of the log categories.

**Figure 496** Displaying Log Categories Example

```

ras> sys logs category
8021x          access      attack      display
error         icmp        ike         ipsec
javablocked   mten       packetfilter ppp
cdr           pki        tls         remote
tcpreset     traffic    upnp        urlblocked
urlforward    wireless

```

- 3 Use `sys logs category` followed by a log category to display the parameters that are available for the category.

**Figure 497** Displaying Log Parameters Example

```

ras> sys logs category access
Usage: [0:none/1:log/2:alert/3:both] [0:don't show debug type/
1:show debug type]

```

- 4 Use `sys logs category` followed by a log category and a parameter to decide what to record.  
Use 0 to not record logs for that category, 1 to record only logs for that category, 2 to record only alerts for that category, and 3 to record both logs and alerts for that category. Not every parameter is available with every category.
- 5 Use the `sys logs save` command to store the settings in the ZyWALL (you must do this in order to record logs).

### Displaying Logs

- Use the `sys logs display` command to show all of the logs in the ZyWALL's log.
- Use the `sys logs category display` command to show the log settings for all of the log categories.
- Use the `sys logs display [log category]` command to show the logs in an individual ZyWALL log category.



- Use the `sys logs clear` command to erase all of the ZyWALL's logs.

## Log Command Example

This example shows how to set the ZyWALL to record the access logs and alerts and then view the results.

```
ras> sys logs load
ras> sys logs category access 3
ras> sys logs save
ras> sys logs display access
```

#	.time	source	destination	notes
	message			
0	06/08/2004 05:58:21	172.21.4.154	224.0.1.24	ACCESS
	BLOCK			
	Firewall default policy: IGMP (W to W/ZW)			
1	06/08/2004 05:58:20	172.21.3.56	239.255.255.250	ACCESS
	BLOCK			
	Firewall default policy: IGMP (W to W/ZW)			
2	06/08/2004 05:58:20	172.21.0.2	239.255.255.254	ACCESS
	BLOCK			
	Firewall default policy: IGMP (W to W/ZW)			
3	06/08/2004 05:58:20	172.21.3.191	224.0.1.22	ACCESS
	BLOCK			
	Firewall default policy: IGMP (W to W/ZW)			
4	06/08/2004 05:58:20	172.21.0.254	224.0.0.1	ACCESS
	BLOCK			
	Firewall default policy: IGMP (W to W/ZW)			
5	06/08/2004 05:58:20	172.21.4.187:137	172.21.255.255:137	ACCESS
	BLOCK			
	Firewall default policy: UDP (W to W/ZW)			

# Index

## Numerics

10/100 Mbps Ethernet WAN [55](#)  
 110V AC [5](#)  
 230V AC [5](#)

## A

Abnormal Working Conditions [6](#)  
 AC [5](#)  
 Access control [247](#)  
 Access Point [545](#)  
 Accessories [5](#)  
 Action for Matched Packets [225](#)  
 Action for No Spam Score [273](#)  
 Action for Spam Mails [271](#)  
 Active [519](#), [521](#), [552](#)  
 Acts of God [6](#)  
 Address Assignment [142](#), [418](#)  
 Advanced Encryption Standard (AES) [304](#)  
 AES [304](#)  
 AH [304](#), [308](#)  
 Airflow [5](#)  
 alert message [726](#)  
 ALG [56](#), [466](#)  
 Allocated Budget [520](#), [554](#)  
 Alternative Subnet Mask Notation [696](#)  
 Anti-Probing [226](#)  
 Anti-Spam [266](#)  
   External DB [271](#)  
   General [270](#)  
 Anti-spam  
   Efficiency [269](#)  
   Speed [269](#)  
 Anti-Spam Customization [273](#)  
 Anti-Spam External Database [266](#)  
 Anti-Spam External DB [271](#)  
 Anti-Virus [258](#)  
 Anti-virus  
   Online update [262](#)  
 anti-virus packet scan [726](#)  
   Windows 98/Me requirements [726](#)  
 Anti-virus scan

  packet types [260](#)  
 AP (access point) [710](#)  
 Application Layer Gateway [56](#), [466](#)  
 Application-level Firewalls [202](#)  
 Applications [62](#)  
 AT command [516](#), [517](#), [613](#)  
 Attack Types [207](#)  
 Authen [519](#), [554](#)  
 Authentication [519](#), [553](#), [554](#), [716](#)  
 Authentication Header (AH) [304](#)  
 Authentication Protocol [553](#)  
 Authority [3](#)  
 Auto-negotiating 10/100 Mbps Ethernet DMZ [55](#)  
 auto-negotiation [55](#)

## B

backdoor [247](#)  
 Backup [497](#), [613](#)  
 Backup WAN [55](#)  
 Bandwidth Borrowing [407](#)  
 Bandwidth Class [402](#)  
 Bandwidth Filter [402](#), [413](#)  
 Bandwidth Management [57](#), [402](#)  
 Bandwidth Management Statistics [414](#)  
 Bandwidth Manager Class Configuration [411](#)  
 Bandwidth Manager Class Setup [410](#)  
 Bandwidth Manager Monitor [415](#)  
 Bandwidth Manager Summary [408](#)  
 Basement [5](#)  
 Blacklist [266](#), [269](#), [275](#)  
 Blank Header Values [270](#)  
 Blocking Time [228](#), [230](#)  
 Boot sector virus [258](#)  
 Bridge Protocol Data Units (BPDUs) [123](#)  
 Brute-force Attack, [206](#)  
 BSS [708](#)  
 Budget Management [630](#), [631](#)  
 buffer overflow [247](#)

**C**

CA [715](#)  
Cable Modem [203](#)  
Cables, Connecting [5](#)  
Call Back Delay [518](#)  
Call Control [630](#)  
Call History [631](#), [632](#)  
Call Scheduling [59](#), [648](#)  
    Max Number of Schedule Sets [648](#)  
    PPPoE [650](#)  
    Precedence [648](#)  
Call-Triggering Packet [608](#)  
CardBus slot [56](#)  
Central Network Management [60](#)  
certificate [321](#)  
Certificate Authority [715](#)  
Certifications [3](#)  
Changes or Modifications [3](#)  
Changing the Password [506](#)  
Channel [710](#)  
    Interference [710](#)  
Channel ID [191](#), [545](#)  
CHAP [519](#), [554](#)  
Charge [6](#)  
Circuit [3](#)  
Class B [3](#)  
Command Interpreter Mode [628](#)  
Command Line [614](#)  
Communications [3](#)  
Community [598](#)  
Compliance, FCC [3](#)  
Components [6](#)  
Computer virus [258](#)  
Computer virus infection and prevention [258](#)  
Computer virus types [258](#)  
Concurrent E-mail Sessions [271](#)  
Condition [6](#)  
Configuration [81](#), [110](#)  
Configuration File  
    Backup [613](#)  
Connecting Cables [5](#)  
Connection ID/Name [555](#)  
Consequential Damages [6](#)  
Console Port [602](#), [603](#), [604](#)  
    Configuration File Upload [625](#)  
    File Backup [617](#)  
    File Upload [624](#)  
    Restoring Files [620](#)  
Contact Information [7](#)  
Contacting Customer Support [7](#)

Content Filter Categories [271](#), [281](#)  
Content Filter General [278](#)  
Content Filtering [58](#), [266](#), [278](#)  
    Categories [278](#)  
    Customizing [288](#)  
    Days and Times [278](#)  
    Filter List [278](#)  
    Restrict Web Features [278](#)  
Copyright [2](#)  
Correcting Interference [3](#)  
Corrosive Liquids [5](#)  
Covers [5](#)  
CTS (Clear to Send) [711](#)  
Custom Ports  
    Creating/Editing [232](#)  
Customer Support [7](#)

**D**

Dampness [5](#)  
Danger [5](#)  
Data Encryption Standard (DES) [304](#)  
DDNS  
    Configuration [510](#)  
DDNS Type [512](#)  
Dealer [3](#)  
Default [499](#)  
Defective [6](#)  
Denial of Service [203](#), [204](#), [227](#), [228](#), [582](#)  
Denial of Services  
    Thresholds [229](#)  
Denmark, Contact Information [7](#)  
DES [304](#)  
Destination Address [217](#)  
DHCP [81](#), [110](#), [112](#), [113](#), [125](#), [175](#), [428](#), [484](#), [528](#)  
DHCP (Dynamic Host Configuration Protocol) [61](#)  
DHCP Ethernet Setup [527](#)  
DHCP Table [81](#)  
Diagnostic [608](#)  
Dial Timeout [518](#)  
Diffie-Hellman Key Groups [315](#)  
Digest [266](#)  
Disclaimer [2](#)  
Discretion [6](#)  
DMZ  
    IP Alias [538](#), [548](#)  
    IP Alias Setup [538](#), [549](#)  
    Port Filter Setup [536](#)  
    Setup [536](#), [537](#), [547](#)  
    TCP/IP Setup [537](#), [548](#)

DNS [452](#)  
 DNS Server  
   For VPN Host [419](#)  
 Domain Name [142](#), [276](#), [384](#), [484](#), [603](#)  
 DoS  
   Basics [204](#)  
   Types [205](#)  
 DoS (Denial of Service) [57](#)  
 Drop Timeout [518](#)  
 DSL Modem [62](#), [553](#)  
 DTR [159](#), [517](#)  
 Dust [5](#)  
 Dynamic DNS [428](#)  
 Dynamic DNS Support [60](#)  
 Dynamic WEP Key Exchange [717](#)  
 DYNDNS Wildcard [419](#), [428](#)

## E

EAP [182](#), [183](#), [187](#)  
 EAP Authentication [714](#), [715](#)  
 ECHO [384](#)  
 Edit IP [520](#), [552](#)  
 e-Donkey [247](#)  
 Efficiency [269](#)  
 Electric Shock [5](#)  
 Electrical Pipes [5](#)  
 E-Mail [276](#)  
 E-mail Attributes [269](#)  
 E-mail virus [258](#)  
 e-Mule [247](#)  
 Enable Wildcard [512](#)  
 Enable Wireless LAN [191](#)  
 Encapsulating Security Payload (ESP) [304](#)  
 Encapsulation [533](#), [552](#), [555](#)  
 Encryption [302](#), [718](#)  
 Entering Information [502](#)  
 Equal Value [6](#)  
 ESP [304](#), [308](#)  
 ESS [709](#)  
 ESSID [545](#)  
 Ethernet [84](#), [86](#), [143](#)  
 Ethernet Encapsulation [532](#), [551](#), [552](#), [558](#)  
 Europe [5](#)  
 Excess E-mail Sessions [271](#)  
 Exposure [5](#)  
 Extended Service Set [709](#)  
 Extended Service Set IDentification [191](#), [545](#)

Extensible Authentication Protocol [187](#)  
 External Database [266](#), [271](#)  
 External Database Service Status [273](#)

## F

Factory Default [515](#)  
 Factory LAN Defaults [110](#)  
 Failure [6](#)  
 Fairness-based Scheduler [404](#)  
 FCC [3](#)  
   Compliance [3](#)  
   Rules, Part 15 [3](#)  
 FCC Rules [3](#)  
 Federal Communications Commission [3](#)  
 File infector [258](#)  
 Filename Conventions [612](#)  
 Filter [525](#), [557](#), [584](#)  
   Applying [596](#)  
   Configuration [584](#)  
   Configuring [587](#)  
   DMZ [596](#)  
   Example [593](#)  
   Generic Filter Rule [591](#)  
   Generic Rule [592](#)  
   NAT [595](#)  
   Remote Node [597](#)  
   Structure [585](#)  
 Filters  
   Executing a Filter Rule [585](#)  
   IP Filter Logic Flow [590](#)  
 Finger [384](#)  
 Fingerprint ID [266](#)  
 Finland, Contact Information [7](#)  
 Firewall [57](#)  
   Access Methods [214](#)  
   Activating [582](#)  
   Address Type [225](#), [276](#)  
   Alerts [218](#)  
   Connection Direction [217](#)  
   Creating/Editing Rules [223](#)  
   Custom Ports See Custom Ports [232](#)  
   Firewall Vs Filters [212](#)  
   Guidelines For Enhancing Security [212](#)  
   Introduction [203](#)  
   Policies [214](#)  
   Rule Logic [216](#)  
   Services [233](#)  
   SMT Menus [582](#)  
   Types [202](#)  
   When To Use [213](#)  
 Firewall Threshold [229](#)

Firmware File  
Maintenance [612](#)  
Fitness [6](#)  
Flow Control [500](#)  
Fragmentation Threshold [711](#)  
Fragmentation threshold [711](#)  
France, Contact Information [7](#)  
Fraudsters [268](#)  
FTP [384](#), [428](#), [432](#), [447](#), [614](#), [638](#)  
File Upload [623](#)  
GUI-based Clients [615](#)  
Restoring Files [618](#)  
FTP File Transfer [621](#)  
FTP Restrictions [432](#), [615](#), [638](#)  
FTP Server [61](#), [575](#)  
Full Network Management [61](#)  
Functionally Equivalent [6](#)  
Fuse  
Replacement [676](#)  
Type [664](#)

## G

Gas Pipes [5](#)  
Gateway IP Addr [556](#)  
Gateway IP Address [533](#), [561](#)  
Gateway Policy [316](#)  
General Setup [484](#), [508](#)  
Germany, Contact Information [7](#)  
Global [374](#)  
God, act of [6](#)

## H

Half-Open Sessions [227](#)  
Harmful Interference [3](#)  
Header [276](#)  
Hidden Menus [502](#)  
Hidden node [710](#)  
High Voltage Points [5](#)  
Host [486](#), [512](#)  
Host IDs [694](#)  
How Prestige virus scan works [260](#)  
How SSH works [441](#)  
How STP Works [123](#)  
HTTP [202](#), [204](#), [384](#)  
HTTPS [57](#), [433](#)

HTTPS Example [436](#)  
HyperTerminal [625](#), [626](#)  
HyperTerminal program [617](#), [620](#)

## I

IBSS [708](#)  
ICMP echo [206](#)  
Identity Theft [268](#)  
Idle Timeout [520](#), [553](#), [554](#)  
IEEE 802.11b [56](#)  
IEEE 802.11g [712](#)  
IEEE 802.1x [59](#)  
IGMP [112](#)  
IKE Phases [313](#)  
IMAP [269](#)  
Incoming Protocol Filters [530](#)  
Independent Basic Service Set [708](#)  
Indirect Damages [6](#)  
Initial Screen [500](#)  
initialization vector (IV) [718](#)  
Inside [374](#)  
Inside Global Address [374](#)  
Inside Local Address [374](#)  
Installation  
Freestanding [672](#)  
Installing Fuses [676](#)  
Insurance [6](#)  
Interactive Applications [396](#)  
Interference [3](#)  
Interference Correction Measures [3](#)  
Interference Statement [3](#)  
Internet Access [84](#)  
ISP's Name [533](#)  
Internet Access Setup [532](#), [533](#), [562](#)  
Internet Control Message Protocol (ICMP) [206](#)  
Internet Message Access Protocol [269](#)  
Internet Protocol Security (IPSec) [302](#)  
Introduction to Filters [584](#)  
Intrusions  
Firewalls [240](#)  
Host [241](#)  
IDP [241](#)  
Network [241](#)  
Invalid Spam Score [273](#)  
IP Address [81](#), [111](#), [113](#), [125](#), [142](#), [175](#), [384](#), [386](#), [387](#),  
[529](#), [530](#), [533](#), [556](#), [569](#)  
Remote [522](#)  
IP Address Assignment [533](#), [556](#)

IP Addressing [694](#)  
 IP Alias [60](#), [530](#)  
 IP Alias Setup [530](#)  
 IP Classes [694](#)  
 IP Multicast [60](#)  
   Internet Group Management Protocol (IGMP) [60](#)  
 IP Policy Routing [60](#)  
 IP Pool [114](#), [164](#), [176](#), [528](#)  
 IP Pool Setup [110](#)  
 IP Ports [204](#)  
 IP Routing Policy (IPPR) [396](#)  
   Benefits [396](#)  
   Cost Savings [396](#)  
   Criteria [396](#)  
   Load Sharing [396](#)  
 IP Spoofing [205](#), [208](#)  
 IP Static Route [560](#), [561](#)  
   Active [561](#)  
   Destination IP Address [561](#)  
   IP Subnet Mask [561](#)  
   Name [561](#)  
   Route Number [561](#)  
 IP Subnet Mask [522](#), [530](#)  
   Remote [522](#)  
 IPSec [302](#)  
 IPSec algorithms [304](#)  
 IPSec and NAT [305](#)  
 IPSec architecture [304](#)  
 IPSec standard [57](#)  
 IPSec VPN Capability [57](#)  
 ISP Parameters [84](#)  
 ISP's Name [533](#)

## J

Junk E-mail [58](#), [266](#)

## K

Key Fields For Configuring Rules [216](#)

## L

Labor [6](#)  
 LAN IP Address [479](#), [482](#)  
 LAN Port Filter Setup [526](#)

LAN Setup [526](#), [527](#)  
 LAN TCP/IP [110](#)  
 LAN to WAN Rules [217](#)  
 LAND [205](#), [206](#)  
 Legal Rights [6](#)  
 Legitimate E-mail. [266](#)  
 Liability [2](#)  
 License [2](#)  
 License Active [273](#)  
 License Inactive [273](#)  
 Lightning [5](#)  
 Link type [71](#), [73](#)  
 Liquids, Corrosive [5](#)  
 Local [374](#)  
 Log [604](#)  
 Log Facility [605](#)  
 Logging [61](#)  
 Login Name [533](#)  
 Login Screen [501](#)

## M

MAC Address [515](#)  
 MAC Address Filter Action [546](#)  
 MAC Address Filtering [200](#)  
 MAC filter [184](#)  
 MAC service data unit [545](#)  
 Macro virus [258](#)  
 Mail Sessions Threshold [271](#)  
 Main Menu [502](#)  
 Main Menu Commands [501](#)  
 Management Information Base (MIB) [449](#)  
 Many to Many No Overload [377](#)  
 Many to Many Overload [377](#)  
 Many to One [377](#)  
 Materials [6](#)  
 Max Age [124](#)  
 Maximize Bandwidth Usage [404](#), [409](#)  
 Maximum Incomplete High [230](#)  
 Maximum Incomplete Low [229](#)  
 Max-incomplete High [227](#)  
 Max-incomplete Low [227](#), [230](#)  
 Mean Time Between Failures [665](#)  
 Merchantability [6](#)  
 Message Integrity Check [187](#)  
 Message Integrity Check (MIC) [718](#)  
 Metric [134](#), [395](#), [523](#), [554](#), [557](#), [561](#)  
 MIC [187](#)

MIME [273](#)  
MIME Header [276](#)  
MIME Headers [270](#)  
MIME Value [276](#)  
Modifications [3](#)  
MSDU [545](#)  
Multicast [112](#), [114](#), [176](#), [523](#), [529](#), [557](#)  
Multimedia [235](#), [469](#)  
Multipurpose Internet Mail Extensions [270](#)  
Mutation virus [258](#)  
My IP Addr [555](#)  
My Login [519](#), [552](#)  
My Login Name [533](#)  
My Password [519](#), [533](#), [552](#)  
My Server IP Addr [555](#)  
My WAN Address [522](#)  
MyDoom [241](#), [243](#)  
mySecurity Zone [254](#), [263](#)  
myZyXEL.com [104](#)

## N

Nailed-Up Connection [554](#)  
Nailed-up Connection [553](#)  
Nailed-Up Connections [555](#)  
NAT [111](#), [384](#), [385](#), [522](#), [523](#), [556](#), [557](#), [595](#)  
    Application [376](#)  
    Applying NAT in the SMT Menus [562](#)  
    Configuring [564](#)  
    Definitions [374](#)  
    Examples [572](#)  
    How NAT Works [375](#)  
    Mapping Types [377](#)  
    NAT Unfriendly Application Programs [578](#)  
    Ordering Rules [567](#)  
    Port Restricted Cone [377](#)  
    What NAT does [375](#)  
NAT Routers [469](#)  
NAT Traversal [456](#), [458](#)  
NAT traversal [310](#)  
Navigation Panel [74](#)  
Negotiation Mode [314](#)  
NetBIOS commands [207](#)  
Network Address Translation [533](#)  
Network Address Translation (NAT) [60](#)  
Network Address Translators [469](#)  
Network Management [384](#)  
Network Policy [316](#)  
New [6](#)  
Nimda [241](#), [242](#)

Nmap [247](#)  
NNTP [384](#)  
North America [5](#)  
North America Contact Information [7](#)  
Norway, Contact Information [7](#)

## O

Offline [512](#)  
One Minute High [229](#)  
One Minute Low [229](#)  
One to One [377](#)  
One-Minute High [228](#)  
Opening [5](#)  
Operating Condition [6](#)  
Out-dated Warranty [6](#)  
Outgoing Protocol Filters [531](#)  
Outlet [3](#)  
Outside [374](#)

## P

Packet Filtering [59](#), [212](#)  
Packet Filtering Firewalls [202](#)  
Pairwise Master Key (PMK) [718](#)  
PAP [519](#), [554](#)  
Parts [6](#)  
Password [485](#), [501](#), [506](#), [533](#), [598](#)  
Patent [2](#)  
Path cost [123](#)  
PCMCIA Port [56](#)  
Perfect Forward Secrecy [315](#)  
Period(hr) [520](#), [554](#)  
Permission [2](#)  
Phishing [268](#)  
Phishing Tag [271](#)  
Photocopying [2](#)  
Ping [610](#)  
Ping of Death [205](#)  
Pipes [5](#)  
Point-to-Point Tunneling Protocol [87](#), [384](#)  
Point-to-Point Tunneling Protocol See PPTP [150](#)  
Policy Actions [248](#)  
    Types [249](#)  
Policy Query [250](#)  
Policy Severity [248](#)

Levels [248](#)  
 Policy-based Routing [396](#)  
 Polyphormic virus [258](#)  
 Pool [5](#)  
 POP2 [269](#)  
 POP3 [204](#), [269](#), [271](#), [273](#), [384](#)  
 Port Forwarding [61](#)  
 Port Restricted Cone NAT [377](#)  
 port scans [240](#)  
 Post Office Protocol [269](#)  
 Postage Prepaid. [6](#)  
 Power Cord [5](#)  
 PPP [520](#)  
 PPPoE [59](#), [84](#), [86](#), [702](#)  
 PPPoE Encapsulation [532](#), [535](#), [551](#), [553](#), [554](#), [558](#)  
 PPTP [84](#), [87](#), [147](#), [150](#), [384](#)  
   Client [534](#)  
   Configuring a Client [534](#)  
 PPTP Encapsulation [59](#), [87](#)  
 Preamble Mode [712](#)  
 Precedence [396](#)  
 Pre-Shared Key [314](#), [321](#)  
 Prestige anti-virus packet scan [259](#)  
 Priority-based Scheduler [404](#)  
 Private [395](#), [523](#), [557](#), [561](#)  
 Private IP Address [142](#)  
 Product Model [7](#)  
 Product Page [3](#)  
 Product Serial Number [7](#)  
 Products [6](#)  
 Proof of Purchase [6](#)  
 Proper Operating Condition [6](#)  
 Proportional Bandwidth Allocation [403](#)  
 Protocol Filters [530](#)  
   Incoming [530](#)  
   Outgoing [530](#)  
 Protocol/Port [479](#), [480](#)  
 Purchase, Proof of [6](#)  
 Purchaser [6](#)

## Q

Qualified Service Personnel [5](#)  
 Quality of Service [396](#)  
 Quick Start Guide [66](#)

## R

Radio Communications [3](#)  
 Radio Frequency Energy [3](#)  
 Radio Interference [3](#)  
 Radio Reception [3](#)  
 Radio Technician [3](#)  
 RADIUS [58](#), [185](#), [713](#)  
   Shared Secret Key [186](#), [714](#)  
 RADIUS Message Types [185](#), [713](#)  
 RADIUS Messages [713](#)  
 Rapid STP [123](#)  
 RAS [397](#)  
 Read Me First [52](#)  
 Real Time Chip [56](#)  
 Real time Transport Protocol [467](#)  
 real-time alert message [726](#)  
 Receiving Antenna [3](#)  
 Registered [2](#)  
 Registered Trademark [2](#)  
 Regular Mail [7](#)  
 Related Documentation [52](#)  
 Relay [528](#)  
 Relocate [3](#)  
 Rem IP Address [522](#)  
 Rem Node Name [519](#), [521](#), [552](#)  
 Re-manufactured [6](#)  
 Remote Authentication Dial In User Service See  
   RADIUS [58](#)  
 Remote Management [636](#)  
 Remote Management Limitations [432](#)  
 Remote Node [550](#)  
 Remote Node Filter [525](#), [557](#)  
 Removing [5](#)  
 Removing and Installing Fuses [676](#)  
 Reorient [3](#)  
 Repair [6](#)  
 Replace [6](#)  
 Replacement [6](#)  
 Reports [478](#)  
 Reproduction [2](#)  
 Required fields [502](#)  
 Reset Button [56](#)  
 Resetting the Time [489](#)  
 Resetting the ZyWALL [67](#)  
 Resource Usage [274](#)  
 Restore [6](#), [497](#)  
 Restore Configuration [618](#)  
 retry count [518](#)  
 retry interval [518](#)



Return Material Authorization (RMA) Number [6](#)  
Returned Products [6](#)  
Returns [6](#)  
RFC 1889 [467](#)  
RFC 3489 [469](#)  
Rights [2](#)  
Rights, Legal [6](#)  
RIP [111](#), [112](#), [523](#), [529](#), [530](#), [557](#)  
    Direction [530](#)  
    Version [530](#), [557](#)  
Risk [5](#)  
Risks [5](#)  
RMA [6](#)  
RoadRunner Support [61](#)  
Roaming [719](#)  
    Example [720](#)  
    Requirements [721](#)  
Root bridge [123](#)  
Root Class [410](#)  
Route [552](#)  
Routing Policy [396](#)  
RTC [486](#), [632](#)  
RTC See Real Time Chip [56](#)  
RTP [467](#)  
RTS (Request To Send) [711](#)  
RTS (Request To Send) threshold [191](#)  
RTS Threshold [710](#), [711](#)  
RTS/CTS handshake [545](#)  
Rubber feet [672](#)  
Rules [214](#), [218](#)  
    Checklist [216](#)  
    Creating Custom [214](#)  
    Key Fields [216](#)  
    LAN to WAN [217](#)  
    Logic [216](#)

## S

SA (Security Association) [302](#)  
Safety Warnings [5](#)  
Saving the State [208](#)  
Schedule Sets  
    Duration [649](#)  
Scheduler [404](#), [409](#)  
Schedules [552](#), [554](#), [555](#)  
Secure FTP Using SSH Example [445](#)  
Secure Telnet Using SSH Example [444](#)  
Security Parameters [719](#)  
Security Ramifications [216](#)

Separation Between Equipment and Receiver [3](#)  
Serial Number [7](#)  
Server [378](#), [488](#), [489](#), [533](#), [552](#), [564](#), [566](#), [568](#), [569](#), [572](#),  
    [574](#), [575](#), [634](#)  
Server IP [552](#)  
Service [5](#), [6](#), [217](#)  
Service Name [554](#)  
Service Personnel [5](#)  
Service Set [191](#)  
Service Status [273](#)  
Service Type [231](#), [232](#), [533](#), [552](#)  
Services [384](#)  
Session Initiation Protocol [235](#), [469](#)  
Set Up a Schedule [648](#)  
Shipping [6](#)  
Shock, Electric [5](#)  
Signature Categories  
    Backdoor/Trojan [247](#)  
    Buffer Overflow [247](#)  
    IM [247](#)  
    P2P [247](#)  
    Scan [247](#)  
    Virus/Worm [248](#)  
Simple Mail Transfer Protocol [269](#)  
SIP Application Layer Gateway [56](#)  
SMT [501](#)  
SMT Menu Overview [504](#)  
SMTP [269](#), [271](#), [273](#), [384](#)  
Smurf [206](#), [207](#)  
SNMP [60](#), [384](#), [448](#)  
    Community [598](#)  
    Configuration [598](#)  
    Get [449](#)  
    Manager [449](#)  
    MIBs [450](#)  
    Trap [449](#)  
    Trusted Host [598](#)  
SNMP (Simple Network Management Protocol) [60](#)  
Source Address [217](#), [225](#)  
Source E-mail Address [276](#)  
Source-Based Routing [396](#)  
Spain, Contact Information [8](#)  
Spam [58](#), [266](#)  
Spam Patterns [266](#)  
Spam Score [268](#), [272](#)  
    Invalid [273](#)  
Spam Score Threshold [272](#)  
Spam Tag [271](#)  
Spam Threshold [268](#), [272](#)  
Spanning Tree Protocol [122](#)  
Speed [269](#)  
Spoofing [269](#)

SSH [57](#), [441](#)  
 SSH Implementation [442](#)  
 startup [728](#)  
 Stateful Inspection [57](#), [202](#), [203](#), [208](#), [209](#)  
     Process [209](#)  
     ZyWALL [210](#)  
 Static Route [392](#)  
 Storage Space [274](#)  
 STP (Spanning Tree Protocol) [56](#)  
 STP Port States [124](#)  
 STP See Spanning Tree Protocol [122](#)  
 STP Terminology [123](#)  
 SUA (Single User Account) [378](#), [562](#)  
 Sub-class Layers [410](#)  
 Subnet Mask [111](#), [113](#), [125](#), [175](#), [225](#), [276](#), [522](#), [529](#),  
     [533](#), [556](#), [561](#)  
 Subnet Masks [695](#)  
 Subnetting [695](#)  
 Supply Voltage [5](#)  
 Support E-mail [7](#)  
 Supporting Disk [52](#)  
 Sweden, Contact Information [8](#)  
 Swimming Pool [5](#)  
 SYN Flood [205](#), [206](#)  
 SYN scanning [247](#)  
 SYN-ACK [205](#)  
 Syntax Conventions [53](#)  
 Syslog [235](#), [239](#)  
 Syslog IP Address [605](#)  
 System Information [600](#), [602](#)  
 System Maintenance [600](#), [601](#), [602](#), [603](#), [604](#), [605](#), [608](#),  
     [609](#), [610](#), [613](#), [616](#), [624](#), [625](#), [628](#), [630](#), [631](#), [633](#), [634](#)  
 System Management Terminal [501](#)  
 System Name [485](#), [508](#)  
 System Statistics [79](#)  
 System Status [600](#)  
 System Timeout [433](#)

## T

Tag for No Spam Score [273](#)  
 Tampering [6](#)  
 task bar properties [727](#)  
 TCP Maximum Incomplete [228](#), [230](#)  
 TCP Security [210](#)  
 TCP/IP [204](#), [205](#), [446](#), [521](#), [527](#), [529](#), [537](#), [547](#), [555](#),  
     [589](#), [590](#), [592](#), [595](#)  
     Setup [529](#)  
 TCP/IP and DHCP Setup [527](#)

TCP/IP filter rule [589](#)  
 Teardrop [205](#)  
 Telephone [7](#)  
 Television Interference [3](#)  
 Television Reception [3](#)  
 Telnet [446](#)  
 Telnet Configuration [446](#)  
 Temporal Key Integrity Protocol [187](#)  
 Temporal Key Integrity Protocol (TKIP) [718](#)  
 Terminal Emulation [500](#)  
 TFTP [616](#)  
     File Upload [623](#)  
     GUI-based Clients [617](#)  
 TFTP and FTP over WAN [615](#)  
 TFTP Restrictions [432](#), [615](#), [638](#)  
 Three-Way Handshake [205](#)  
 Threshold Values [227](#)  
 Thunderstorm [5](#)  
 Time and Date [56](#)  
 Time and Date Setting [632](#), [633](#)  
 Time Zone [486](#), [635](#)  
 Timeout [520](#), [534](#), [535](#), [554](#)  
 TKIP [187](#)  
 ToS (Type of Service) [396](#)  
 Trace [604](#)  
 Traceroute [208](#)  
 Tracing [61](#)  
 Trademark [2](#)  
 Trademark Owners [2](#)  
 Trademarks [2](#)  
 Traffic Redirect [61](#), [153](#), [154](#)  
 Translation [2](#)  
 Transport mode [305](#)  
 Trial Active [273](#)  
 Trigger Port Forwarding [579](#)  
 Trivial File Transfer Protocol [616](#)  
 Trojan horse [247](#)  
 Tunnel mode [305](#)  
 TV Technician [3](#)  
 Type of Service [396](#)  
 Types of Anti-virus scanner [259](#)

## U

UDP/ICMP Security [211](#)  
 Undesired Operations [3](#)  
 Universal Plug and Play (UPnP) [456](#), [457](#)  
 UNIX Syslog [605](#)

Unsolicited Commercial E-mail [266](#)  
Upload Firmware [621](#)  
UPnP [58](#), [456](#)  
UPnP Examples [459](#)  
UPnP Port Mapping [458](#)  
Upper Layer Protocols [210](#), [211](#)  
Use Server Detected IP [513](#)  
User Authentication [187](#), [718](#)  
User Name [510](#)  
User Profiles [370](#)

## V

Value [6](#)  
Vendor [5](#)  
Ventilation Slots [5](#)  
Viewing Certifications [3](#)  
Virtual Private Network [57](#)  
virus [248](#)  
Virus attack [258](#)  
Virus life cycle [258](#)  
Voltage Supply [5](#)  
Voltage, High [5](#)  
VPN [150](#)  
    encapsulation [304](#)  
    keep alive [310](#)  
    key management [304](#)  
    secure gateway [309](#)  
VPN Application [62](#), [303](#)  
VT100 [500](#)

## W

Wall Mount [5](#)  
WAN DHCP [609](#), [610](#)  
WAN Setup [143](#), [514](#)  
WAN to LAN Rules [218](#)  
Warnings [5](#)  
Warranty [6](#)  
Warranty Information [7](#)  
Warranty Period [6](#)  
Water [5](#)  
Water Pipes [5](#)  
Web [446](#)  
Web attack [248](#)  
Web Configurator [66](#), [68](#), [203](#), [212](#), [216](#), [583](#)  
Web Site [7](#)

Web Site Hits [479](#), [480](#)  
WEP Encryption [59](#), [193](#), [197](#), [200](#)  
WEP encryption [716](#)  
Wet Basement [5](#)  
Whitelist [266](#), [269](#), [274](#)  
Wi-Fi Protected Access [187](#)  
WinPopup window [726](#)  
Wireless LAN [56](#)  
Wireless LAN MAC Address Filtering [59](#)  
Wireless LAN Setup [544](#)  
Wizard Setup [84](#)  
WLAN  
    Interference [710](#)  
    Security parameters [719](#)  
Workmanship [6](#)  
Worldwide Contact Information [7](#)  
Worm [242](#), [258](#)  
    Blaster [242](#)  
    SQL Slammer [242](#)  
worm [248](#)  
WPA [187](#)  
WPA-PSK [187](#)  
Written Permission [2](#)  
WWW [434](#)  
www.dyndns.org [512](#)

## X

Xmodem  
    File Upload [625](#)  
XMODEM Protocol [613](#)

## Z

ZyNOS [2](#), [603](#), [613](#)  
ZyNOS F/W Version [603](#), [613](#)  
ZyXEL Communications Corporation [2](#)  
ZyXEL Home Page [3](#)  
ZyXEL Limited Warranty  
    Note [6](#)  
ZyXEL Network Operating System [2](#)  
ZyXEL's Firewall  
    Introduction [203](#)